REGULAMENTO (UE) 2019/881 DO PARLAMENTO EUROPEU E DO CONSELHO

de 17 de abril de 2019

relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança)

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu ([1]),

Tendo em conta o parecer do Comité das Regiões ([2]),

Deliberando de acordo com o processo legislativo ordinário ([3]),

Considerando o seguinte:

(1) As redes e os sistemas de informação e as redes e os serviços de comunicações eletrónicas desempenham um papel crucial na sociedade e tornaram-se a espinha dorsal do crescimento económico. As tecnologias da informação e comunicação (TIC) estão na base de sistemas complexos que apoiam as atividades sociais quotidianas, asseguram o funcionamento das nossas economias em setores determinantes como a saúde, a energia, as finanças e os transportes e apoiam, em especial, o funcionamento do mercado interno.

(2) A utilização de redes e sistemas de informação por cidadãos, organizações e empresas da União é agora generalizada. A digitalização e a conectividade estão a tornar-se características centrais num número cada vez maior de produtos e serviços e, com o surgimento da Internet das coisas (IdC), espera-se que um número extremamente elevado de dispositivos digitais conectados seja implantado em toda a União durante a próxima década. Embora haja cada vez mais dispositivos conectados à Internet, a segurança e a resiliência não são suficientemente integradas na conceção, o que conduz a uma insuficiência a nível da cibersegurança. Nesse contexto, a utilização reduzida da certificação conduz à insuficiência da informação ao dispor dos utilizadores, sejam estes particulares, organizações ou empresas, sobre as características de cibersegurança dos produtos, serviços e processos de TIC, o que compromete a confiança nas soluções digitais. As redes e os sistemas de informação têm capacidade para apoiar todos os aspetos das nossas vidas e impulsionar o crescimento económico da União, constituindo a pedra angular da realização do mercado único digital.

(3) A digitalização e conectividade crescentes acarretam maiores riscos para a cibersegurança, tornando, assim, a sociedade em geral mais vulnerável a ciberameaças e agravando os perigos que as pessoas enfrentam, nomeadamente as pessoas vulneráveis como as crianças. A fim de reduzir esses riscos, têm de ser adotadas todas as medidas necessárias para aumentar a cibersegurança na União de modo a que as redes e os sistemas de informação, as redes de comunicações e os produtos, serviços e dispositivos digitais utilizados pelos cidadãos, organizações e empresas — desde as pequenas e médias empresas (PME) na aceção da Recomendação 2003/361/CE da Comissão ([4]) aos operadores de infraestruturas críticas — estejam melhor protegidos das ciberameaças.

([1]) JO C 227 de 28.6.2018, p. 86.
([2]) JO C 176 de 23.5.2018, p. 29.
([3]) Posição do Parlamento Europeu de 12 de março de 2019 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 9 de abril de 2019.
([4]) Recomendação da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

(4) Ao disponibilizar ao público as informações relevantes, a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), criada pelo Regulamento (UE) n.º 526/2013 do Parlamento Europeu e do Conselho ([5]) contribui para o desenvolvimento da indústria da cibersegurança na União, em especial as PME e as empresas em fase de arranque. A ENISA deverá envidar esforços no sentido de uma cooperação mais estreita com as universidades e os organismos de investigação, a fim de contribuir para reduzir a dependência de produtos e serviços de cibersegurança de fora da União e para reforçar as cadeias de abastecimento no interior da União.

(5) Os ciberataques aumentam e as economias e sociedades conectadas, mais vulneráveis a ciberameaças e ciberataques, requerem defesas mais robustas. No entanto, apesar de os ciberataques terem amiúde uma natureza transfronteiriça, a competência das autoridades responsáveis pela cibersegurança e pelo controlo da aplicação da lei é predominantemente nacional, bem como as ações por estas adotadas. Os incidentes em grande escala são suscetíveis de perturbar a prestação de serviços essenciais na União. Esta realidade implica uma atuação e gestão de crises efetiva e coordenada a nível da União, com base em políticas específicas e instrumentos mais abrangentes para a solidariedade e a assistência mútua a nível europeu. Além disso, é importante para os decisores políticos, para a indústria e os utilizadores que se proceda a uma avaliação regular da situação em matéria de cibersegurança e de resiliência na União, com base em dados fiáveis da União, bem como a previsões sistemáticas da evolução, dos desafios e das ameaças futuras, tanto a nível da União como a nível mundial.

(6) Atendendo aos desafios de cibersegurança cada vez maiores que a União enfrenta, afigura-se necessário um conjunto abrangente de medidas que tenha por base ações anteriores da União e que promova objetivos que se reforcem mutuamente. Entre estes contam-se o reforço das capacidades e do grau de preparação dos Estados-Membros e das empresas, bem como melhorar a cooperação, o intercâmbio de informações e a coordenação entre Estados-Membros e instituições, órgãos e organismos da União. Além disso, atendendo à natureza transfronteiriça das ciberameaças, é necessário aumentar a nível da União as capacidades suscetíveis de complementar a ação dos Estados-Membros, designadamente em casos de crises e incidentes transfronteiriços em grande escala, tendo simultaneamente em conta a importância de manter e reforçar as capacidades nacionais de resposta a ciberameaças de qualquer escala.

(7) São também necessários mais esforços para aumentar a sensibilização dos cidadãos, das organizações e das empresas para as questões da cibersegurança. Além disso, dado que os incidentes comprometem a confiança, nomeadamente dos consumidores, nos prestadores de serviços digitais e no próprio mercado único digital, é necessário continuar a reforçar a confiança mediante a disponibilização de informações de forma transparente sobre o nível de segurança dos produtos, processos e serviços de TIC, realçando que mesmo um nível elevado de certificação da cibersegurança não consegue garantir a total segurança de um produto, serviço ou processo de TIC. O aumento da confiança pode ser mais facilmente alcançado por meio de uma certificação a nível da União que preveja requisitos de cibersegurança e critérios de avaliação comuns nos mercados e setores nacionais.

(8) A cibersegurança não é só uma questão relacionada com a tecnologia; o comportamento humano é igualmente importante. Por conseguinte, dever-se-á promover ativamente aquilo que se entente por «ciber-higiene», ou seja, medidas simples de rotina que, quando implementadas e aplicadas com regularidade pelos cidadãos, as organizações e as empresas, minimizam a sua exposição aos riscos decorrentes de ciberameaças.

(9) No intuito de reforçar as estruturas de cibersegurança da União, é importante manter e desenvolver as capacidades dos Estados-Membros para responder de forma exaustiva às ciberameaças, incluindo os incidentes transfronteiriços.

(10) As empresas e os consumidores particulares deverão dispor de informações exatas sobre o nível de garantia para o qual foi certificada a segurança dos seus produtos, serviços e processos de TIC. Ao mesmo tempo, nenhum produto ou serviço de TIC é totalmente ciberseguro e é necessário promover e dar prioridade a regras básicas de ciber-higiene. Dada a crescente disponibilidade de dispositivos da IdC, há uma gama de medidas voluntárias que o setor privado pode tomar para reforçar a confiança na segurança dos produtos, serviços e processos de TIC.

(11) Os produtos e sistemas de TIC modernos integram e baseiam-se muitas vezes numa ou em mais tecnologias e componentes de terceiros, tais como módulos ou bibliotecas de programas informáticos ou interfaces de programação de aplicações. Esta situação, que se designa por «dependência», poderá acarretar riscos adicionais para a cibersegurança, uma vez que as vulnerabilidades existentes em componentes de terceiros também poderão afetar a segurança dos produtos, serviços e processos de TIC. Em muitos casos, a identificação e a documentação dessas dependências permite que os utilizadores finais dos produtos, serviços e processos de TIC aperfeiçoem as suas atividades de gestão dos riscos para a cibersegurança, reforçando, por exemplo, a gestão das vulnerabilidades de cibersegurança dos utilizadores, assim como os procedimentos de correção.

([5]) Regulamento (UE) n.º 526/2013 do Parlamento Europeu e do Conselho, de 21 de maio de 2013, relativo à Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004 (JO L 165 de 18.6.2013, p. 41).

(12) As organizações, os fabricantes ou os prestadores de serviços envolvidos na conceção e no desenvolvimento de produtos, serviços ou processos de TIC deverão ser incentivados a tomar medidas, nas fases iniciais de conceção e desenvolvimento, para proteger a segurança desses produtos, serviços e processos ao nível mais elevado possível, de uma tal forma que se presuma a ocorrência de ciberataques e que se preveja e minimize o seu impacto («segurança desde a conceção»). É necessário garantir a segurança ao longo da vida útil dos produtos, serviços ou processos de TIC, através de processos de conceção e desenvolvimento em evolução constante de modo a reduzir os prejuízos causados por exploração maliciosa.

(13) As empresas, as organizações e o setor público deverão configurar os produtos, serviços ou processos de TIC por eles concebidos de forma a garantir um nível mais elevado de segurança, o que deverá assegurar que o primeiro utilizador disponha de uma configuração por defeito com definições da mais elevada segurança possível («segurança por defeito»), reduzindo assim o ónus que impende sobre os utilizadores de configurarem os produtos, serviços ou processo de TIC de forma adequada. A segurança por defeito não deverá exigir uma configuração extensa, nem conhecimentos técnicos específicos ou comportamentos não intuitivos da parte do utilizador e deverá permitir um funcionamento fácil e fiável quando implementada. Se, numa base caso a caso, em função de uma análise de risco e da facilidade de utilização, se concluir que uma tal definição por defeito não é viável, os utilizadores deverão ser alertados para optarem pela definição mais segura.

(14) O Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho ([6]) criou a ENISA, a fim de contribuir para a consecução dos objetivos de garantir um nível elevado e eficaz de segurança das redes e da informação na União e de desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas. O Regulamento (CE) n.º 1007/2008 do Parlamento Europeu e do Conselho ([7]) prorrogou o mandato da ENISA até março de 2012. O Regulamento (UE) n.º 580/2011 do Parlamento Europeu e do Conselho ([8]) prorrogou novamente o mandato da Agência até 13 de setembro de 2013. O Regulamento (UE) n.º 526/2013 prorrogou o mandato da ENISA até 19 de junho de 2020.

(15) A União já tomou medidas importantes para garantir a cibersegurança e reforçar a confiança nas tecnologias digitais. Em 2013, foi adotada a Estratégia da União Europeia para a Cibersegurança, a fim de orientar a resposta política da União às ciberameaças e aos riscos para a cibersegurança. Num esforço para melhor proteger os cidadãos em linha, a União adotou o primeiro ato legislativo no domínio da cibersegurança em 2016: a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([9]). A Diretiva (UE) 2016/1148 estabeleceu requisitos relativos às capacidades nacionais no domínio da cibersegurança, criou os primeiros mecanismos para reforçar a cooperação estratégica e operacional entre os Estados-Membros e impôs obrigações relativas às medidas de segurança e notificações de incidentes nos setores que são vitais para a economia e a sociedade, tais como a energia, os transportes, o fornecimento e a distribuição de água potável, a banca, as infraestruturas do mercado financeiro, os cuidados de saúde, as infraestruturas digitais, bem como os prestadores de serviços digitais essenciais (motores de busca, serviços de computação em nuvem e mercados em linha).

Foi atribuída à ENISA uma função importante de apoio à execução da referida diretiva. Além disso, a luta eficaz contra a cibercriminalidade constitui uma prioridade importante da Agenda Europeia para a Segurança, o que contribui para o objetivo geral de alcançar um elevado nível de cibersegurança. Há ainda outros atos jurídicos, como o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([10]) e as Diretivas 2002/58/CE ([11]) e (UE) 2018/1972 ([12]) do Parlamento Europeu e do Conselho, que também contribuem para um elevado nível de cibersegurança no mercado único digital.

([6]) Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação (JO L 77 de 13.3.2004, p. 1).

([7]) Regulamento (CE) n.º 1007/2008 do Parlamento Europeu e do Conselho, de 24 de setembro de 2008, que altera o Regulamento (CE) n.º 460/2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, no que respeita à duração da agência (JO L 293 de 31.10.2008, p. 1).

([8]) Regulamento (UE) n.º 580/2011 do Parlamento Europeu e do Conselho, de 8 de junho de 2011, que altera o Regulamento (CE) n.º 460/2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, no que respeita à duração da agência (JO L 165 de 24.6.2011, p. 3).

([9]) Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

([10]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

([11]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

([12]) Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas (JO L 321 de 17.12.2018, p. 36).

(16) Desde a adoção da Estratégia da União Europeia para a Cibersegurança, de 2013, e da última revisão do mandato da ENISA, o contexto geral de ação política alterou-se significativamente, uma vez que o ambiente mundial se tornou mais incerto e menos seguro. Com este pano de fundo e no contexto da evolução positiva da função da ENISA como ponto de referência em matéria de aconselhamento e conhecimentos especializados e como facilitadora da cooperação e do desenvolvimento de capacidades, assim como no âmbito da nova política de cibersegurança da União, é necessário rever o mandato da ENISA para estabelecer o seu papel no ecossistema alterado de cibersegurança e assegurar que contribua eficazmente para a resposta da União aos desafios de cibersegurança decorrentes do cenário de ciberameaça radicalmente transformado, para o qual, conforme se reconheceu durante a avaliação da própria ENISA, o mandato atual não é suficiente.

(17) A ENISA criada pelo presente regulamento deverá suceder à ENISA criada pelo Regulamento (UE) n.º 526/2013. A ENISA deverá exercer as atribuições que lhe são conferidas pelo presente regulamento e pelos outros atos jurídicos da União no domínio da cibersegurança, nomeadamente disponibilizando aconselhamento e conhecimentos especializados e funcionando como um centro de informação e de conhecimentos da União. A ENISA deverá promover o intercâmbio de melhores práticas entre os Estados-Membros e as partes interessadas do setor privado, apresentando à Comissão e aos Estados-Membros sugestões de ação política, atuando como um ponto de referência para as iniciativas de política setorial da União no tocante às questões de cibersegurança e promovendo a cooperação operacional entre os Estados-Membros e entre os Estados-Membros e as instituições, órgãos e organismos da União.

(18) No âmbito da Decisão 2004/97/CE, Euratom, tomada de comum acordo entre os representantes dos Estados-Membros reunidos a nível de Chefes de Estados ou de Governo ([13]), os representantes dos Estados-Membros decidiram que a ENISA ficaria sediada numa cidade da Grécia, a determinar pelo Governo grego. O Estado-Membro de acolhimento da ENISA deverá assegurar as melhores condições possíveis para o funcionamento normal e eficiente da ENISA. Para poder exercer correta e eficientemente as suas atribuições, recrutar e fixar o seu pessoal e aumentar a eficiência das suas atividades de rede, é indispensável que a ENISA esteja sediada num local adequado que ofereça, nomeadamente, ligações de transporte e serviços adequados aos cônjuges e filhos dos membros do seu pessoal. As disposições necessárias deverão ser estabelecidas num acordo entre a ENISA e o Estado-Membro de acolhimento, celebrado após aprovação do conselho de administração da ENISA.

(19) Atendendo ao aumento dos riscos e desafios de cibersegurança que a União enfrenta, haverá que aumentar os recursos financeiros e humanos atribuídos à ENISA para refletir o reforço do seu papel e das suas atribuições, bem como a sua posição crucial no sistema das organizações que defendem o ecossistema digital da União, permitindo-lhe exercer com eficácia as atribuições que lhe são conferidas pelo presente regulamento.

(20) A ENISA deverá desenvolver e manter um elevado nível de conhecimentos especializados e servir de ponto de referência que instaure a confiança no mercado único graças à sua independência, à qualidade do aconselhamento prestado, à qualidade das informações que divulga, à transparência dos seus procedimentos, à transparência dos seus métodos de funcionamento e à sua diligência no exercício das suas atribuições. A ENISA deverá apoiar ativamente os esforços nacionais e contribuir de forma proativa para os esforços da União, exercendo simultaneamente as suas atribuições em plena cooperação com as instituições, os órgãos e os organismos da União e com os Estados-Membros, evitando a duplicação de esforços e promovendo as sinergias. Além disso, a ENISA deverá tirar partido da cooperação com o setor privado e outras partes interessadas e dos seus contributos. Um conjunto de atribuições deverá determinar o modo como a ENISA deverá atingir os seus objetivos, permitindo-lhe ao mesmo tempo flexibilidade de funcionamento.

(21) A fim de poder prestar um apoio adequado à cooperação operacional entre os Estados-Membros, a ENISA deverá reforçar ainda mais as suas próprias capacidades e competências a nível técnico e humano. A ENISA deverá aumentar os seus conhecimentos especializados e as suas capacidades. A ENISA e os Estados-Membros poderão, a título voluntário, desenvolver programas de destacamento de peritos nacionais para a ENISA, criando grupos de peritos e fomentando o intercâmbio de pessoal.

(22) A ENISA deverá prestar assistência à Comissão por meio de aconselhamento, da formulação de pareceres e da realização de análises sobre todas as matérias da competência da União relacionadas com a elaboração, atualização e revisão das políticas e da legislação no domínio da cibersegurança e dos respetivos aspetos setoriais específicos, a fim de aumentar a pertinência das políticas e da legislação da União com uma vertente de cibersegurança e de permitir a aplicação coerente dessas políticas e dessa legislação. A ENISA deverá atuar como um ponto de referência de aconselhamento e conhecimentos especializados para iniciativas políticas e legislativas que envolvam questões relacionadas com a cibersegurança. A ENISA deverá informar regularmente o Parlamento Europeu sobre as suas atividades.

([13]) Decisão 2004/97/CE, Euratom, tomada de comum acordo pelos Representantes dos Estados-Membros, reunidos a nível de Chefe de Estado ou de Governo, de 13 de dezembro de 2003, sobre a localização das sedes de certos serviços e agências de União Europeia (JO L 29 de 3.2.2004, p. 15).

(23) O núcleo público da internet aberta, ou seja, os seus principais protocolos e infraestruturas, que são um bem público mundial, assegura a principal funcionalidade da internet no seu conjunto e serve de base ao seu funcionamento normal. A ENISA deverá apoiar a segurança do núcleo público da internet aberta e a estabilidade do seu funcionamento, incluindo, entre outros, os protocolos essenciais (nomeadamente, DNS, BGP e IPv6), o funcionamento do sistema de nomes de domínio (tal como o funcionamento de todos os domínios de topo) e o funcionamento da zona de raiz.

(24) A atribuição de base da ENISA é promover a aplicação coerente do regime jurídico aplicável, nomeadamente a execução eficaz da Diretiva (UE) 2016/1148 e de outros instrumentos jurídicos aplicáveis que contenham elementos de cibersegurança, o que é essencial para aumentar a ciber-resiliência. Atendendo à rápida evolução do cenário de ciberameaça, é evidente que os Estados-Membros devem ser apoiados através de uma abordagem mais abrangente e transversal em matéria de ação política para reforçar a ciber-resiliência.

(25) A ENISA deverá prestar assistência aos Estados-Membros e às instituições, órgãos e organismos da União nos seus esforços para criar e reforçar as capacidades e o grau de preparação para prevenir, detetar e responder a ciberameaças e incidentes de cibersegurança e em relação à segurança das redes e dos sistemas de informação. Concretamente, a ENISA deverá apoiar o desenvolvimento e o reforço da equipa de resposta a incidentes de segurança informática (CSIRT) nacionais e da União, previstas na Diretiva (UE) 2016/1148 a fim de que estas atinjam um elevado nível comum de maturidade na União. As atividades exercidas pela ENISA que se relacionem com as capacidades operacionais dos Estados-Membros deverão apoiar ativamente as medidas por estes adotadas para dar cumprimento às obrigações que lhes incumbem por força da Diretiva (UE) 2016/1148, não devendo, pois, substituí-las.

(26) A ENISA deverá igualmente prestar assistência no desenvolvimento e na atualização, a nível da União e, a pedido, dos Estados-Membros, de estratégias de segurança das redes e dos sistemas de informação, nomeadamente de cibersegurança, e deverá promover a divulgação dessas estratégias e acompanhar os progressos realizados na sua execução. A ENISA deverá também contribuir para dar resposta às necessidades de formação e de material de formação, inclusive dos organismos públicos, e, se se justificar, em grande medida, para «formar os formadores» com base no Quadro de Competências Digitais para os Cidadãos, no intuito de assistir os Estados-Membros e as instituições, os órgãos e organismos da União no desenvolvimento das suas próprias capacidades de formação.

(27) A ENISA deverá apoiar os Estados-Membros nos domínios da sensibilização e da educação para a cibersegurança, facilitando o reforço da coordenação e o intercâmbio das melhores práticas entre os Estados-Membros. Esse apoio poderá consistir, nomeadamente, no desenvolvimento de uma rede de pontos de contacto nacionais em matéria de educação e de uma plataforma de formação em matéria de cibersegurança. A rede de pontos de contacto nacionais em matéria de educação poderá funcionar dentro da rede de agentes de ligação nacionais e servir de ponto de partida para a futura coordenação no interior dos Estados-Membros.

(28) A ENISA deverá assistir o grupo de cooperação criado pela Diretiva (UE) 2016/1148 no exercício das suas atribuições, em especial fornecendo conhecimentos especializados e aconselhamento e facilitando o intercâmbio das melhores práticas, referentes, entre outros, à identificação dos operadores de serviços essenciais pelos Estados-Membros, incluindo quanto a dependências transfronteiriças, no que respeita a riscos e incidentes.

(29) Com vista a estimular a cooperação entre o setor público e privado e dentro do setor privado, nomeadamente para apoiar a defesa de infraestruturas críticas, a ENISA deverá apoiar a partilha de informações dentro dos diferentes setores e entre eles, em particular setores enumerados no anexo II da Diretiva (UE) 2016/1148, divulgando as melhores práticas e orientações sobre os instrumentos e os procedimentos disponíveis, bem como prestando orientações sobre a forma de abordar questões regulamentares relativas à partilha de informações, designadamente facilitando a criação de centros de partilha e análise de informações a nível setorial.

(30) Uma vez que aumenta constantemente o potencial impacto negativo das vulnerabilidades dos produtos, serviços e processos de TIC, a deteção e correção dessas vulnerabilidades é importante para reduzir o risco global de cibersegurança. Está demonstrado que a cooperação entre as organizações, os fabricantes de produtos de TIC vulneráveis, os prestadores de serviços de TIC vulneráveis e os fornecedores de processos de TIC vulneráveis e os membros da comunidade de investigação no domínio da cibersegurança, bem como os governos que detetam tais vulnerabilidades contribui significativamente para o aumento das taxas de deteção e de correção das vulnerabilidades em produtos, serviços e processos de TIC. A divulgação coordenada das vulnerabilidades consiste num processo estruturado de cooperação em que as vulnerabilidades são comunicadas ao proprietário do sistema de informação, dando a essa organização a oportunidade de diagnosticar e corrigir as vulnerabilidades antes de serem divulgadas a terceiros ou ao público informações pormenorizadas sobre essas vulnerabilidades. O processo prevê igualmente a coordenação entre a entidade que deteta as vulnerabilidades e a organização, no que diz respeito à publicação dessas vulnerabilidades. A existência de processos de gestão da divulgação coordenada das vulnerabilidades pode desempenhar um papel importante nos esforços dos Estados-Membros para reforçar a cibersegurança.

(31) A ENISA deverá agregar e analisar relatórios nacionais partilhados a título voluntário das CSIRT e da equipa de resposta a emergências informáticas para as instituições, órgãos e organismos da UE, criada pelo Acordo entre o Parlamento Europeu, o Conselho Europeu, o Conselho da União Europeia, a Comissão Europeia, o Tribunal de Justiça da União Europeia, o Banco Central Europeu, o Tribunal de Contas Europeu, o Serviço Europeu para a Ação Externa, o Comité Económico e Social Europeu, o Comité das Regiões Europeu e o Banco Europeu de Investimento sobre a organização e o funcionamento de uma equipa de resposta a emergências informáticas das instituições, órgãos e organismos da União (CERT-UE) ([14]) com o objetivo de contribuir para criar procedimentos, linguagem e terminologia comuns para o intercâmbio de informações. Nesse contexto, a ENISA deverá envolver o setor privado, no âmbito da Diretiva (UE) 2016/1148 que estabelece os fundamentos para o intercâmbio voluntário de informações técnicas a nível operacional no âmbito da rede de equipas de resposta a incidentes de segurança informática («rede de CSIRT») criada pela referida diretiva.

(32) A Agência deverá contribuir para uma resposta a nível da União, em caso de crise e incidentes transfronteiriços em grande escala relacionados com a cibersegurança. Esta atribuição deverá ser exercida de acordo com o mandato da ENISA, nos termos do presente regulamento, e segundo uma abordagem a ser definida pelos Estados-Membros no contexto da Recomendação (UE) 2017/1584 da Comissão ([15]) e das Conclusões do Conselho de 26 de junho de 2018 sobre a resposta coordenada da União a incidentes e crises de cibersegurança de grande escala. Essa atribuição poderá abranger a recolha de informações relevantes e a atividade de facilitação entre a rede de CSIRT, a comunidade técnica e os decisores políticos responsáveis pela gestão de crises. Além disso, a ENISA deverá apoiar a cooperação operacional entre os Estados-Membros, a pedido de um ou mais Estados-Membros, no tratamento de incidentes de uma perspetiva técnica, através da facilitação do intercâmbio de soluções técnicas pertinentes entre Estados-Membros e de contribuições para a comunicação com o público. A ENISA deverá apoiar a cooperação operacional testando modalidades dessa cooperação por meio de exercícios regulares de cibersegurança.

(33) Ao prestar apoio à cooperação operacional, a ENISA deverá recorrer aos conhecimentos especializados de natureza técnica e operacional da CERT-UE mediante uma cooperação estruturada. Essa cooperação estruturada poderá basear-se nos conhecimentos especializados da ENISA. Sempre que pertinente, deverão ser acordadas entre as duas organizações as disposições adequadas para definir o modo de pôr em prática essa cooperação e evitar a duplicação de atividades.

(34) Em consonância com a sua atribuição de prestar apoio à cooperação operacional no âmbito da rede de CSIRT, a ENISA deverá estar apta a prestar apoio aos Estados-Membros, a pedido destes, nomeadamente aconselhando-os sobre a forma de reforçarem as suas capacidades de prevenção, deteção e resposta a incidentes, facilitando o tratamento técnico de incidentes com um impacto significativo ou substancial ou assegurando a análise de ciberameaças e incidentes. A ENISA deverá facilitar o tratamento técnico de incidentes com um impacto significativo ou substancial, em particular, apoiando a partilha voluntária de soluções técnicas entre os Estados-Membros ou produzindo informações técnicas combinadas, designadamente soluções técnicas partilhadas pelos Estados-Membros a título voluntário. A Recomendação (UE) 2017/1584 recomenda que os Estados-Membros cooperem de boa-fé e partilhem entre si e com a ENISA, sem atrasos injustificados, informações sobre incidentes e crises em grande escala relacionados com a cibersegurança. Essas informações deveriam ajudar a ENISA no exercício das suas atribuições de apoio à cooperação operacional.

(35) Como parte da cooperação regular a nível técnico para apoiar o conhecimento da situação na União, a ENISA deverá, em estreita colaboração com os Estados-Membros, elaborar regularmente um relatório aprofundado sobre a situação técnica da cibersegurança na União quanto a incidentes e ciberameaças, baseando-se em informações publicamente disponíveis, nas suas próprias análises e em relatórios com ela partilhados pelas CSIRT dos Estados-Membros ou pelos pontos de contacto únicos nacionais para a segurança das redes e dos sistemas de informação (a seguir designados «ponto de contacto único») previstos na Diretiva (UE) 2016/1148, ambos numa base voluntária, pelo Centro Europeu da Cibercriminalidade (EC3) da Europol, pela CERT-UE e, se pertinente, pelo Centro de Situação e de Informações da UE (INTCEN) do Serviço Europeu para a Ação Externa. O referido relatório deverá ser disponibilizado ao Conselho, à Comissão, ao Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança e à rede de CSIRT.

(36) O apoio prestado pela ENISA, a pedido dos Estados-Membros em causa, em inquéritos técnicos *ex post* a incidentes com impacto significativo ou substancial deverá concentrar-se na prevenção de futuros incidentes. Os Estados-Membros em causa deverão fornecer as informações e a assistência necessárias para que a ENISA possa apoiar eficazmente o inquérito técnico *ex post*.

([14]) JO C 12 de 13.1.2018, p. 1.
([15]) Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

(37) Os Estados-Membros poderão convidar as empresas afetadas pelo incidente a cooperarem mediante o fornecimento das informações e da assistência necessárias à ENISA, sem prejuízo do seu direito de protegerem as informações comercialmente sensíveis e as informações relevantes para a segurança pública.

(38) Para compreender melhor os desafios no domínio da cibersegurança, e com vista a prestar aconselhamento estratégico de longo prazo aos Estados-Membros e às instituições, aos órgãos e organismos da União, a ENISA necessita de analisar os riscos atuais e emergentes para a cibersegurança. Para o efeito, a ENISA deverá, em cooperação com os Estados-Membros e, se pertinente, com institutos de estatística e outros organismos, recolher informações relevantes publicamente disponíveis ou partilhadas a título voluntário, analisar tecnologias emergentes e fornecer avaliações dos tópicos específicos sobre o possível impacto societal, jurídico, económico e regulamentar das inovações tecnológicas sobre a segurança das redes e da informação, nomeadamente sobre a cibersegurança. Além disso, a ENISA deverá apoiar os Estados-Membros e as instituições, órgãos e organismos da União na identificação dos riscos emergentes para a cibersegurança e na prevenção dos incidentes, mediante a análise das ciberameaças, das vulnerabilidades e dos incidentes.

(39) A fim de aumentar a resiliência da União, a ENISA deverá desenvolver conhecimentos especializados no domínio da cibersegurança das infraestruturas, designadamente, em apoio dos setores enumerados no anexo II da Diretiva (UE) 2016/1148 e das infraestruturas que são utilizadas pelos prestadores dos serviços digitais enumerados no anexo III da mesma diretiva, prestando aconselhamento, emitindo orientações e procedendo ao intercâmbio das melhores práticas. Com vista a assegurar um acesso mais fácil a informações mais bem estruturadas sobre os riscos para a cibersegurança e as eventuais soluções, a ENISA deverá desenvolver e manter o «polo de informação» da União, um portal único que preste ao público informações sobre cibersegurança provenientes das instituições, dos órgãos e dos organismos da União e nacionais. Facilitar o acesso a informações mais bem estruturadas sobre os riscos para a cibersegurança e as eventuais soluções também pode ajudar os Estados-Membros a reforçar as suas capacidades e alinhar as suas práticas, aumentando, assim, a sua resiliência geral aos ciberataques.

(40) A ENISA deverá contribuir para a sensibilização do público para os riscos para a cibersegurança, incluindo através de uma campanha de sensibilização a nível da União promovendo a educação, e deverá fornecer orientações destinadas aos cidadãos, às organizações e às empresas sobre as boas práticas para utilizadores individuais. A ENISA deverá também contribuir para promover as melhores práticas e soluções, incluindo a ciber-higiene e a ciberliteracia, a nível dos cidadãos, organizações e empresas, recolhendo e analisando informações publicamente disponíveis relativas a incidentes importantes e coligindo e publicando relatórios e orientações destinados aos cidadãos, às organizações e às empresas, a fim de a melhorar o seu nível geral de preparação e resiliência. A ENISA deverá igualmente procurar prestar aos consumidores informações pertinentes sobre os sistemas de certificação aplicáveis, por exemplo, emitindo orientações e recomendações. Além disso, a ENISA deverá organizar, em conformidade com o Plano de Ação para a Educação Digital criado pela Comunicação da Comissão de 17 de janeiro de 2018, e em cooperação com os Estados-Membros e as instituições, órgãos e organismos da União, ações de sensibilização e campanhas públicas de informação regulares destinadas aos utilizadores finais, a fim de promover comportamentos individuais em linha mais seguros e a literacia digital, de sensibilizar para as potenciais ciberameaças, incluindo atividades criminosas em linha, como os ataques de mistificação da interface (phishing), as redes de computadores infetados (botnets), as fraudes financeiras e bancárias e a falsificação de dados, e de prestar aconselhamento básico, sobre a autenticação multifatores, o patching, a cifragem, a anonimização e a proteção de dados.

(41) A ENISA deverá desempenhar um papel central na rápida sensibilização dos utilizadores finais para a segurança dos dispositivos e para uma utilização segura dos serviços, e deverá promover, a nível da União, a segurança desde a conceção e a privacidade desde a conceção. Na consecução deste objetivo, a ENISA deverá recorrer às melhores práticas e experiências disponíveis, especialmente de instituições académicas e investigadores no domínio da segurança informática.

(42) A fim de apoiar as empresas que operam no setor da cibersegurança, bem como os utilizadores de soluções de cibersegurança, a ENISA deverá desenvolver e manter um «observatório do mercado» mediante a realização de análises regulares e a divulgação das principais tendências no mercado da cibersegurança, tanto do lado da procura como da oferta.

(43) A ENISA deverá contribuir para os esforços da União para cooperar com organizações internacionais, bem como no âmbito de quadros de cooperação internacional relevantes no domínio da cibersegurança. Em particular, a ENISA deverá, quando se justificar, contribuir para a cooperação com organizações como a OCDE, a OSCE e a OTAN. Tal cooperação poderá compreender exercícios conjuntos de cibersegurança e de coordenação da resposta a incidentes. Nesse contexto, haverá que assegurar o pleno respeito dos princípios da inclusividade, da reciprocidade e da autonomia de decisão da União, sem prejuízo do caráter específico da política de segurança e defesa de qualquer dos Estados-Membros.

(44) A fim de assegurar a plena realização dos seus objetivos, a ENISA deverá estabelecer ligações com as autoridades de supervisão e outras autoridades competentes na União, as instituições, os órgãos e os organismos da União, incluindo a CERT-UE, o EC3, a Agência Europeia de Defesa (AED), a Agência do sistema global de navegação por satélite (Agência do GNSS Europeu), o Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE), a Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), o Banco Central Europeu (BCE), a Autoridade Bancária Europeia (EBA), o Comité Europeu para a Proteção de Dados (CEPD), a Agência de Cooperação dos Reguladores da Energia (ACER), a Agência Europeia para a Segurança da Aviação (AESA) e qualquer outro organismo da União que esteja envolvido na cibersegurança. A ENISA deverá ainda estabelecer ligações com autoridades com responsabilidades no domínio da proteção de dados, a fim de partilhar conhecimentos especializados e melhores práticas e deverá prestar aconselhamento sobre os aspetos da cibersegurança suscetíveis de afetarem o trabalho dessas autoridades. Deverão poder participar no grupo consultivo da ENISA representantes das autoridades nacionais e da União encarregadas do controlo da aplicação da lei e da proteção de dados. Ao estabelecer ligações com as autoridades encarregadas do controlo da aplicação da lei sobre os aspetos de segurança das redes e da informação que possam afetar o seu trabalho, a ENISA deverá respeitar os canais de informação existentes e as redes estabelecidas.

(45) Poderão ser estabelecidas parcerias com instituições académicas que desenvolvam iniciativas de investigação nos domínios relevantes, e os contributos das associações de consumidores e de outras organizações deverão dispor de canais adequados e ser tomados em consideração.

(46) A ENISA, ao assegurar o serviço de secretariado da rede de CSIRT, deverá apoiar as CSIRT dos Estados-Membros e a CERT-UE na cooperação operacional no que se refere às atribuições relevantes da rede de CSIRT, referidas na Diretiva (UE) 2016/1148. Além disso, a ENISA deverá promover e apoiar a cooperação entre as CSIRT pertinentes em caso de incidentes, ataques ou perturbações nas redes ou infraestruturas por estas geridas ou protegidas e que impliquem, ou sejam capazes de implicar, pelo menos duas CSIRT, tendo simultaneamente na devida conta os procedimentos operacionais normalizados da rede de CSIRT.

(47) Com vista a elevar o grau de preparação da União na resposta aos incidentes, a ENISA deverá organizar regularmente exercícios de cibersegurança a nível da União e, a seu pedido, apoiar os Estados-Membros e as instituições, os órgãos e os organismos da União na organização de tais exercícios. De dois em dois anos, deverão ser organizados exercícios abrangentes em grande escala, que incluam elementos técnicos, operacionais ou estratégicos. Além disso, a ENISA deverá poder organizar regularmente exercícios menos abrangentes com o mesmo objetivo de aumentar o grau de preparação da União para dar resposta a incidentes.

(48) A ENISA deverá ainda desenvolver e manter os seus conhecimentos especializados em matéria de certificação da cibersegurança, com vista a apoiar a política da União neste domínio. A ENISA deverá basear-se nas melhores práticas existentes e promover a adoção da certificação da cibersegurança na União, nomeadamente contribuindo para a criação e manutenção de um enquadramento para a certificação da cibersegurança a nível da União (a seguir designado «enquadramento europeu para a certificação da cibersegurança») com vista a aumentar a transparência no que respeita à garantia da cibersegurança dos produtos, serviços e processos de TIC e, desta forma, reforçar a confiança e a competitividade no mercado interno digital.

(49) As políticas de cibersegurança eficientes deverão basear-se em métodos bem desenvolvidos de avaliação dos riscos, tanto no setor público quanto no setor privado. Os métodos de avaliação dos riscos são utilizados a diferentes níveis, sem que exista uma prática comum para a sua aplicação eficiente. A promoção e o desenvolvimento de melhores práticas em matéria de avaliação dos riscos e de soluções interoperáveis de gestão de riscos nas organizações dos setores público e privado elevarão o nível de cibersegurança na União. Para esse efeito, a ENISA deverá apoiar a cooperação entre as partes interessadas a nível da União e facilitar os seus esforços no que respeita à criação e à aplicação de normas europeias e internacionais em matéria de gestão dos riscos e de segurança mensurável dos produtos, sistemas, redes e serviços eletrónicos que, juntamente com os suportes lógicos, constituem as redes e os sistemas de informação.

(50) A ENISA deverá encorajar os Estados-Membros, os fabricantes de produtos de TIC, os prestadores de serviços de TIC e os fornecedores de processos de TIC a reforçarem as suas normas gerais de segurança, para que todos os utilizadores da internet possam tomar as medidas necessárias para assegurar a sua própria cibersegurança e deverão receber incentivos para tal. Concretamente, os fabricantes de produtos de TIC, os prestadores de serviços de TIC e os fornecedores de processos de TIC deverão assegurar as atualizações necessárias e recolher, retirar ou reciclar os produtos e os serviços ou processos de TIC que não cumpram as normas de cibersegurança, enquanto os importadores e distribuidores deverão assegurar que os produtos, os serviços e os processos de TIC que colocam no mercado da União cumpram os requisitos aplicáveis e não comportem riscos para os consumidores da União.

(51) Em cooperação com as autoridades competentes, a ENISA deverá poder divulgar informações relativas ao nível de cibersegurança dos produtos, serviços e processos de TIC disponibilizados no mercado interno e emitir alertas que visem os fabricantes de produtos de TIC, os prestadores de serviços de TIC e os fornecedores de processos de TIC e solicitar-lhes que reforcem a segurança dos seus produtos, serviços e processos de TIC, incluindo a cibersegurança.

(52) A ENISA deverá ter plenamente em conta as atividades de investigação, desenvolvimento e avaliação tecnológica em curso, em especial as realizadas pelas diversas iniciativas de investigação da União, a fim de aconselhar as instituições e os órgãos e organismos da União e, se se justificar, os Estados-Membros, a pedido destes, sobre as necessidades e prioridades de investigação no domínio da cibersegurança. A fim de identificar as necessidades e prioridades de investigação, a ENISA deverá igualmente consultar os grupos de utilizadores pertinentes. Mais especificamente, poderá estabelecer-se a cooperação com o Conselho Europeu de Investigação, o Instituto Europeu de Inovação e Tecnologia e o Instituto de Estudos de Segurança da União Europeia.

(53) A ENISA deverá consultar com regularidade os organismos de normalização, em particular os organismos europeus de normalização, nomeadamente aquando da elaboração dos sistemas europeus de certificação da cibersegurança.

(54) As ciberameaças constituem um problema mundial. É necessário reforçar a cooperação internacional a fim de aperfeiçoar as normas de cibersegurança, incluindo a necessidade de contar com a definição de normas comuns de comportamento e a adoção de códigos de conduta, a aplicação de normas internacionais e a partilha de informações, promovendo assim uma colaboração internacional mais célere na resposta aos problemas de segurança das redes e da informação, bem como uma abordagem global comum desses problemas. Para esse efeito, a ENISA deverá apoiar um maior envolvimento e cooperação da União com os países terceiros e com as organizações internacionais fornecendo, quando necessário, os conhecimentos especializados e as análises necessárias às instituições, órgãos e organismos competentes da União.

(55) A ENISA deverá estar apta a responder a pedidos *ad hoc* de aconselhamento e assistência da parte dos Estados-Membros e das instituições, órgãos e organismos da União sobre matérias abrangidas pelo seu mandato.

(56) É sensato e recomendável aplicar certos princípios relativos à governação da ENISA a fim de dar cumprimento à Declaração Comum e à Abordagem Comum acordadas em julho de 2012 pelo Grupo de Trabalho Interinstitucional sobre as agências descentralizadas da União, cujo objetivo consiste em racionalizar as atividades das agências descentralizadas e melhorar o seu desempenho. As recomendações constantes da Declaração Comum e da Abordagem Comum deverão também ser refletidas, conforme adequado, nos programas de trabalho, nas avaliações, na elaboração dos relatórios e nas práticas administrativas da ENISA.

(57) O conselho de administração, composto por representantes dos Estados-Membros e da Comissão, deverá estabelecer a orientação geral das operações da ENISA e garantir que esta exerça as suas atribuições de acordo com o presente regulamento. O conselho de administração deverá ser dotado dos poderes necessários para elaborar o orçamento, verificar a sua execução, aprovar as regras financeiras adequadas, estabelecer procedimentos de trabalho transparentes para o processo decisório da ENISA, aprovar o documento único de programação da ENISA, aprovar o seu próprio regulamento interno, nomear o diretor executivo e decidir da prorrogação ou do termo do mandato deste último.

(58) Para o funcionamento correto e eficaz da ENISA, a Comissão e os Estados-Membros deverão assegurar que as pessoas nomeadas para o conselho de administração tenham as competências profissionais especializadas e a experiência adequadas. A Comissão e os Estados-Membros deverão também procurar limitar a rotação dos seus representantes no conselho de administração, a fim de assegurar a continuidade do trabalho deste órgão.

(59) O bom funcionamento da ENISA exige que o seu diretor executivo seja nomeado com base no mérito e em competências administrativas e de gestão documentadas, bem como na competência e experiência relevantes para a cibersegurança. As funções do diretor executivo deverão ser exercidas com total independência. O diretor executivo deverá preparar uma proposta de programa de trabalho anual da ENISA, após consulta à Comissão, e tomar todas as medidas necessárias para garantir a boa execução do programa de trabalho. O diretor executivo deverá preparar um relatório anual que cubra a execução do programa de trabalho anual da ENISA, a apresentar ao conselho de administração, elaborar um projeto de mapa previsional das receitas e despesas da ENISA e executar o orçamento. Além disso, o diretor executivo deverá ter a possibilidade de criar grupos de trabalho *ad hoc* para questões específicas, designadamente de natureza científica, técnica, legal ou socioeconómica. Em especial no que diz respeito à preparação de um projeto de sistema europeu de certificação da cibersegurança específico (a seguir designado «projeto de sistema»), é considerada necessária a criação de um grupo de trabalho *ad hoc*. O diretor executivo deverá assegurar que os membros dos grupos de trabalho *ad hoc* sejam selecionados segundo os mais elevados padrões de especialização, com o objetivo de assegurar o equilíbrio entre os géneros e uma representação equilibrada, em

função das questões específicas em causa, entre as administrações públicas dos Estados-Membros, as instituições, os órgãos e organismos da União e o setor privado, incluindo empresas, utilizadores e académicos especializados em segurança das redes e da informação.

(60) A comissão executiva deverá contribuir para o funcionamento eficaz do conselho de administração. No âmbito do seu trabalho preparatório relacionado com as decisões do conselho de administração, o conselho executivo deverá examinar pormenorizadamente as informações pertinentes, explorar as opções disponíveis e disponibilizar aconselhamento e soluções para preparar as decisões do conselho de administração.

(61) A ENISA deverá dispor de um grupo consultivo da ENISA, como órgão consultivo, para assegurar o diálogo regular com o setor privado, com as associações de consumidores e com outras partes interessadas. O grupo consultivo da ENISA, criado pelo conselho de administração sob proposta do diretor executivo, deverá concentrar-se em questões pertinentes para as partes interessadas e submetê-las à apreciação da ENISA. Esse grupo consultivo deverá ser consultado particularmente no que diz respeito ao projeto de programa de trabalho anual da ENISA. A composição do grupo consultivo da ENISA e as atribuições que lhe são conferidas deverão assegurar uma representação suficiente das partes interessadas.

(62) Deverá ser criado o grupo das partes interessadas para a certificação da cibersegurança a fim de ajudar a ENISA e a Comissão a facilitarem a consulta das partes interessadas. Esse grupo deverá ser constituído por membros que representem o setor numa proporção equilibrada, tanto do lado da procura como do lado da oferta de produtos e serviços de TIC, incluindo, em especial, as PME, os prestadores de serviços digitais, os organismos de normalização europeus e internacionais, os organismos nacionais de acreditação, as autoridades de supervisão da proteção de dados, e os organismos de avaliação da conformidade, de acordo com disposto no Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho ([16]), e o meio académico, bem como as organizações de consumidores.

(63) A ENISA deverá dispor de regras em matéria de prevenção e gestão de conflitos de interesses. A ENISA deverá igualmente aplicar as disposições relevantes da União sobre o acesso do público a documentos previstas no Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho ([17]). O tratamento de dados pessoais por parte da ENISA deverá estar sujeito ao disposto no Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([18]). A ENISA deverá respeitar as disposições aplicáveis às instituições, órgãos e organismos da União e a legislação nacional relativa ao tratamento de informações, nomeadamente de informações sensíveis não classificadas e de informações classificadas da União Europeia (ICUE).

(64) A fim de assegurar a plena autonomia e independência da ENISA e de lhe permitir exercer atribuições adicionais, incluindo atribuições de emergência imprevistas, a ENISA deverá ser dotada de um orçamento autónomo suficiente cujas receitas provenham essencialmente de uma contribuição da União e de contribuições dos países terceiros que participem nos trabalhos da ENISA. É fundamental dispor de um orçamento adequado para garantir que a ENISA tenha capacidade suficiente para exercer cabalmente as suas crescentes atribuições e atingir os seus objetivos. A maior parte do pessoal da ENISA deverá estar diretamente implicada na execução operacional do mandato da Agência. O Estado-Membro de acolhimento, e qualquer outro Estado-Membro, deverá poder contribuir voluntariamente para as receitas da ENISA. O procedimento orçamental da União deverá permanecer aplicável no que diz respeito a todas as subvenções imputadas ao orçamento geral da União. Além disso, o Tribunal de Contas deverá proceder à auditoria das contas da ENISA, a fim de assegurar a transparência e a responsabilização.

(65) A certificação da cibersegurança desempenha um papel importante no aumento da confiança e segurança dos produtos, serviços e processos de TIC. O mercado único digital e, em especial, a economia dos dados e a IdC, apenas pode prosperar se houver uma confiança pública generalizada em que esses produtos, serviços e processos forneçam um determinado nível de cibersegurança. Os automóveis conectados e automatizados, os dispositivos médicos eletrónicos, os sistemas de controlo da automação industrial ou as redes inteligentes são apenas alguns exemplos de setores nos quais a certificação é já amplamente utilizada ou suscetível de o vir a ser no futuro próximo. Os setores regulados pela Diretiva (UE) 2016/1148 são também setores nos quais a certificação da cibersegurança é crucial.

([16]) Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

([17]) 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).

([18]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais por parte das instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

(66) Na comunicação de 2016 intitulada «Reforçar o sistema de ciber-resiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora», a Comissão salientou a necessidade de se dispor de produtos e soluções de cibersegurança de elevada qualidade, a preços acessíveis e interoperáveis. O fornecimento de produtos, serviços e processos de TIC no mercado único continua a ser geograficamente muito fragmentado. Esta circunstância deve-se ao facto de a indústria da cibersegurança na Europa se ter desenvolvido essencialmente com base na procura pública nacional. Além disso, a falta de soluções interoperáveis (normas técnicas), de práticas e mecanismos de certificação à escala da União são outras das lacunas que afetam o mercado único no domínio da cibersegurança. Esta situação reduz a capacidade concorrencial das empresas europeias a nível nacional, da União e mundial e a escolha de tecnologias de cibersegurança viáveis e utilizáveis a que os cidadãos e as empresas têm acesso. De igual modo, na Comunicação de 2017 sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital — «Um Mercado Único Digital Conectado para todos», a Comissão salientou a necessidade de dispor de produtos e sistemas conectados seguros e indicou que a criação de um enquadramento europeu de segurança das TIC que defina regras sobre o modo de organizar a certificação da segurança das TIC na União poderia preservar a confiança na internet e resolver a atual fragmentação do mercado interno.

(67) Atualmente, a certificação da cibersegurança de produtos, serviços e processos de TIC é utilizada apenas de forma limitada. Quando existe, verifica-se na sua maioria a nível do Estado-Membro ou no âmbito de sistemas impulsionados pela indústria. Neste contexto, um certificado emitido por uma autoridade nacional de certificação da cibersegurança não é, em princípio, reconhecido noutros Estados-Membros. Por conseguinte, as empresas poderão ter de certificar os seus produtos, serviços e processos de TIC nos vários Estados-Membros onde operam, nomeadamente com vista a participar em processo nacionais de adjudicação de contratos, o que representa custos suplementares para as empresas. Acresce que, embora estejam a surgir novos sistemas, parece não existir uma abordagem coerente e holística das questões horizontais de cibersegurança, designadamente no domínio da IdC. Os sistemas existentes apresentam insuficiências e diferenças consideráveis em termos de cobertura de produtos, níveis de garantia, critérios substantivos e utilização efetiva, o que impede a existência de mecanismos de reconhecimento mútuo no interior da União.

(68) Foram já envidados alguns esforços para assegurar o reconhecimento mútuo de certificados na União. Todavia, tais esforços apenas foram parcialmente bem-sucedidos. O exemplo mais importante a este respeito é o acordo de reconhecimento mútuo (ARM) do Grupo de Altos Funcionários para a Segurança dos Sistemas de Informação (SOG-IS). Embora represente o modelo mais importante para cooperação e reconhecimento mútuo no domínio da certificação da segurança, o SOG-IS apenas abrange uma parte dos Estados-Membros. Este facto limitou a eficácia do ARM do SOG-IS do ponto de vista do mercado interno.

(69) Atendendo ao que precede, afigura-se necessário adotar uma abordagem comum e criar um enquadramento europeu para a certificação da cibersegurança que estabeleça os principais requisitos horizontais para os sistemas europeus de certificação da cibersegurança a desenvolver e que permita que os certificados de cibersegurança europeus e as declarações União de conformidade dos produtos, serviços e processos de TIC sejam reconhecidos e utilizados em todos os Estados-Membros. Para tal, é essencial tomar por base os sistemas nacionais e internacionais, bem como sistemas de reconhecimento mútuo, designadamente o SOG-IS, e permitir uma transição harmoniosa dos sistemas existentes para os sistemas aplicáveis ao abrigo do novo enquadramento europeu para a certificação da cibersegurança. O enquadramento europeu para a certificação da cibersegurança deverá ter uma dupla finalidade: em primeiro lugar, deverá ajudar a aumentar a confiança nos produtos, serviços e processos de TIC que tenham sido certificados ao abrigo dos sistemas europeus de certificação da cibersegurança. Em segundo lugar, deverá ajudar a evitar a multiplicação de sistemas nacionais de certificações da cibersegurança que entrem em conflito ou que se sobreponham e, desta forma, reduzir os custos a cargo das empresas que operam no mercado único digital. Os sistemas europeus de certificação da cibersegurança deverão ser não discriminatórios e basear-se em normas europeias ou internacionais, salvo se tais normas forem ineficazes ou desadequadas para satisfazer os objetivos legítimos da União a este respeito.

(70) Deverá ser estabelecido um enquadramento europeu para a certificação da cibersegurança de forma homogénea em todos os Estados-Membros para evitar a procura da certificação mais vantajosa («certification shopping») com base na disparidade dos níveis de exigência existentes entre os diferentes Estados-Membros.

(71) Os sistemas europeus de certificação da cibersegurança deverão assentar no que já existe a nível internacional e nacional e, se necessário, nas especificações técnicas de fóruns e consórcios, colhendo ensinamentos dos atuais pontos fortes e avaliando e corrigindo eventuais pontos fracos.

(72) São necessárias soluções flexíveis em matéria de cibersegurança para que a indústria se antecipe a ciberameaças, pelo que os sistemas de certificação deverão ser concebidos de forma a evitar o risco de ficarem rapidamente desatualizados.

(73) Deverão ser conferidos poderes à Comissão para adotar sistemas europeus de certificação da cibersegurança relativamente a grupos específicos de produtos, serviços e processos de TIC. Esses sistemas deverão ser implementados e supervisionados por autoridades nacionais de certificação da cibersegurança e os certificados emitidos ao abrigo desses sistemas deverão ser válidos e reconhecidos em toda a União. Os sistemas de certificação geridos pela indústria ou outras organizações privadas deverão ser excluídos do âmbito de aplicação do presente regulamento. Contudo, os organismos que giram tais sistemas deverão poder propor à Comissão que os considere como base para a aprovação de sistemas europeus de certificação de cibersegurança.

(74) As disposições do presente regulamento deverão aplicar-se sem prejuízo do direito da União que preveja regras específicas em matéria de certificação de produtos, serviços e processos de TIC. Designadamente, o Regulamento (UE) 2016/679 estabelece disposições para a criação de procedimentos de certificação e de selos e marcas de proteção de dados, para efeitos de comprovação da conformidade com o referido regulamento das operações de tratamento efetuadas pelos responsáveis pelo tratamento e subcontratantes. Tais procedimentos de certificação e selos e marcas de proteção de dados deverão permitir que os titulares dos dados avaliem rapidamente o nível de proteção de dados proporcionado pelos produtos, serviços e processos de TIC em causa. O presente regulamento aplica-se sem prejuízo da certificação das operações de tratamento de dados ao abrigo do Regulamento (UE) 2016/679, nomeadamente quando essas operações estejam integradas em produtos, serviços e processos de TIC.

(75) Os sistemas europeus de certificação da cibersegurança deverão ter por objetivo garantir que os produtos, serviços e processos de TIC certificados ao seu abrigo cumpram os requisitos especificados a fim de proteger a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados, transmitidos ou tratados, ou das funções conexas ou dos serviços oferecidos por esses produtos, processos, serviços ou acessíveis por via deles ao longo do respetivo ciclo de vida. É impossível definir pormenorizadamente no presente regulamento os requisitos de cibersegurança relativos a todos os produtos, serviços e processos de TIC. Os produtos, serviços e processos de TIC e as necessidades de cibersegurança conexas são de tal forma diversos que é muito difícil definir requisitos de cibersegurança globais aplicáveis em todas as circunstâncias. Por conseguinte, é necessário adotar uma noção lata e geral de cibersegurança para efeitos de certificação, que deverá ser complementada por um conjunto de objetivos específicos de cibersegurança que deverão ser tidos em conta durante a conceção dos sistemas europeus de certificação da cibersegurança. As disposições segundo as quais esses objetivos serão alcançados em produtos, serviços e processos de TIC específicos deverão depois ser estabelecidas em pormenor a nível do sistema de certificação individual adotado pela Comissão, nomeadamente mediante referência a normas ou especificações técnicas, se não estiverem disponíveis normas adequadas.

(76) As especificações técnicas a utilizar nos sistemas europeus de certificação da cibersegurança deverão respeitar os princípios estabelecidos no anexo II do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ([19]). Contudo, poderão ser considerados necessários alguns desvios a estes requisitos, em casos devidamente justificados em que essas especificações técnicas devam ser utilizadas num sistema europeu de certificação da cibersegurança correspondente a um nível de garantia «elevado». Deverão ser divulgadas as razões que justificaram tais desvios.

(77) A avaliação da conformidade é um procedimento que se destina a avaliar se foram cumpridos os requisitos especificados para um determinado produto, serviço ou processo de TIC. Esse procedimento é executado por um terceiro independente, que não é o fabricante do produto TIC, o prestador do serviço de TIC nem o fornecedor do processo TIC alvo da avaliação. O certificado europeu de cibersegurança deverá ser emitido na sequência de uma avaliação bem-sucedida de um determinado produto, serviço ou processo de TIC. O certificado europeu de cibersegurança deverá ser considerado a confirmação de que a avaliação foi efetuada corretamente. Consoante o nível de garantia, o sistema europeu de certificação da cibersegurança deverá indicar se o certificado europeu de cibersegurança deve ser emitido por uma entidade pública ou privada. A avaliação e a certificação da conformidade não podem garantir por si sós que os produtos, serviços e processos de TIC certificados sejam ciberseguros. Consistem antes em procedimentos e metodologias técnicas para atestar que os produtos, serviços e processos de TIC foram ensaiados e que cumprem determinados requisitos de cibersegurança estabelecidos por outros meios, por exemplo, em normas técnicas.

(78) A escolha da certificação adequada e dos requisitos de segurança conexos pelos utilizadores dos certificados europeus de cibersegurança deverá basear-se numa análise dos riscos associados com a utilização do produto, serviço ou processo de TIC. Por conseguinte, o nível de garantia deverá ser proporcional ao nível do risco associado à utilização prevista do produto, serviço ou processo de TIC.

([19]) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

(79) Os sistemas europeus de certificação da cibersegurança poderão prever a realização de uma avaliação da conformidade sob a exclusiva responsabilidade do fabricante de produtos de TIC, do prestador de serviços de TIC ou do fornecedor de processos de TIC (a seguir designada «autoavaliação da conformidade»). Nesses casos, deverá bastar que o próprio fabricante dos produtos de TIC, o prestador dos serviços de TIC ou o fornecedor de processos de TIC efetue todos os controlos a fim de garantir que os produtos, serviços ou processos de TIC são conformes com o sistema europeu de certificação de cibersegurança. A autoavaliação da conformidade deverá ser considerada adequado para produtos e serviços de TIC de reduzida complexidade ou processos de TIC que apresentem um risco baixo, tais como uma conceção e um mecanismo de produção simples. Além disso, a autoavaliação da conformidade deverá ser permitida para os produtos, serviços e processos de TIC que correspondam apenas ao nível de garantia «básico».

(80) Os sistemas europeus de certificação da cibersegurança poderão permitir tanto a autoavaliação da conformidade como as certificações dos produtos, serviços e processos de TIC. Nesse caso, o sistema deverá prever meios claros e compreensíveis para os consumidores ou outros utilizadores poderem distinguir entre os produtos, serviços e processos de TIC que são avaliados sob a responsabilidade do fabricante de produtos de TIC, do prestador de serviços de TIC ou do fornecedor de processos de TIC e os produtos, serviços e processos de TIC que são certificados por terceiros.

(81) O fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC que realize uma autoavaliação da conformidade deverá poder emitir e assinar a declaração UE de conformidade no âmbito do procedimento de avaliação da conformidade. A declaração UE de conformidade é o documento que atesta que determinado produto, serviço ou processo de TIC cumpre os requisitos do sistema europeu de certificação da cibersegurança. Ao emitir e assinar a declaração UE de conformidade, o fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC assume a responsabilidade pela conformidade do produto, serviço ou processo de TIC com os requisitos legais do sistema europeu de certificação da cibersegurança. Deverá ser apresentada à autoridade nacional de certificação da cibersegurança e à ENISA uma cópia da declaração UE de conformidade.

(82) O fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC deverá manter à disposição da autoridade nacional de certificação da cibersegurança competente, pelo prazo previsto no sistema europeu de certificação da cibersegurança em causa, a declaração UE de conformidade, a documentação técnica e todas as outras informações relevantes sobre a conformidade dos produtos, serviços ou processos de TIC com um determinado sistema europeu de certificação da cibersegurança. A documentação técnica deverá especificar os requisitos aplicáveis por força do sistema e abranger, na medida em que for relevante para a autoavaliação da conformidade, a conceção, o fabrico e o funcionamento do produto, serviço ou processo de TIC. A documentação técnica deverá ser compilada de modo a permitir avaliar se um produto, um serviço ou um processo de TIC cumpre os requisitos aplicáveis por força desse sistema.

(83) A governação do enquadramento europeu para a certificação da cibersegurança tem em conta a participação dos Estados-Membros, bem como a participação adequada das partes interessadas e determina o papel da Comissão Europeia em todo o processo de planeamento, apresentação de propostas, apresentação de pedidos, elaboração, adoção e revisão de sistemas europeus de certificação da cibersegurança.

(84) A Comissão deverá preparar, com o apoio do grupo europeu para a certificação da cibersegurança (GECC) e o grupo das partes interessadas para a certificação da cibersegurança e após uma consulta aberta e alargada, um programa de trabalho evolutivo da União para os sistemas europeus de certificação da cibersegurança e proceder à sua publicação sob a forma de um instrumento não vinculativo. O programa de trabalho evolutivo da União deverá ser um documento estratégico que permita que a indústria, as autoridades nacionais e os organismos de normalização, em particular, se preparem com antecedência para os futuros sistemas europeus de certificação da cibersegurança. O programa de trabalho evolutivo da União deverá incluir um resumo plurianual dos pedidos de projetos de sistemas que a Comissão tenciona apresentar à ENISA para preparação, com base em motivos específicos. A Comissão deverá ter em conta o programa de trabalho evolutivo da União durante a elaboração do seu próprio plano evolutivo para a normalização das TIC e os pedidos de normalização apresentados aos organismos europeus de normalização. Atendendo à rápida introdução e adoção de novas tecnologias, à emergência de riscos para a cibersegurança anteriormente desconhecidos ou à evolução em termos legislativos e de mercado, a Comissão ou o GECC deverão poder pedir à ENISA que elabore projetos de sistemas que não tenham sido incluídos no programa de trabalho evolutivo da União. Nesses casos, a Comissão e o GECC deverão também avaliar a pertinência de tal pedido, tendo para isso em conta as metas e os objetivos globais do presente regulamento e a necessidade de assegurar a continuidade no que diz respeito ao planeamento e à utilização de recursos por parte da ENISA.

Na sequência de tal pedido, a ENISA deverá elaborar sem demora injustificada projetos de sistemas destinados a produtos, serviços ou projetos de TIC específicos. A Comissão deverá avaliar o impacto positivo e negativo do seu pedido no mercado específico em causa, especialmente o impacto nas PME, na inovação, nos obstáculos à entrada nesse mercado e aos custos a cargo dos utilizadores finais. Deverão ser conferidos poderes à Comissão para adotar, com base no projeto de sistema elaborado pela ENISA, o sistema europeu de certificação da cibersegurança por meio de atos de execução. Tendo em conta a finalidade geral e os objetivos de segurança identificados no presente regulamento, os sistemas europeus de certificação da cibersegurança adotados pela Comissão deverão especificar um conjunto mínimo de elementos relativos ao objeto, ao âmbito de aplicação e ao funcionamento do sistema em causa. Os referidos elementos deverão incluir, entre outras coisas, o âmbito de aplicação e o objeto da certificação da cibersegurança, designadamente as categorias de produtos, serviços e processos de TIC abrangidos, a especificação pormenorizada dos requisitos de cibersegurança, por exemplo mediante referência a normas ou especificações técnicas, os critérios específicos de avaliação e os métodos de avaliação, bem como o nível previsto de garantia («básico», «substancial» ou «elevado») e os níveis de avaliação, quando aplicável. A ENISA deverá poder recusar um pedido do GECC. Essas decisões deverão ser adotadas e devidamente justificadas pelo conselho de administração.

(85) A ENISA deverá manter um sítio Web que disponibilize informações sobre os sistemas europeus de certificação da cibersegurança e para os publicitar, que deverá incluir, nomeadamente, os pedidos de elaboração de um projeto de sistema e as reações recebidas no processo de consulta realizado pela ENISA durante a fase de elaboração. O referido sítio Web deverá igualmente disponibilizar informações sobre os certificados europeus de cibersegurança e as declarações UE de conformidade emitidos nos termos do presente regulamento, incluindo informação sobre a revogação e caducidade de tais certificados e declarações. O sítio Web deverá ainda indicar quais os sistemas nacionais de certificação da cibersegurança que tenham sido substituídos por um sistema europeu de certificação da cibersegurança.

(86) O nível de garantia dado por um sistema europeu de certificação é a base que permite confiar em que um processo, um produto ou serviço de TIC cumpre os requisitos de segurança de um determinado sistema europeu de certificação da cibersegurança. A fim de assegurar a coerência do enquadramento europeu para a certificação da cibersegurança, um sistema europeu de certificação da cibersegurança deverá poder especificar níveis de garantia para os certificados europeus de cibersegurança e para as declarações UE de conformidade emitidas ao abrigo desse sistema. Cada certificado europeu de cibersegurança poderá corresponder a um dos níveis de garantia — «básico», «substancial» ou «elevado» —, ao passo que a declaração UE de conformidade apenas poderá corresponder ao nível de garantia «básico». Os níveis de garantia deverão corresponder ao rigor e à exaustividade da avaliação do produto, serviço ou processo de TIC e deverão caracterizar-se por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos cujo objetivo consista em reduzir o impacto ou prevenir incidentes. Cada nível de garantia deverá ser coerente entre os diferentes domínios setoriais nos quais é aplicada a certificação.

(87) Os sistemas europeus de certificação da cibersegurança poderão especificar vários níveis de avaliação em função do rigor e do alcance da metodologia de avaliação utilizada. Os níveis de avaliação deverão corresponder a um dos níveis de garantia e estar associados a uma combinação adequada de componentes de garantia. Para todos os níveis de garantia, o produto, serviço ou processo de TIC deverá conter um conjunto de funcionalidades de segurança, tal como especificadas pelo sistema, que podem incluir: uma configuração inovadora segura, um código de assinatura, atualizações seguras e técnicas de mitigação e proteção completa de memórias empilhadas ou amontoadas (*stack* ou *heap*). Essas funcionalidades deverão ser elaboradas e mantidas seguindo abordagens de desenvolvimento centradas na segurança e utilizando as ferramentas conexas, para assegurar que sejam incorporados mecanismos eficazes tanto de programas informáticos como de equipamento informático de forma fiável.

(88) Para o nível de garantia «básico», a avaliação deverá ser orientada, no mínimo, pelos seguintes componentes de garantia: a avaliação deverá incluir, pelo menos, uma análise da documentação técnica do produto, serviço ou processo de TIC pelo organismo de avaliação da conformidade. Quando a certificação incluir processos de TIC, o processo utilizado para conceber, desenvolver e manter um produto, serviço ou processo de TIC também deverá ser objeto de exame técnico. Nos casos em que um sistema europeu de certificação da cibersegurança preveja uma autoavaliação da conformidade, deverá ser suficiente que o fabricante de produtos de TIC, o prestador de serviços de TIC e o fornecedor de processos de TIC realize uma autoavaliação da conformidade dos produtos, serviços ou processos de TIC com o sistema de certificação.

(89) Para o nível de garantia «substancial», a avaliação deverá, para além dos requisitos previstos para o nível de garantia «básico», ser orientada, no mínimo, pela verificação da conformidade das funcionalidades de segurança do produto, serviço ou processo de TIC com a respetiva documentação técnica.

(90) Para o nível de garantia «elevado», a avaliação deverá, para além dos requisitos previstos para o nível de garantia «substancial», ser orientada, no mínimo, por um ensaio de eficiência que avalie a resistência das funcionalidades de segurança do produto, serviço ou processo de TIC a ciberataques elaborados, levados a cabo por pessoas com competências e recursos significativos.

(91) O recurso à certificação europeia da cibersegurança e a declarações UE de conformidade deverá ser voluntário, salvo disposição em contrário no direito da União ou dos Estados-Membros adotado nos termos do direito da União. Na falta de legislação harmonizada, os Estados-Membros podem adotar regulamentação técnica nacional, que preveja a certificação obrigatória por força de um sistema europeu de certificação da cibersegurança, nos termos da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho ([20]). Os Estados-Membros podem recorrer também à certificação europeia da cibersegurança no contexto da adjudicação de contratos públicos e da Diretiva 2014/24/UE do Parlamento Europeu e do Conselho ([21]).

(92) Em algumas áreas, poderá vir a ser necessário impor determinados requisitos de cibersegurança e tornar obrigatória a respetiva certificação para certos produtos, serviços ou processos de TIC, a fim de elevar o nível de cibersegurança na União. A Comissão deverá acompanhar regularmente o impacto dos sistemas europeus de certificação da cibersegurança adotados sobre a disponibilidade de produtos, serviços e processos de TIC seguros no mercado interno e deverá avaliar regularmente o nível de utilização dos sistemas de certificação pelos fabricantes de produtos TIC, prestadores de serviços de TIC ou fornecedores de processos de TIC da União. A eficiência dos sistemas europeus de certificação da cibersegurança e a necessidade de tornar obrigatórios determinados sistemas específicos deverão ser apreciadas à luz da legislação da União em matéria de cibersegurança, em especial a Diretiva (UE) 2016/1148, tomando em consideração a segurança das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais.

(93) Os certificados europeus de cibersegurança e as declarações UE de conformidade deverão ajudar os utilizadores finais a fazerem escolhas informadas. Por conseguinte, os produtos, processos e serviços de TIC que tenham sido certificados ou para os quais tenha sido emitido um certificado UE de conformidade deverão ser acompanhados de informações estruturadas adaptadas ao nível técnico esperado dos utilizadores finais a que se destinam. Todas as informações deverão estar disponíveis em linha e, se adequado, em formato físico. O utilizador final deverá ter acesso às informações relativas ao número de referência do sistema de certificação, ao nível de garantia, à descrição dos riscos para a cibersegurança associados ao produto, serviço ou processo de TIC e à autoridade ou ao organismo emissor, ou deverá poder obter uma cópia do certificado europeu de cibersegurança. Além disso, o utilizador final deverá ser informado da política de apoio à cibersegurança do fabricante do produto de TIC, do fornecedor do serviço de TIC ou do fornecedor do processo de TIC, ou seja, durante quanto tempo o utilizador final pode esperar receber atualizações e correções de cibersegurança. Se for o caso, deverão ser disponibilizadas orientações sobre as medidas que o utilizador final pode tomar ou as definições que pode selecionar para manter ou aumentar a cibersegurança do produto ou serviço de TIC, e informações sobre um ponto de contacto único para comunicar e receber apoio em caso de ciberataque (para além da comunicação automática). Essas informações deverão ser regularmente atualizadas e disponibilizadas num sítio Web que forneça informações sobre os sistemas europeus de certificação da cibersegurança.

(94) Com vista à consecução dos objetivos do presente regulamento e para evitar a fragmentação do mercado interno, os sistemas ou procedimentos nacionais de certificação da cibersegurança de produtos, serviços e processos de TIC abrangidos por um sistema europeu de certificação da cibersegurança deverão deixar de se aplicar a partir de uma data fixada pela Comissão através de atos de execução. Além disso, os Estados-Membros não deverão criar novos sistemas nacionais de certificação da cibersegurança de produtos, serviços e processos de TIC já abrangidos por um sistema europeu de certificação da cibersegurança existente. No entanto, os Estados-Membros não deverão ser impedidos de criar ou manter sistemas nacionais de certificação da cibersegurança para efeitos de segurança nacional. Os Estados-Membros deverão informar a Comissão e o GECC da intenção de criar novos sistemas nacionais de certificação da cibersegurança. A Comissão e o GECC deverão avaliar o impacto dos novos sistemas nacionais de certificação da cibersegurança sobre o bom funcionamento do mercado interno, ponderando o interesse estratégico de solicitar, em vez disso, um sistema europeu de certificação da cibersegurança.

(95) Os sistemas europeus de certificação da cibersegurança destinam-se a contribuir para harmonizar as práticas de cibersegurança na União. Esses sistemas devem contribuir para elevar o nível de cibersegurança na União. A conceção de sistemas europeus de certificação de cibersegurança deverá ter em conta e permitir inovações no domínio da cibersegurança.

([20]) Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1).

([21]) Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65).

(96) Os sistemas europeus de certificação da cibersegurança deverão ter em conta os atuais métodos de desenvolvimento de programas e equipamentos informáticos e, em especial, o impacto das frequentes atualizações dos programas informáticos ou do firmware nos certificados europeus da cibersegurança individuais. Os sistemas europeus de certificação da cibersegurança deverão especificar as condições em que uma atualização pode exigir que determinado produto, serviço ou processo de TIC volte a ser certificado ou que o âmbito de um certificado europeu de cibersegurança seja reduzido, tendo em conta os eventuais efeitos negativos da atualização sobre a conformidade desse certificado com os requisitos de segurança.

(97) Quando for adotado um sistema europeu de certificação da cibersegurança, os fabricantes de produtos de TIC, os prestadores de serviços de TIC ou os fornecedores de processos de TIC deverão poder apresentar candidaturas para a certificação dos seus produtos, serviços ou processos de TIC a um organismo de avaliação da conformidade da sua escolha, em qualquer ponto da União. Os organismos de avaliação da conformidade deverão ser acreditados por um organismo de acreditação nacional se cumprirem determinados requisitos estabelecidos no presente regulamento. A acreditação deverá ser emitida por um período máximo de cinco anos e deverá ser renovável nas mesmas condições, desde que o organismo de avaliação da conformidade continue a cumprir os requisitos. Os organismos de acreditação nacionais deverão restringir, suspender ou revogar a acreditação de um organismo de avaliação da conformidade se as condições para a acreditação não forem cumpridas ou deixarem de ser cumpridas, ou se o organismo de avaliação da conformidade tomar medidas que constituam infração ao presente regulamento.

(98) As referências da legislação nacional para normas nacionais que tenham deixado de ser aplicáveis em virtude da entrada em vigor de um sistema europeu de certificação da cibersegurança, podem constituir uma fonte de confusão. Por conseguinte, os Estados-Membros deverão refletir na sua legislação nacional a adoção de um sistema europeu de certificação da cibersegurança.

(99) A fim de assegurar a equivalência das normas em toda a União, facilitar o reconhecimento mútuo e promover a aceitação global dos certificados europeus de cibersegurança e das declarações UE de conformidade, é necessário pôr em prática um sistema de análise pelos pares entre as autoridades nacionais de certificação da cibersegurança. A análise pelos pares deverá abranger os procedimentos destinados a supervisionar a conformidade dos produtos, serviços e processos de TIC com os certificados europeus de cibersegurança, a controlar o cumprimento das obrigações dos fabricantes de produtos TIC, dos prestadores de serviços de TIC ou dos fornecedores de processos de TIC ou que procedam à autoavaliação da conformidade e a fiscalizar os organismos de avaliação de conformidade, bem como a adequação das competências técnicas do pessoal dos organismos emissores de certificados para o nível «elevado» de garantia. A Comissão deverá, através de atos de execução, estabelecer pelo menos um plano quinquenal para as análises pelos pares e definir os critérios e as metodologias para o funcionamento do sistema de análise pelos pares.

(100) Sem prejuízo do sistema geral de análise pelos pares a pôr em prática entre todas as autoridades nacionais de certificação da cibersegurança de acordo com o enquadramento europeu para a certificação da cibersegurança, determinados sistemas europeus de certificação da cibersegurança poderão compreender um sistema de avaliação pelos pares aplicável aos organismos emissores dos certificados europeus de cibersegurança para produtos, serviços e processos de TIC com o nível de garantia «elevado» ao abrigo de tais sistemas. O GECS deverá apoiar a aplicação desse tipo de sistemas de avaliação pelos pares. As avaliações pelos pares deverão, em especial, verificar se os organismos em causa desempenham as suas funções de forma harmonizada, podendo prever mecanismos de recurso. Os resultados das avaliações pelos pares deverão ser disponibilizados ao público. Os organismos em causa poderão adotar medidas adequadas para adaptar as suas práticas e os seus conhecimentos especializados de acordo com os resultados.

(101) Os Estados-Membros deverão designar uma ou mais autoridades nacionais de certificação da cibersegurança para supervisionar o cumprimento das obrigações decorrentes do presente regulamento. Uma autoridade nacional de certificação de cibersegurança pode ser uma autoridade já existente ou uma autoridade nova. Os Estados-Membros deverão também poder, em acordo com outro Estado-Membro, designar uma ou mais autoridades nacionais de certificação da cibersegurança no território desse outro Estado-Membro.

(102) As autoridades nacionais de certificação da cibersegurança deverão, nomeadamente, controlar e fazer cumprir as obrigações dos fabricantes de produtos de TIC, dos fornecedores de serviços de TIC ou dos fornecedores de processos de TIC estabelecidos no respetivo território no que respeita à declaração UE de conformidade, deverão prestar assistência aos organismos nacionais de acreditação no controlo e na supervisão das atividades dos organismos de avaliação da conformidade, disponibilizando-lhes conhecimentos especializados e as informações pertinentes, autorizar os organismos de avaliação da conformidade a exercer as suas atribuições quando cumpram os requisitos adicionais estabelecidos no sistema europeu de certificação de cibersegurança, e deverão acompanhar as evoluções pertinentes no domínio da certificação da cibersegurança. As autoridades nacionais de certificação da cibersegurança deverão também tratar as reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados europeus de cibersegurança por elas emitidos ou a certificados emitidos por organismos de avaliação da conformidade que indiquem um nível de garantia «elevado», investigar, na medida do necessário, o

objeto das reclamações e informar os respetivos autores do andamento e do resultado da investigação num prazo razoável. Além disso, deverão cooperar com outras autoridades nacionais de certificação da cibersegurança ou outras autoridades públicas, nomeadamente através da partilha de informações sobre a eventual não conformidade de produtos, serviços e processos de TIC com os requisitos do presente regulamento ou com sistemas europeus específicos de certificação da cibersegurança. A Comissão deverá facilitar a partilha de informações através da disponibilização de um sistema geral de apoio às informações eletrónicas, por exemplo o Sistema de Fiscalização do Mercado e de Intercâmbio de Informações (ICSMS) e o sistema de alerta rápido para produtos de consumo não alimentares (RAPEX), já utilizados pelas autoridades de fiscalização do mercado de acordo com o Regulamento (CE) n.º 765/2008.

(103) Com vista a assegurar a aplicação consistente do enquadramento europeu para a certificação da cibersegurança, deverá ser criado um GECC composto por representantes das autoridades nacionais de certificação da cibersegurança ou outras autoridades nacionais competentes. As principais atribuições do GECC deverão ser: aconselhar e assistir a Comissão no seu trabalho destinado a assegurar uma execução e uma aplicação coerentes do enquadramento europeu para a certificação da cibersegurança; assistir e cooperar estreitamente com a ENISA na preparação de projetos de sistemas de certificação da cibersegurança; em casos devidamente justificados, solicitar à ENISA que elabore um projeto de sistema europeu de certificação da cibersegurança; adotar pareceres à atenção da ENISA a respeito dos projetos de sistemas e adotar pareceres à atenção da Comissão a respeito da manutenção e revisão dos sistemas europeus de certificação da cibersegurança existentes. O GECC deverá facilitar o intercâmbio de boas práticas e dos conhecimentos especializados entre as diversas autoridades nacionais de certificação da cibersegurança responsáveis pela autorização dos organismos de avaliação da conformidade e pela emissão de certificados europeus de cibersegurança.

(104) A fim de sensibilizar para os futuros sistemas de certificação da cibersegurança da União e de facilitar a sua aceitação, a Comissão pode emitir orientações gerais ou setoriais sobre cibersegurança, abordando, por exemplo, as boas práticas de cibersegurança ou o comportamento responsável em matéria de cibersegurança, salientando o efeito positivo da utilização de produtos, serviços e processos de TIC certificados.

(105) A fim de facilitar mais o comércio, e reconhecendo que as cadeias de abastecimento de TIC são mundiais, podem ser celebrados pela União, nos termos do artigo 218.º do Tratado sobre o Funcionamento da União Europeia (TFUE), acordos de reconhecimento mútuo relativos aos certificados europeus de cibersegurança. A Comissão, tendo em conta o aconselhamento prestado pela ENISA e pelo GECC, pode recomendar a abertura de negociações nesse sentido. Cada sistema europeu de certificação da cibersegurança deverá prever condições específicas para esses acordos de reconhecimento mútuo com os países terceiros.

(106) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão. Tais competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([22]).

(107) O procedimento de exame deverá ser seguido para a adoção de atos de execução relativos aos sistemas europeus de certificação da cibersegurança de produtos, serviços e processos de TIC, às disposições relativas à realização de inquéritos por parte da ENISA, a um plano para a análise pelos pares das autoridades nacionais de certificação da cibersegurança, e às circunstâncias, formatos e procedimentos de notificação dos organismos de avaliação da conformidade acreditados pelas autoridades nacionais de certificação da cibersegurança à Comissão.

(108) As atividades da ENISA deverão ser submetidas a uma avaliação regular e independente. Essa avaliação deverá incidir sobre os objetivos por parte da ENISA, os seus métodos de trabalho e a relevância das suas atribuições, em especial, as relacionadas com a cooperação operacional a nível da União. Essa avaliação deverá também incidir sobre o impacto, a eficácia e a eficiência do enquadramento europeu para a certificação da cibersegurança. Em caso de revisão, a Comissão deverá verificar de que modo será possível reforçar o papel da ENISA enquanto ponto de referência em matéria de aconselhamento e de conhecimentos especializados e a possibilidade de a ENISA desempenhar um papel de apoio na avaliação dos produtos, serviços e processos de TIC de países terceiros que entrem no território da União e não cumpram as regras da União.

([22]) Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

(109) Atendendo a que os objetivos do presente regulamento não podem ser suficientemente alcançados pelos Estados-Membros, mas podem, devido à sua dimensão e aos seus efeitos, ser mais bem alcançados a nível da União, a União pode adotar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia (TUE). Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esses objetivos.

(110) O Regulamento (UE) n.º 526/2013 deverá ser revogado,

ADOTARAM O PRESENTE REGULAMENTO:

TÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. Com vista a assegurar o bom funcionamento do mercado interno e, simultaneamente, a alcançar um nível elevado de cibersegurança, de ciber-resiliência e de confiança no seio da União, o presente regulamento estabelece:

a) Os objetivos, as atribuições e os aspetos organizativos da ENISA («Agência da União Europeia para a Cibersegurança»); e

b) Um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de TIC na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União.

O enquadramento referido na alínea b) do primeiro parágrafo, é aplicável sem prejuízo de disposições específicas constantes de outros atos jurídicos da União em matéria de certificação de caráter voluntário ou obrigatório.

2. O presente regulamento não prejudica as competências dos Estados-Membros no que toca às suas atividades em matéria de segurança pública, de defesa e de segurança nacional, nem as atividades do Estado no domínio do direito penal.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Cibersegurança», todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas;

2) «Rede e sistema de informação», uma rede e um sistema de informação na aceção do artigo 4.º, ponto 1, da Diretiva (UE) 2016/1148;

3) «Estratégia nacional de segurança das redes e dos sistemas de informação», uma estratégia nacional de segurança das redes e dos sistemas de informação, na aceção do artigo 4.º, ponto 3, da Diretiva (UE) 2016/1148;

4) «Operador de serviços essenciais», um operador de serviços essenciais, na aceção do artigo 4.º, ponto 4, da Diretiva (UE) 2016/1148;

5) «Prestador de serviços digitais», um prestador de serviços digitais na aceção do artigo 4.º, ponto 6, da Diretiva (UE) 2016/1148;

6) «Incidente», um incidente na aceção do artigo 4.º, ponto 7, da Diretiva (UE) 2016/1148;

7) «Tratamento de incidentes», o tratamento de incidentes na aceção do artigo 4.º, ponto 8, da Diretiva (UE) 2016/1148;

8) «Ciberameaça», uma circunstância, um evento ou uma ação potenciais suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas;

9) «Sistema europeu de certificação da cibersegurança», o conjunto abrangente, de regras, requisitos técnicos, normas e procedimentos estabelecidos a nível da União e aplicáveis à certificação ou à avaliação da conformidade dos produtos, serviços e processos de TIC;

10) «Sistema nacional de certificação da cibersegurança», o conjunto abrangente de regras, requisitos técnicos, normas e procedimentos estabelecidos e adotados por uma autoridade pública nacional e aplicáveis à certificação ou à avaliação da conformidade de produtos, serviços e processos de TIC abrangidos pelo âmbito de aplicação desse sistema específico;

11) «Certificado europeu de cibersegurança», um documento emitido por um organismo competente, que ateste que determinado produto, serviço ou processo de TIC foi avaliado para determinar a sua conformidade com os requisitos de segurança específicos estabelecidos por um sistema europeu de certificação da cibersegurança;

12) «Produto de TIC», um elemento ou grupo de elementos de uma rede ou um sistema de informação;

13) «Serviço de TIC», um serviço que consiste total ou principalmente na transmissão, no armazenamento, na extração ou no tratamento de informações através de redes e sistemas de informação;

14) «Processo de TIC», um conjunto de atividades realizadas com o objetivo de conceber, desenvolver, fornecer ou manter um produto ou serviço de TIC;

15) «Acreditação», a acreditação na aceção do artigo 2.º, ponto 10, do Regulamento (CE) n.º 765/2008;

16) «Organismo nacional de acreditação», um organismo nacional de acreditação na aceção do artigo 2.º, ponto 11, do Regulamento (CE) n.º 765/2008;

17) «Avaliação da conformidade», uma avaliação da conformidade na aceção do artigo 2.º, ponto 12, do Regulamento (CE) n.º 765/2008;

18) «Organismo de avaliação da conformidade», um organismo de avaliação da conformidade na aceção do artigo 2.º, ponto 13, do Regulamento (CE) n.º 765/2008;

19) «Norma», uma norma na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012;

20) «Especificação técnica», um documento que define os requisitos técnicos a cumprir pelos produtos, serviços ou processos de TIC, ou os procedimentos de avaliação da conformidade relativos aos produtos, serviços ou processos de TIC;

21) «Nível de garantia», a base da confiança de que um produto, serviço ou processo de TIC cumpre os requisitos de segurança de um determinado sistema europeu de certificação da cibersegurança, que indica a que nível esse produto, serviço ou processo de TIC foi avaliado, mas não mede, por si só, a segurança dos produtos, serviços ou processos de TIC em si mesmos;

22) «Autoavaliação da conformidade», uma ação realizada por um fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC para avaliar se esses produtos, serviços ou processos de TIC cumprem os requisitos de um sistema europeu de certificação da cibersegurança.

TÍTULO II

ENISA (AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA)

CAPÍTULO I

Mandato e objetivos

Artigo 3.º

Mandato

1. A ENISA exerce as atribuições que lhe são conferidas ao abrigo do presente regulamento com o objetivo de alcançar um elevado nível comum de cibersegurança na União, nomeadamente apoiando ativamente os Estados-Membros e as instituições, órgãos e organismos da União a reforçarem a cibersegurança. A ENISA atua como um ponto de referência em matéria de aconselhamento e de conhecimentos especializados sobre cibersegurança para as instituições, órgãos e organismos da União, assim como para outras partes interessadas da União.

A ENISA contribui para reduzir a fragmentação do mercado interno ao exercer as atribuições que lhe são conferidas ao abrigo do presente regulamento.

2. A ENISA exerce as atribuições que lhe sejam conferidas por atos jurídicos da União que definam medidas para aproximar as disposições legislativas, regulamentares e administrativas dos Estados-Membros relacionadas com a cibersegurança.

3. No exercício das suas atribuições, a ENISA atua com independência, evitando a duplicação das atividades dos Estados-Membros e tendo em conta os conhecimentos especializados dos Estados-Membros.

4. A ENISA desenvolve os seus próprios recursos, incluindo as capacidades e competências a nível técnico e humano, necessários para o exercício das atribuições que lhe são conferidas pelo presente regulamento.

Artigo 4.º

Objetivos

1. A ENISA é um centro de conhecimentos especializados em matéria de cibersegurança, graças à sua independência, à qualidade científica e técnica do aconselhamento e da assistência que presta, às informações que divulga, à transparência dos seus procedimentos operacionais, aos seus métodos de funcionamento e à sua diligência no exercício das suas atribuições.

2. A ENISA presta assistência às instituições, órgãos e organismos da União, bem como aos Estados-Membros, na elaboração e execução de políticas da União relacionadas com a cibersegurança, incluindo políticas setoriais em matéria de cibersegurança.

3. A ENISA apoia o reforço das capacidades e do grau de preparação em toda a União, prestando assistência às instituições, órgãos e organismos da União, bem como aos Estados-Membros e às partes interessadas públicas e privadas para reforçar a proteção das suas redes e dos seus sistemas de informação, desenvolver e aumentar a ciber-resiliência e as capacidades de resposta e desenvolver capacidades e competências no domínio da cibersegurança.

4. A ENISA promove a cooperação incluindo a partilha de informações e a coordenação a nível da União entre os Estados-Membros, as instituições, órgãos e organismos da União, e as partes interessadas relevantes dos setores público e privado, nas questões relacionadas com a cibersegurança.

5. A ENISA contribui para aumentar as capacidades em matéria de cibersegurança a nível da União, a fim de apoiar as ações dos Estados-Membros na prevenção e resposta a ciberameaças, em especial em caso de incidentes transfronteiriços.

6. A ENISA promove o recurso a uma certificação europeia da cibersegurança, com vista a evitar a fragmentação do mercado interno. A ENISA contribui para a criação e a manutenção de um enquadramento europeu para a certificação da cibersegurança, nos termos do título III do presente regulamento, a fim de aumentar a transparência no que respeita à cibersegurança dos produtos, serviços e processos de TIC, reforçando, assim, a confiança no mercado interno digital e a sua competitividade.

7. A ENISA promove um elevado nível de sensibilização em matéria de cibersegurança, designadamente a ciber-higiene e a ciberliteracia dos cidadãos, das organizações e das empresas.

CAPÍTULO II

Atribuições

Artigo 5.º

Elaboração e execução da política e do direito da União

A ENISA contribui para a elaboração e a execução da política e do direito da União, nomeadamente:

1) Prestando assistência e aconselhamento no que respeita à elaboração e à revisão da política e do direito da União no domínio da cibersegurança, e às iniciativas legislativas e de políticas setoriais que envolvam questões relacionadas com a cibersegurança nomeadamente fornecendo pareceres e análises independentes e realizando trabalhos preparatórios;

2) Prestando assistência aos Estados-Membros na execução coerente da política e do direito da União em matéria de cibersegurança, nomeadamente no que diz respeito à Diretiva (UE) 2016/1148, nomeadamente através da emissão de pareceres e orientações, da disponibilização de aconselhamento e das melhores práticas sobre questões como a gestão do risco, a comunicação de incidentes e a partilha de informações, bem como da facilitação do intercâmbio das melhores práticas entre as autoridades competentes nesse domínio;

3) Prestando assistência aos Estados-Membros e às instituições, órgãos e organismos da União na elaboração e promoção de políticas de cibersegurança que apoiem a disponibilidade geral ou a integridade do núcleo público da Internet aberta;

4) Contribuindo para os trabalhos do grupo de cooperação, nos termos do artigo 11.º da Diretiva (UE) 2016/1148, fornecendo conhecimentos especializados e assistência;

5) Apoiando:

   a) A elaboração e a execução da política da União no domínio da identificação eletrónica e dos serviços de confiança, nomeadamente prestando aconselhamento e emitindo orientações técnicas, e facilitando o intercâmbio das melhores práticas entre as autoridades competentes;

   b) A promoção de um reforço do nível de segurança das comunicações eletrónicas, nomeadamente disponibilizando aconselhamento e conhecimentos especializados, e facilitando o intercâmbio das melhores práticas entre as autoridades competentes;

   c) Os Estados-Membros na aplicação dos aspetos específicos de cibersegurança das políticas e do direito da União em matéria de proteção de dados e privacidade, incluindo através da emissão, a pedido, de parecer dirigido ao Comité Europeu para a Proteção de Dados;

6) Apoiando a análise regular das atividades políticas da União, elaborando para isso um relatório anual sobre o estado da execução do respetivo regime jurídico, no que diz respeito:

   a) Às informações sobre as notificações de incidentes ocorridos nos Estados-Membros apresentadas pelos pontos únicos de contacto ao grupo de cooperação, nos termos do artigo 10.º, n.º 3, da Diretiva (UE) 2016/1148;

   b) Aos resumos das notificações de violações da segurança ou de perda de integridade recebidas da parte dos prestadores de serviços de confiança que as entidades supervisoras tenham fornecido à ENISA, nos termos do artigo 19.º, n.º 3, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([23]);

   c) Às notificações de incidentes de segurança transmitidas pelos fornecedores de redes de comunicações eletrónicas públicas ou de serviços de comunicações eletrónicas acessíveis ao público que as autoridades competentes tenham fornecido à ENISA, nos termos do artigo 40.º da Diretiva (UE) 2018/1972.

([23]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

Artigo 6.º

Reforço das capacidades

1. A ENISA presta assistência:

a) Aos Estados-Membros, nos seus esforços para melhorar a prevenção, a deteção e a análise de ciberameaças e incidentes, e a capacidade de resposta a tais ciberameaças e incidentes, disponibilizando-lhes conhecimentos especializados;

b) Aos Estados-Membros e às instituições, órgãos e organismos da União, na elaboração e execução das políticas de divulgação de vulnerabilidades numa base voluntária;

c) Às instituições, órgãos e organismos da União, nos seus esforços para melhorar a prevenção, a deteção e a análise de ciberameaças e incidentes, e melhorar as suas capacidades de resposta a tais ciberameaças e incidentes, em particular por meio do apoio adequado à (CERT-UE);

d) Aos Estados-Membros, na criação de equipas nacionais de CSIRT, a pedido, nos termos do artigo 9.º, n.º 5, da Diretiva (UE) 2016/1148;

e) Aos Estados-Membros, na elaboração de estratégias nacionais de segurança das redes e dos sistemas de informação, se a pedido, nos termos do artigo 7.º, n.º 2, da Diretiva (UE) 2016/1148, e promovendo a divulgação dessas estratégias e registando os progressos alcançados na sua execução em toda a União, a fim de promover as melhores práticas;

f) Às instituições da União, na elaboração e análise das estratégias da União em matéria de cibersegurança, promovendo a sua divulgação e acompanhando o avanço da sua execução;

g) Às CSIRT nacionais e da União, na subida do nível das suas capacidades, nomeadamente promovendo o diálogo e o intercâmbio de informações, a fim de assegurar que, tendo em conta o estado da tecnologia, cada CSIRT possua uma base comum de capacidades mínimas e funcione de acordo com as melhores práticas;

h) Aos Estados-Membros, organizando regularmente os exercícios de cibersegurança a nível da União a que se refere o artigo 7.º, n.º 5, pelo menos de dois em dois anos, e emitindo recomendações de orientação política com base no processo de avaliação dos exercícios e dos ensinamentos deles retirados;

i) Aos organismos públicos competentes, disponibilizando formação em matéria de cibersegurança, quando se justificar em cooperação com as partes interessadas;

j) Ao grupo de cooperação, no intercâmbio de boas práticas referentes a riscos e incidentes, em particular no que diz respeito à identificação pelos Estados-Membros dos operadores de serviços essenciais, nos termos do artigo 11.º, n.º 3, alínea l), da Diretiva (UE) 2016/1148, nomeadamente quanto às dependências transfronteiriças.

2. A ENISA apoia a partilha de informações nos diferentes setores e entre eles, em particular nos setores enumerados no anexo II da Diretiva (UE) 2016/1148, através da disponibilização de melhores práticas e orientações sobre os instrumentos disponíveis e os procedimentos, bem como sobre a forma de abordar questões regulamentares relativas à partilha de informações.

Artigo 7.º

Cooperação operacional a nível da União

1. A ENISA apoia a cooperação operacional entre os Estados-Membros, as instituições, os órgãos e os organismos da União e entre as partes interessadas.

2. A ENISA coopera a nível operacional e estabelece sinergias com as instituições, órgãos e organismos da União, incluindo a CERT-UE, com os serviços que se ocupam da cibercriminalidade e as autoridades supervisoras responsáveis pela proteção da privacidade e dos dados pessoais, a fim de dar resposta a questões de interesse comum através, nomeadamente:

a) Do intercâmbio de competências técnicas e de melhores práticas;

b) Da prestação de aconselhamento e da emissão de orientações sobre questões relevantes relacionadas com a cibersegurança;

c) Do estabelecimento de disposições práticas com vista à execução de tarefas específicas, após consulta à Comissão.

3. A ENISA assegura os serviços de secretariado da rede de CSIRT, nos termos do artigo 12.º, n.º 2, da Diretiva (UE) 2016/1148 e, nessa qualidade, apoia ativamente a partilha de informações e a cooperação entre os seus membros.

4. A ENISA apoia os Estados-Membros no que se refere à cooperação operacional no âmbito da rede de CSIRT, nomeadamente:

a) Aconselhando-os sobre a forma de reforçar as suas capacidades de prevenção, deteção e resposta a incidentes e, a pedido de um ou mais Estados-Membros, prestando aconselhamento em relação a ciberameaças específicas;

b) Prestando assistência, a pedido de um ou mais Estados-Membros, na avaliação de incidentes com impacto significativo ou substancial, através da disponibilização dos seus conhecimentos especializados e facilitando o tratamento técnico desses incidentes, em particular, através do apoio à partilha voluntária de informações relevantes e de soluções técnicas entre os Estados-Membros;

c) Analisando vulnerabilidades e incidentes com base em informações publicamente disponíveis ou em informações fornecidas pelos Estados-Membros a título voluntário para esse efeito; e

d) Prestando apoio, a pedido de um ou mais Estados-Membros, à realização de inquéritos técnicos ex post relativos a incidentes com um impacto significativo ou substancial, na aceção da Diretiva (UE) 2016/1148.

No exercício dessas atribuições, a ENISA e a CERT-UE encetam uma cooperação estruturada, a fim de beneficiar de sinergias e evitar a duplicação de atividades.

5. A ENISA organiza regularmente exercícios de cibersegurança a nível da União e apoia, a seu pedido, os Estados-Membros e as instituições, órgãos e organismos da União na organização de exercícios de cibersegurança. Tais exercícios de cibersegurança a nível da União podem incluir elementos técnicos, operacionais ou estratégicos. A ENISA organiza um exercício em grande escala com uma regularidade bienal.

A ENISA contribui também para exercícios setoriais de cibersegurança e ajuda a organizá-los, juntamente com as organizações competentes que também participam nos exercícios de cibersegurança a nível da União.

6. A ENISA, em estreita colaboração com os Estados-Membros, elabora regularmente um relatório aprofundado sobre a situação técnica da cibersegurança na UE quanto a incidentes e ciberameaças, com base em informações publicamente disponíveis, nas suas próprias análises e em relatórios partilhados, nomeadamente pelas CSIRT dos Estados-Membros ou pelos pontos únicos de contacto criados pela Diretiva (UE) 2016/1148 (ambos numa base voluntária), pelo EC3 e pela CERT-UE.

7. A ENISA contribui para a preparação de uma resposta colaborativa, a nível da União e dos Estados-Membros, a incidentes de cibersegurança transfronteiriços em grande escala ou a crises de cibersegurança, essencialmente:

a) Agregando e analisando relatórios provenientes de fontes nacionais, que sejam públicos ou tenham sido partilhados numa base voluntária, com vista a contribuir para estabelecer um conhecimento comum da situação;

b) Assegurando o fluxo eficaz das informações e a existência de mecanismos de escalada das decisões entre a rede de CSIRT e os decisores técnicos e políticos a nível da União;

c) A pedido, facilitando o tratamento técnico de tais incidentes ou crises, em particular através do apoio à partilha voluntária de soluções técnicas entre Estados-Membros;

d) Apoiando as instituições, os órgãos e organismos da União e, a seu pedido, os Estados-Membros na comunicação pública relativa a tais incidentes ou crises;

e) Ensaiando os planos de cooperação destinados a responder a esses incidentes ou crises a nível da União e, a seu pedido, prestando apoio aos Estados-Membros no ensaio desses planos ao nível nacional.

Artigo 8.º

Mercado, certificação da cibersegurança e normalização

1. A ENISA apoia e promove a elaboração e a execução da política da União em matéria de certificação da cibersegurança dos produtos, serviços e processos de TIC, tal como estabelecido no título III do presente regulamento:

a) Acompanhando continuamente a evolução nos domínios relacionados com a normalização e recomendando especificações técnicas adequadas para utilização na criação de sistemas europeus de certificação da cibersegurança, por força do artigo 54.º, n.º 1, alínea c), caso não existam normas estabelecidas;

b) Elaborando projetos de sistemas europeus de certificação da cibersegurança («projetos de sistemas») dos produtos, serviços e processos de TIC, nos termos do artigo 49.º;

c) Avaliando os sistemas europeus de certificação da cibersegurança adotados, nos termos do artigo 49.º, n.º 8;

d) Participando nas análises pelos pares, nos termos do artigo 59.º, n.º 4;

e) Prestando assistência à Comissão para assegurar os serviços de secretariado do GECC, nos termos do artigo 62.º, n.º 5.

2. A ENISA assegura os serviços de secretariado do grupo das partes interessadas para a certificação da cibersegurança, nos termos do artigo 22.º, n.º 4.

3. A ENISA compila e publica orientações e desenvolve boas práticas em matéria de requisitos de cibersegurança dos produtos, serviços e processos de TIC, em cooperação com as autoridades nacionais de certificação da cibersegurança e a indústria, de modo formal, estruturado e transparente.

4. A ENISA contribui para o reforço de capacidades relacionado com os processos de avaliação e certificação através da compilação e emissão de orientações e da prestação de apoio aos Estados-Membros, a pedido destes.

5. A ENISA facilita a elaboração e a adoção de normas europeias e internacionais em matéria de gestão dos riscos e de segurança dos produtos, serviços e processos de TIC.

6. A ENISA elabora, em colaboração com os Estados-Membros e a indústria, recomendações e orientações relativas aos domínios técnicos relacionados com os requisitos de segurança aplicáveis aos operadores de serviços essenciais e aos prestadores de serviços digitais, bem como relativas a normas já existentes, incluindo normas nacionais dos Estados-Membros, nos termos do artigo 19.º, n.º 2, da Diretiva (UE) 2016/1148.

7. A ENISA analisa regularmente as principais tendências do mercado da cibersegurança, tanto na perspetiva da oferta como da procura, e divulga os resultados com vista à promoção do mercado da cibersegurança na União.

Artigo 9.º

Conhecimento e informação

A ENISA:

a) Analisa as tecnologias emergentes e avalia as inovações tecnológicas no domínio da cibersegurança especificamente quanto ao seu impacto esperado no plano societal, jurídico, económico e regulamentar;

b) Realiza análises estratégicas de longo prazo das ciberameaças e dos incidentes de cibersegurança, a fim de identificar tendências emergentes e ajudar a prevenir incidentes;

c) Em cooperação com peritos das autoridades dos Estados-Membros e das partes interessadas, presta aconselhamento e disponibiliza orientações e melhores práticas para a segurança das redes e dos sistemas de informação, em especial para a segurança das infraestruturas de apoio aos setores enumerados no anexo II da Diretiva (UE) 2016/1148 e das infraestruturas utilizadas pelos prestadores de serviços digitais enumerados no anexo III da mesma diretiva;

d) Através de um portal especialmente concebido para o efeito, reúne, organiza e disponibiliza ao público, informações sobre cibersegurança fornecidas pelas instituições, órgãos e organismos da União e, a título voluntário, informações sobre cibersegurança fornecidas pelos Estados-Membros e pelas partes interessadas dos setores público e privado;

e) Recolhe e analisa informações publicamente disponíveis sobre incidentes importantes e elabora relatórios com vista a fornecer orientações aos cidadãos, às organizações e às empresas em toda a União.

Artigo 10.º

Sensibilização e educação

No que respeita à sensibilização e à educação, a ENISA:

a) Sensibiliza o público para os riscos para a cibersegurança e fornece orientações sobre boas práticas dos utilizadores destinadas aos cidadãos, às organizações e às empresas, designadamente no que se refere à ciber-higiene e ciberliteracia;

b) Organiza, em cooperação com os Estados-Membros, as instituições, os órgãos e os organismos da União e a indústria, campanhas de sensibilização regulares, a fim de aumentar a cibersegurança e a sua visibilidade na União e de incentivar um amplo debate público;

c) Presta assistência aos Estados-Membros nos seus esforços de sensibilização para a cibersegurança e de promoção da educação para a cibersegurança;

d) Promove uma coordenação e um intercâmbio mais estreitos das melhores práticas entre os Estados-Membros no que se refere à sensibilização e à educação para a cibersegurança.

Artigo 11.º

Investigação e inovação

No que respeita à investigação e à inovação, a ENISA:

a) Presta aconselhamento às instituições, órgãos e organismos da União e aos Estados-Membros sobre as necessidades e prioridades de investigação no domínio da cibersegurança, a fim de lhes permitir responder eficazmente aos riscos e às ciberameaças atuais e emergentes, nomeadamente no que respeita às tecnologias novas e emergentes da informação e comunicação e a fim de utilizar de forma eficaz as tecnologias de prevenção dos riscos;

b) Participa, se a Comissão lhe conferir os poderes necessários, na fase de execução de programas de financiamento da investigação e inovação ou é ela própria beneficiária desses programas.

c) Contribui para a agenda estratégica de investigação e inovação a nível da União no domínio da cibersegurança.

Artigo 12.º

Cooperação internacional

A ENISA contribui para os esforços de cooperação da União com os países terceiros e organizações internacionais, bem como no âmbito dos quadros de cooperação internacional relevantes, para promover a cooperação internacional em matéria de cibersegurança:

a) Implicando-se, quando se justifique, na qualidade de observadora na organização de exercícios internacionais, analisando os resultados desses exercícios e deles informando o conselho de administração;

b) Facilitando, a pedido da Comissão, o intercâmbio das melhores práticas;

c) Disponibilizando, a pedido desta, conhecimentos especializados à Comissão;

d) Prestando apoio e aconselhamento à Comissão sobre questões relativas a acordos de reconhecimento mútuo de certificados de cibersegurança com países terceiros, em colaboração com o GECC criado nos termos do artigo 62.º.

CAPÍTULO III

Organização da ENISA

Artigo 13.º

Estrutura da ENISA

A estrutura administrativa e de gestão da ENISA é composta por:

a) Um conselho de administração;

b) Uma comissão executiva;

c) Um diretor executivo;

d) Um grupo consultivo da ENISA;

e) Uma rede de agentes de ligação nacionais.

Secção 1

Conselho de administração

Artigo 14.º

Composição do conselho de administração

1. O conselho de administração é composto por um membro nomeado por cada Estado-Membro e dois membros nomeados pela Comissão. Todos os membros têm direito de voto.

2. Cada membro do conselho de administração tem um suplente. O suplente representa o membro na sua ausência.

3. Os membros do conselho de administração e os seus suplentes são nomeados em função dos seus conhecimentos no domínio da cibersegurança, tendo em conta as suas competências de gestão, administrativas e orçamentais relevantes. A Comissão e os Estados-Membros procuram limitar a rotação dos seus representantes no conselho de administração, a fim de assegurar a continuidade dos trabalhos desse órgão. A Comissão e os Estados-Membros procuraram assegurar o equilíbrio de género no conselho de administração.

4. O mandato dos membros efetivos e dos membros suplentes do conselho de administração tem a duração de quatro anos. O mandato é renovável.

Artigo 15.º

Competências do conselho de administração

1. Compete ao conselho de administração:

a) Estabelecer a direção geral das atividades da ENISA e assegurar que esta funcione de acordo com as regras e os princípios estabelecidos no presente regulamento, bem como assegurar a coerência do trabalho da ENISA com as atividades realizadas pelos Estados-Membros e a nível da União;

b) Adotar o projeto de documento único de programação da ENISA a que se refere o artigo 24.º, antes da sua apresentação à Comissão para parecer;

c) Adotar o documento único de programação da ENISA tendo em conta o parecer da Comissão;

d) Supervisionar a execução da programação anual e plurianual prevista no documento único de programação;

e) Adotar o orçamento anual da ENISA e exercer outras competências respeitantes ao orçamento da ENISA, nos termos do capítulo IV;

f) Avaliar e adotar o relatório anual consolidado de atividades da ENISA, incluindo as contas da ENISA e uma descrição do modo como esta cumpriu os seus indicadores de desempenho, enviar esse relatório anual e a respetiva avaliação, até 1 de julho do ano seguinte, ao Parlamento Europeu, ao Conselho, à Comissão e ao Tribunal de Contas e publicar o relatório anual;

g) Adotar as regras financeiras aplicáveis à ENISA, nos termos do artigo 32.º;

h) Adotar uma estratégia de luta contra a fraude proporcional aos riscos, tendo em conta uma análise de custo-benefício das medidas a aplicar;

i) Adotar regras de prevenção e gestão de conflitos de interesses relativamente aos seus membros;

j) Assegurar o seguimento adequado das conclusões e recomendações decorrentes dos inquéritos do Organismo Europeu de Luta Antifraude (OLAF) e dos diversos relatórios de auditoria e avaliações a nível interno ou externo;

k) Adotar o seu regulamento interno, incluindo as regras sobre a adoção de decisões provisórias a respeito da delegação de tarefas específicas, ao abrigo do artigo 19.º, n.º 7;

l) Exercer, em relação ao pessoal da ENISA, os poderes atribuídos pelo Estatuto dos Funcionários da União Europeia («Estatuto dos Funcionários») e pelo Regime Aplicável aos Outros Agentes da União Europeia («Regime aplicável aos Outros Agentes»), estabelecido no Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho ([24]) à entidade competente para proceder a nomeações, e à autoridade investida do poder de celebrar contratos («poderes da autoridade investida do poder de nomeação»), nos termos do n.º 2 do presente artigo;

m) Adotar regras de execução do Estatuto dos Funcionários e do Regime Aplicável aos Outros Agentes da União Europeia, pelo procedimento previsto no artigo 110.º do Estatuto dos Funcionários;

n) Nomear o diretor executivo e, sendo caso disso, prorrogar o seu mandato ou exonerá-lo das suas funções, nos termos do artigo 36.º;

o) Nomear um contabilista, que pode ser o contabilista da Comissão, o qual é totalmente independente no exercício das suas funções;

p) Tomar todas as decisões relativas à criação e, sempre que necessário, à alteração das estruturas internas da ENISA, tendo em consideração as necessidades decorrentes das atividades desta e uma boa gestão orçamental;

q) Autorizar a celebração de acordos de trabalho, nos termos do artigo 7.º;

r) Autorizar a celebração de acordos de cooperação nos termos do artigo 42.º.

2. O conselho de administração adota, nos termos do artigo 110.º do Estatuto dos Funcionários, uma decisão com base no artigo 2.º, n.º 1, do Estatuto dos Funcionários, e no artigo 6.º do Regime Aplicável aos Outros Agentes, pela qual delega no diretor executivo os poderes relevantes da autoridade investida do poder de nomeação e determina as condições em que essa delegação de competências pode ser suspensa. O diretor executivo pode subdelegar esses poderes.

([24]) JO L 56 de 4.3.1968, p. 1.

3. Se circunstâncias excecionais assim o impuserem, o conselho de administração pode adotar uma decisão para suspender temporariamente a delegação de poderes da autoridade investida do poder de nomeação no diretor executivo e os poderes subdelegados por este último, passando a exercê-los ou delegando-os num dos seus membros ou num membro do pessoal, salvo o diretor executivo.

Artigo 16.º

Presidente do conselho de administração

O conselho de administração elege de entre os seus membros, por maioria de dois terços, um presidente e um vice-presidente. O mandato do presidente e do vice-presidente tem uma duração de quatro anos e é renovável uma vez. Todavia, se os seus mandatos de membros do conselho de administração terminarem durante a vigência dos respetivos mandatos de presidente e vice-presidente, estes últimos caducam automaticamente na mesma data. O vice-presidente substitui automaticamente o presidente na sua falta ou impedimento.

Artigo 17.º

Reuniões do conselho de administração

1. O conselho de administração reúne-se por convocação do seu presidente.

2. O conselho de administração reúne-se a título ordinário, pelo menos duas vezes por ano. Além disso, reúne-se a título extraordinário por iniciativa do seu presidente, a pedido da Comissão, ou a pedido de, pelo menos, um terço dos seus membros.

3. O diretor executivo participa nas reuniões do conselho de administração, mas sem direito de voto.

4. Os membros do grupo consultivo da ENISA podem participar nas reuniões do conselho de administração, a convite do presidente, mas sem direito de voto.

5. Os membros do conselho de administração e os seus suplentes podem ser assistidos nas reuniões do conselho de administração por consultores ou peritos, sob reserva do disposto no regulamento interno do conselho de administração.

6. A ENISA assegura os serviços de secretariado do conselho de administração.

Artigo 18.º

Regras de votação do conselho de administração

1. O conselho de administração delibera por maioria dos seus membros.

2. É necessária uma maioria de dois terços dos membros do conselho de administração para a adoção do documento único de programação e do orçamento anual e para a nomeação do diretor executivo, para a prorrogação do seu mandato ou para a sua exoneração.

3. Cada membro do conselho de administração dispõe de um voto. Na falta de um dos membros, o seu suplente pode exercer o direito de voto.

4. O presidente do conselho de administração participa na votação.

5. O diretor executivo não participa na votação.

6. O regulamento interno do conselho de administração estabelece regras de votação mais pormenorizadas, em especial as condições em que os membros podem agir em nome de outros.

Secção 2

Comissão Executiva

Artigo 19.º

Comissão executiva

1. O conselho de administração é assistido por uma comissão executiva.

2. Compete à comissão executiva:

a) Preparar as decisões a adotar pelo conselho de administração;

b) Assegurar, em conjunto com o conselho de administração, o seguimento adequado das conclusões e recomendações decorrentes dos inquéritos do OLAF e dos diversos relatórios de auditoria e avaliações a nível interno e externo;

c) Sem prejuízo das funções do diretor executivo estabelecidas no artigo 20.º, prestar assistência e aconselhamento ao diretor executivo na execução das decisões do conselho de administração em matéria administrativa e orçamental, nos termos do artigo 20.º.

3. A comissão executiva é composta por cinco membros. Os membros da comissão executiva são nomeados de entre os membros do conselho de administração. Um dos membros é o presidente do conselho de administração que pode também presidir à comissão executiva, e outro membro é um dos representantes da Comissão. As nomeações dos membros da comissão executiva devem procurar assegurar o equilíbrio de género na comissão executiva. O diretor executivo participa nas reuniões da comissão executiva, mas sem direito de voto.

4. O mandato dos membros da comissão executiva tem a duração de quatro anos. O mandato é renovável.

5. A comissão executiva reúne-se, pelo menos, uma vez de três em três meses. O presidente da comissão executiva convoca reuniões adicionais a pedido dos seus membros.

6. O conselho de administração estabelece o regulamento interno da comissão executiva.

7. Se necessário, por motivos de urgência, a comissão executiva pode tomar determinadas decisões provisórias em nome do conselho de administração, nomeadamente em matéria de gestão administrativa, incluindo a suspensão da delegação de poderes da autoridade investida do poder de nomeação, e em matéria orçamental. Estas decisões provisórias são comunicadas ao conselho de administração sem demora injustificada. O conselho de administração decide em seguida da aprovação ou rejeição das decisões provisórias, o mais tardar três meses após a tomada da decisão. A comissão executiva não pode tomar decisões em nome do conselho de administração que tenham de ser aprovadas por maioria de dois terços dos membros do conselho de administração.

Secção 3

Diretor Executivo

Artigo 20.º

Funções do diretor executivo

1. A ENISA é gerida pelo seu diretor executivo, que desempenha as suas funções com independência. O diretor executivo responde perante o conselho de administração.

2. O diretor executivo apresenta ao Parlamento Europeu relatórios sobre o desempenho das suas funções, sempre que for convidado a fazê-lo. O Conselho pode convidar o diretor executivo a apresentar relatórios sobre o desempenho das suas funções.

3. Compete ao diretor executivo:

a) Assegurar a gestão corrente da ENISA;

b) Executar as decisões adotadas pelo conselho de administração;

c) Elaborar o projeto de documento único de programação e apresentá-lo ao conselho de administração para aprovação antes da sua apresentação à Comissão;

d) Executar o documento único de programação e apresentar relatórios ao conselho de administração sobre a sua execução;

e) Elaborar o relatório anual consolidado sobre as atividades da ENISA, incluindo a execução do programa de trabalho anual da ENISA, e apresentá-lo ao conselho de administração para avaliação e adoção;

f) Preparar um plano de ação que dê seguimento às conclusões das avaliações retrospetivas e apresentar à Comissão, de dois em dois anos, um relatório sobre os progressos realizados;

g) Elaborar um plano de ação que dê seguimento às conclusões dos relatórios das auditorias internas ou externas, assim como dos inquéritos do OLAF, e apresentar relatórios sobre os progressos realizados, duas vezes por ano, à Comissão, e regularmente ao conselho de administração;

h) Elaborar o projeto das regras financeiras aplicáveis à ENISA referido no artigo 32.º;

i) Elaborar o projeto de mapa previsional de receitas e despesas da ENISA e executar o seu orçamento;

j) Proteger os interesses financeiros da União mediante a aplicação de medidas preventivas contra a fraude, a corrupção e quaisquer outras atividades ilícitas, a realização de controlos efetivos e, caso sejam detetadas irregularidades, a recuperação dos montantes indevidamente pagos e, se se justificar, mediante a aplicação de sanções administrativas e financeiras efetivas, proporcionadas e dissuasivas;

k) Elaborar uma estratégia antifraude para a ENISA e apresentá-la ao conselho de administração para aprovação;

l) Desenvolver e manter o contacto com a comunidade empresarial e com as associações de consumidores, a fim de assegurar um diálogo regular com as partes interessadas;

m) Manter uma troca regular de opiniões e informações com as instituições, os órgãos e os organismos da União no que se refere às suas atividades em matéria de cibersegurança a fim de garantir a coerência na elaboração e na aplicação da política da União;

n) Desempenhar outras funções que lhe sejam conferidas pelo presente regulamento.

4. Se necessário, e no âmbito dos objetivos e das atribuições da ENISA, o diretor executivo pode criar grupos de trabalho *ad hoc* compostos por peritos, nomeadamente peritos das autoridades competentes dos Estados-Membros. O diretor executivo informa antecipadamente o conselho de administração do facto. Os procedimentos relativos, nomeadamente, à composição e ao funcionamento dos grupos de trabalho e à nomeação dos peritos que os compõem pelo diretor executivo são especificados no regulamento interno da ENISA.

5. Se necessário, de modo a assegurar o exercício eficaz e eficiente das atribuições da ENISA e com base numa análise adequada de custo-benefício, o diretor executivo pode decidir criar uma ou mais delegações locais num ou mais Estados-Membros. Antes de decidir criar uma delegação local, o diretor executivo solicita o parecer do Estado-Membro ou Estados-Membros interessados, incluindo o Estado-Membro onde a ENISA tem sede, e obtém o consentimento prévio da Comissão e do conselho de administração. Em caso de desacordo durante o processo de consulta entre o diretor executivo e os Estados-Membros interessados, o assunto é levado ao Conselho para debate. O número agregado de membros do pessoal em todas as delegações locais é o mais reduzido possível e não pode exceder 40 % do total dos membros do pessoal da ENISA situado no Estado-Membro onde esta tem sede. O número de membros do pessoal em cada delegação local não pode exceder 10 % do total dos membros do pessoal da ENISA situado no Estado-Membro onde esta tem sede.

A decisão de criação de uma delegação local especifica o âmbito das atividades a realizar pela delegação local, de modo a evitar custos desnecessários e a duplicação de funções administrativas da ENISA.

Secção 4

Grupo consultivo da ENISA, Grupo das Partes Interessadas para a Certificação da Cibersegurança e Rede dos Agentes Nacionais de Ligação

Artigo 21.º

Grupo consultivo da ENISA

1. O conselho de administração, agindo sob proposta do diretor executivo, cria, com transparência, o grupo consultivo da ENISA, composto por peritos reconhecidos que representam as partes interessadas, nomeadamente a indústria de TIC, os fornecedores de redes ou serviços de comunicações eletrónicas disponibilizados ao público, as PME, os operadores de serviços essenciais, as associações de consumidores, os peritos académicos no domínio da cibersegurança e os representantes das autoridades competentes nacionais notificadas nos termos da Diretiva (UE) 2018/1972, os organismos europeus de normalização, bem como as autoridades supervisoras responsáveis pelo controlo da aplicação da lei e pela proteção dos dados. O conselho de administração tem por objetivo assegurar o equilíbrio adequado entre os géneros e as origens geográficas, bem como o equilíbrio entre os diferentes grupos de partes interessadas.

2. Os procedimentos relativos ao grupo consultivo da ENISA, nomeadamente quanto à sua composição, à proposta do diretor executivo a que se refere o n.º 1, ao número, à nomeação dos seus membros e ao seu funcionamento são especificados no regulamento interno da ENISA e publicados.

3. O grupo consultivo da ENISA é presidido pelo diretor executivo ou por qualquer outra pessoa por este, caso a caso, nomeada.

4. O mandato dos membros do grupo consultivo da ENISA tem a duração de dois anos e meio. Os membros do conselho de administração não podem ser membros do grupo consultivo da ENISA. Podem assistir às reuniões do grupo consultivo da ENISA, e participar nos seus trabalhos, peritos da Comissão e dos Estados-Membros. Podem ser convidados a assistir às reuniões do grupo consultivo da ENISA, e a participar nos seus trabalhos, representantes de outros organismos que o diretor executivo considere relevantes e que não sejam membros do grupo consultivo da ENISA.

5. O grupo consultivo da ENISA presta aconselhamento à ENISA quanto ao exercício das suas atribuições, exceto quanto à aplicação do título III do presente regulamento. Em particular, o grupo presta aconselhamento ao diretor executivo quanto à elaboração da proposta de programa de trabalho anual da ENISA e à comunicação com as partes interessadas sobre as questões ligadas ao programa de trabalho anual.

6. O grupo consultivo da ENISA informa regularmente o conselho de administração das suas atividades.

Artigo 22.º

Grupo das partes interessadas para a certificação da cibersegurança

1. É criado o grupo das partes interessadas para a certificação da cibersegurança.

2. O grupo das partes interessadas para a certificação da cibersegurança é constituído por membros selecionados de entre peritos reconhecidos que representem as partes interessadas. Na sequência de um concurso transparente e aberto, a Comissão seleciona os membros do grupo das partes interessadas para a certificação da cibersegurança com base numa proposta da ENISA, garantindo o equilíbrio entre os diferentes grupos de partes interessadas, bem como entre géneros e origens geográficas.

3. Compete ao grupo das partes interessadas para a certificação da cibersegurança:

a) Aconselhar a Comissão sobre questões estratégicas relacionadas com o enquadramento europeu para a certificação da cibersegurança;

b) Aconselhar a ENISA, a pedido, sobre questões gerais e estratégicas respeitantes às atribuições da ENISA relacionadas com o mercado, a certificação da cibersegurança e a normalização;

c) Assistir a Comissão na elaboração do programa de trabalho evolutivo da União a que se refere o artigo 47.º;

d) Emitir parecer sobre o programa de trabalho evolutivo da União nos termos do artigo 47.º, n.º 4; e

e) Aconselhar, em casos urgentes, a Comissão e o GCEC sobre a necessidade de dispor de sistemas de certificação suplementares não incluídos no programa de trabalho evolutivo, conforme indicado nos artigos 47.º e 48.º.

4. O grupo das partes interessadas para a certificação da cibersegurança é copresidido pela Comissão e pela ENISA e o seu secretariado é assegurado pela ENISA.

Artigo 23.º

Rede de agentes nacionais de ligação

1. O conselho de administração, deliberando sob proposta do diretor executivo, cria uma rede de agentes nacionais de ligação composta por representantes dos Estados-Membros. Cada Estado-Membro nomeia um representante para a rede de agentes nacionais de ligação. As reuniões da rede de agentes nacionais de ligação podem realizar-se em diferentes configurações de peritos.

2. Em particular, a rede de agentes de ligação nacionais facilita o intercâmbio de informações entre a ENISA e os Estados-Membros e apoia a ENISA na divulgação das suas atividades, conclusões e recomendações às partes interessadas em toda a União.

3. Os agentes nacionais de ligação servem de ponto de contacto focal a nível nacional para facilitar a cooperação entre a ENISA e os peritos nacionais no contexto da execução do programa de trabalho anual da ENISA.

4. Os agentes nacionais de ligação, apesar de cooperarem estreitamente com os representantes dos respetivos Estados-Membros no conselho de administração, não podem, por si só, duplicar o trabalho do conselho de administração nem o de outra instância da União.

5. As funções da rede de agentes nacionais de ligação e os procedimentos que lhe são aplicáveis são especificados no regulamento interno da ENISA e tornados públicos.

Secção 5

Funcionamento

Artigo 24.º

Documento único de programação

1. A ENISA exerce as suas atividades de acordo com um documento único de programação que contém a sua programação anual e plurianual e que inclui todas as suas atividades planeadas.

2. Todos os anos, o diretor executivo elabora um projeto de documento único de programação contendo a programação anual e plurianual e o respetivo planeamento de recursos financeiros e humanos, nos termos do artigo 32.º do Regulamento Delegado (UE) n.º 1271/2013 da Comissão ([25]) e tendo em conta as orientações fornecidas pela Comissão.

3. Até 30 de novembro de cada ano, o conselho de administração adota o documento único de programação referido no n.º 1 e transmite-o ao Parlamento Europeu, ao Conselho e à Comissão, até 31 de janeiro do ano seguinte, acompanhado de eventuais versões atualizadas.

4. O documento único de programação torna-se final após a aprovação definitiva do orçamento geral da União, devendo ser adaptado, se necessário.

([25]) Regulamento Delegado (UE) n.º 1271/2013 da Comissão, de 30 de setembro de 2013, que institui o regulamento financeiro quadro dos organismos referidos no artigo 208.º do Regulamento (UE, Euratom) n.º 966/2012 do Parlamento Europeu e do Conselho (JO L 328 de 7.12.2013, p. 42).

5. O programa de trabalho anual prevê objetivos pormenorizados e os resultados esperados, incluindo indicadores de desempenho. Inclui igualmente uma descrição das ações a financiar e uma indicação dos recursos financeiros e humanos afetados a cada ação, em conformidade com os princípios da orçamentação e gestão por atividades. O programa de trabalho anual deve ser coerente com o programa de trabalho plurianual referido no n.º 7. Deve indicar claramente as atribuições que tenham sido acrescentadas, modificadas ou suprimidas em comparação com o exercício financeiro anterior.

6. O conselho de administração altera o programa de trabalho anual adotado sempre que seja cometida à ENISA uma nova atribuição. As alterações substanciais do programa de trabalho anual são adotadas segundo o procedimento aplicado ao programa de trabalho anual inicial. O conselho de administração pode delegar no diretor executivo os poderes para efetuar alterações não substanciais ao programa de trabalho anual.

7. O programa de trabalho plurianual estabelece a programação estratégica global, incluindo os objetivos, os resultados esperados e os indicadores de desempenho. Estabelece igualmente a programação dos recursos, incluindo o orçamento plurianual e o quadro de pessoal.

8. A programação dos recursos é atualizada anualmente. A programação estratégica é atualizada sempre que se justifique, particularmente em função do resultado da avaliação referida no artigo 67.º.

Artigo 25.º

Declaração de interesses

1. Os membros do conselho de administração, o diretor executivo e os agentes destacados pelos Estados-Membros a título temporário fazem uma declaração de compromisso e uma declaração que indique a inexistência ou a existência de interesses diretos ou indiretos que possam ser considerados prejudiciais para a sua independência. As declarações devem ser exatas e completas, apresentadas anualmente por escrito e atualizadas sempre que necessário.

2. Os membros do conselho de administração, o diretor executivo e os peritos externos que participem em grupos de trabalho *ad hoc* declaram de forma exata e completa, o mais tardar no início de cada reunião, os interesses que possam ser considerados prejudiciais para a sua independência em relação aos pontos da ordem do dia, e abstêm-se de participar na discussão e na votação desses pontos.

3. A ENISA estabelece, no seu regulamento interno, as disposições de execução das regras relativas às declarações de interesses referidas nos n.os 1 e 2.

Artigo 26.º

Transparência

1. A ENISA executa as suas atividades com um elevado nível de transparência e nos termos do artigo 28.º.

2. A ENISA assegura que o público e as partes interessadas recebam informações adequadas, objetivas, fiáveis e facilmente acessíveis, nomeadamente no que respeita aos resultados do seu trabalho. A ENISA publica as declarações de interesses feitas nos termos do artigo 25.º.

3. O conselho de administração, deliberando sob proposta do diretor executivo, pode autorizar partes interessadas a participarem, como observadores, em algumas atividades da ENISA.

4. A ENISA estabelece, no seu regulamento interno, as disposições de execução das regras relativas à transparência referidas nos n.os 1 e 2.

Artigo 27.º

Confidencialidade

1. Sem prejuízo do disposto no artigo 28.º, a ENISA não divulga a terceiros informações por si tratadas ou recebidas em relação às quais tenha sido apresentado um pedido fundamentado de tratamento confidencial.

2. Os membros do conselho de administração, o diretor executivo, os membros do grupo consultivo da ENISA, os peritos externos que participam nos grupos de trabalho *ad hoc* e os membros do pessoal da ENISA, incluindo os agentes destacados pelos Estados-Membros a título temporário, estão sujeitos à obrigação de confidencialidade prevista no artigo 339.º do TFUE, mesmo após a cessação das suas funções.

3. A ENISA estabelece, no seu regulamento interno, as disposições de execução das regras relativas à confidencialidade referidas nos n.os 1 e 2.

4. Se necessário para o exercício das atribuições da ENISA, o conselho de administração autoriza a ENISA a tratar informações classificadas. Nesse caso, a ENISA adota, de comum acordo com os serviços da Comissão, regras de segurança que respeitem os princípios de segurança estabelecidos nas Decisões (UE, Euratom) 2015/443 ([26]) e (UE, Euratom) 2015/444 ([27]) da Comissão. Essas regras de segurança devem compreender disposições relativas ao intercâmbio, tratamento e armazenamento de informações classificadas.

Artigo 28.º

Acesso a documentos

1. O Regulamento (CE) n.º 1049/2001 é aplicável aos documentos na posse da ENISA.

2. O conselho de administração adota disposições de execução do Regulamento (CE) n.º 1049/2001 até 28 de dezembro de 2019.

3. As decisões tomadas pela ENISA ao abrigo do artigo 8.º do Regulamento (CE) n.º 1049/2001 podem ser objeto de queixa perante o Provedor de Justiça Europeu, nos termos do artigo 228.º do TFUE, ou ser impugnadas perante o Tribunal de Justiça da União Europeia, nos termos do artigo 263.º do TFUE.

CAPÍTULO IV

Elaboração e estrutura do orçamento da ENISA

Artigo 29.º

Elaboração do orçamento da ENISA

1. O diretor executivo elabora anualmente um projeto de mapa previsional de receitas e despesas da ENISA para o exercício orçamental seguinte e transmite-o ao conselho de administração, acompanhado de um projeto do quadro de pessoal. As receitas e as despesas devem ser equilibradas.

2. O conselho de administração elabora anualmente, com base no projeto de mapa previsional de receitas e despesas, o mapa previsional de receitas e despesas da ENISA para o exercício orçamental seguinte.

3. Até 31 de janeiro de cada ano, o conselho de administração envia o mapa previsional, que faz parte do projeto de documento único de programação, à Comissão e aos países terceiros com os quais a União tenha celebrado acordos nos termos do artigo 42.º, n.º 2.

4. Com base no mapa previsional, a Comissão inscreve no projeto de orçamento geral da União as previsões que considere necessárias no que respeita ao quadro de pessoal e o montante da subvenção a cargo do orçamento geral da União, e apresenta-o ao Parlamento Europeu e ao Conselho, nos termos do artigo 314.º do TFUE.

5. O Parlamento Europeu e o Conselho autorizam as dotações a título da subvenção da União destinada à ENISA.

6. O Parlamento Europeu e o Conselho aprovam o quadro de pessoal da ENISA.

([26]) 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).

([27]) 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).

7. O conselho de administração adota o orçamento da ENISA em conjunto com o documento único de programação. O orçamento da ENISA torna-se final após a aprovação do orçamento geral da União. Se necessário, o conselho de administração adapta o orçamento e o documento único de programação da ENISA em função do orçamento geral da União.

Artigo 30.º

Estrutura do orçamento da ENISA

1. Sem prejuízo de outros recursos, as receitas da ENISA compreendem:

a) Uma subvenção proveniente do orçamento geral da União;

b) Receitas afetadas ao financiamento de despesas específicas, nos termos das regras financeiras referidas no artigo 32.º;

c) Financiamento da União sob a forma de acordos de contribuição ou subvenções *ad hoc*, nos termos das regras financeiras referidas no artigo 32.º e das disposições dos instrumentos relevantes de apoio às políticas da União;

d) Contribuições de países terceiros que participem nos trabalhos da ENISA, como referido no artigo 42.º;

e) Eventuais contribuições voluntárias dos Estados-Membros, em numerário ou em espécie.

Os Estados-Membros que efetuem contribuições voluntárias nos termos do primeiro parágrafo, alínea e), não podem reivindicar quaisquer direitos ou serviços específicos em contrapartida dessas contribuições.

2. As despesas da ENISA incluem a remuneração do pessoal, o apoio administrativo e técnico, as despesas de infraestrutura e de funcionamento e as despesas decorrentes de contratos celebrados com terceiros.

Artigo 31.º

Execução do orçamento da ENISA

1. O diretor executivo é responsável pela execução do orçamento da ENISA.

2. O auditor interno da Comissão exerce, em relação à ENISA, os mesmos poderes que exerce em relação aos serviços da Comissão.

3. O contabilista da ENISA comunica as contas provisórias relativas ao exercício financeiro (ano N) ao contabilista da Comissão e ao Tribunal de Contas até 1 de março do exercício financeiro seguinte (1 de março do ano N+1).

4. Depois de receber as observações do Tribunal de Contas sobre as contas provisórias da ENISA, nos termos do artigo 246.º do Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho ([28]), o contabilista da ENISA elabora as contas definitivas desta sob a sua responsabilidade e submete-as à apreciação do conselho de administração para parecer.

5. O conselho de administração emite parecer sobre as contas definitivas da ENISA.

6. Até 31 de março do ano N+1, o diretor executivo transmite o relatório sobre a gestão orçamental e financeira ao Parlamento Europeu, ao Conselho, à Comissão e ao Tribunal de Contas.

7. Até 1 de julho do ano N+1, o contabilista da ENISA comunica as contas definitivas da ENISA, acompanhadas do parecer do conselho de administração, ao Parlamento Europeu, ao Conselho, ao contabilista da Comissão e ao Tribunal de Contas Europeu.

([28]) Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União, que altera os Regulamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, (UE) n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 e (UE) n.º 283/2014, e a Decisão n.º 541/2014/UE, e revoga o Regulamento (UE, Euratom) n.º 966/2012 (JO L 193 de 30.7.2018, p. 1).

8. Na mesma data da transmissão das contas definitivas da ENISA, o contabilista da ENISA envia igualmente ao Tribunal de Contas uma carta de representação que abrange essas contas definitivas, com cópia para o contabilista da Comissão.

9. Até 15 de novembro do ano N+1, o diretor executivo publica as contas definitivas da ENISA no *Jornal Oficial da União Europeia*.

10. Até 30 de setembro do ano N+1, o diretor executivo envia ao Tribunal de Contas uma resposta às suas observações e envia uma cópia dessa resposta ao conselho de administração e à Comissão.

11. O diretor executivo apresenta ao Parlamento Europeu, a pedido deste, todas as informações necessárias ao bom desenrolar do processo de quitação relativo ao exercício em causa, nos termos do artigo 261.º, n.º 3 do Regulamento (UE, Euratom) 2018/1046.

12. Sob recomendação do Conselho, o Parlamento Europeu, antes de 15 de maio do ano N+2, o Parlamento Europeu dá quitação ao diretor executivo quanto à execução do orçamento para o ano N.

Artigo 32.º

Regras financeiras

O conselho de administração adota as regras financeiras aplicáveis à ENISA, após consulta à Comissão. Estas regras só podem divergir do Regulamento Delegado (UE) n.º 1271/2013 se o funcionamento da ENISA especificamente o exigir e a Comissão o tiver previamente autorizado.

Artigo 33.º

Luta contra a fraude

1. A fim de facilitar a luta contra a fraude, a corrupção e outras atividades ilícitas ao abrigo do Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho ([29]), a ENISA deve, até 28 de dezembro de 2019, aderir ao Acordo Interinstitucional de 25 de maio de 1999 entre o Parlamento Europeu, o Conselho da União Europeia e a Comissão das Comunidades Europeias relativo aos inquéritos internos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF) ([30]). A ENISA deve adotar as disposições adequadas aplicáveis a todo o seu pessoal, utilizando o modelo que figura no anexo desse acordo.

2. O Tribunal de Contas dispõe de poderes para auditar, com base em documentos e em inspeções no local, todos os beneficiários de subvenções, contratantes e subcontratantes que tenham recebido fundos da União por intermédio da ENISA.

3. O OLAF pode realizar inquéritos, incluindo inspeções e verificações no local, de acordo com as disposições e os procedimentos estabelecidos no Regulamento (UE, Euratom) n.º 883/2013 e no Regulamento (Euratom, CE) n.º 2185/96 do Conselho ([31]), a fim de determinar a existência de fraude, corrupção ou outras atividades ilícitas que afetem os interesses financeiros da União no âmbito de uma subvenção ou de um contrato financiado pela ENISA.

4. Sem prejuízo do disposto nos n.os 1, 2 e 3, os acordos de cooperação com países terceiros ou com organizações internacionais, os contratos, as convenções e as decisões de subvenção da ENISA devem conter disposições que confiram expressamente ao Tribunal de Contas e ao OLAF poderes para realizarem essas auditorias e inquéritos, de acordo com as respetivas competências.

([29]) 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).

([30]) JO L 136 de 31.5.1999, p. 15.

([31]) Regulamento (Euratom, CE) n.º 2185/96 do Conselho, de 11 de novembro de 1996, relativo às inspeções e verificações no local efetuadas pela Comissão para proteger os interesses financeiros das Comunidades Europeias contra a fraude e outras irregularidades (JO L 292 de 15.11.1996, p. 2).

CAPÍTULO V

Pessoal

Artigo 34.º

Disposições gerais

O Estatuto dos Funcionários e o Regime Aplicável aos Outros Agentes, bem como as regras adotadas por acordo entre as instituições da União para aplicação do Estatuto dos Funcionários e ao Regime Aplicável aos Outros Agentes, aplicam-se ao pessoal da ENISA.

Artigo 35.º

Privilégios e imunidades

O Protocolo n.º 7 relativo aos Privilégios e Imunidades da União Europeia, anexo ao TUE e ao TFUE, é aplicável à ENISA e ao seu pessoal.

Artigo 36.º

Diretor executivo

1. O diretor executivo é contratado como agente temporário da ENISA, nos termos do artigo 2.º, alínea a), do Regime Aplicável aos Outros Agentes.

2. O diretor executivo é nomeado pelo conselho de administração de entre uma lista de candidatos propostos pela Comissão, na sequência de um processo de seleção aberto e transparente.

3. Para efeitos da celebração do contrato de trabalho com o diretor executivo, a ENISA é representada pelo presidente do conselho de administração.

4. Antes de ser nomeado, o candidato selecionado pelo conselho de administração é convidado a proferir uma declaração perante a comissão competente do Parlamento Europeu e a responder a perguntas dos deputados.

5. O mandato do diretor executivo tem a duração de cinco anos. No termo desse período, a Comissão procede a uma avaliação do trabalho realizado pelo diretor executivo e das futuras atribuições e desafios da ENISA.

6. O conselho de administração adota as suas decisões sobre a nomeação, a prorrogação do mandato ou a exoneração do diretor executivo nos termos do artigo 18.º, n.º 2.

7. O conselho de administração, deliberando sob uma proposta da Comissão que tenha em conta a avaliação referida no n.º 5, pode prorrogar uma vez o mandato do diretor executivo, por um período de cinco anos.

8. O conselho de administração informa o Parlamento Europeu da sua intenção de prorrogar o mandato do diretor executivo. No prazo de três meses antes de tal prorrogação, o diretor executivo profere, se a tal for convidado, uma declaração perante a comissão competente do Parlamento Europeu e responde a perguntas dos deputados.

9. O diretor executivo cujo mandato tenha sido prorrogado não pode participar noutro processo de seleção para o mesmo lugar.

10. O diretor executivo só pode ser exonerado por decisão do conselho de administração, deliberando sob proposta da Comissão.

Artigo 37.º

Peritos nacionais destacados e outro pessoal

1. A ENISA pode recorrer a peritos nacionais destacados ou a outro pessoal não contratado pela ENISA. O Estatuto dos Funcionários e o Regime Aplicável aos Outros Agentes não se aplicam a esse pessoal.

2. O conselho de administração adota uma decisão que estabelece as regras aplicáveis ao destacamento de peritos nacionais para a ENISA.

CAPÍTULO VI

Disposições gerais relativas à ENISA

Artigo 38.º

Estatuto jurídico da ENISA

1. A ENISA é um organismo da União dotado de personalidade jurídica.

2. A ENISA goza, em cada um dos Estados-Membros, da mais ampla capacidade jurídica que o respetivo direito nacional reconhece às pessoas coletivas. Pode, designadamente, adquirir e alienar bens móveis e imóveis e estar em juízo.

3. A ENISA é representada pelo seu diretor executivo.

Artigo 39.º

Responsabilidade da ENISA

1. A responsabilidade contratual da ENISA é regulada pelo direito aplicável ao contrato em causa.

2. O Tribunal de Justiça da União Europeia é competente para se pronunciar por força de cláusula de arbitragem constante dos contratos celebrados pela ENISA.

3. Em matéria de responsabilidade extracontratual, a ENISA procede à reparação dos danos causados por si ou pelo seu pessoal no exercício das suas funções, de acordo com os princípios gerais comuns ao direito dos Estados-Membros.

4. O Tribunal de Justiça da União Europeia é competente em qualquer litígio relativo à reparação dos danos a que se refere o n.º 3.

5. A responsabilidade pessoal do pessoal perante a ENISA é regulada pelas disposições relevantes do regime aplicável ao pessoal da ENISA.

Artigo 40.º

Regime linguístico

1. O Regulamento n.º 1 ([32]) do Conselho é aplicável à ENISA. Os Estados-Membros e os outros organismos por eles designados podem dirigir-se à ENISA e receber resposta na língua oficial das instituições da União da sua escolha.

2. Os serviços de tradução necessários ao funcionamento da ENISA são assegurados pelo Centro de Tradução dos Organismos da União Europeia.

Artigo 41.º

Proteção de dados pessoais

1. O tratamento de dados pessoais pela ENISA está sujeito às disposições do Regulamento (UE) 2018/1725.

2. O conselho de administração adota as disposições de execução a que se refere o artigo 45.º, n.º 3, do Regulamento (UE) 2018/1725. O conselho de administração pode adotar medidas adicionais necessárias para a aplicação do Regulamento (UE) 2018/1725 pela ENISA.

([32]) Regulamento n.º 1 do Conselho que estabelece o regime linguístico da Comunidade Económica Europeia (JO 17 de 6.10.1958, p. 385).

Artigo 42.º

Cooperação com países terceiros e organizações internacionais

1. A ENISA pode, em função do necessário para alcançar os objetivos fixados no presente regulamento, cooperar com as autoridades competentes de países terceiros ou com organizações internacionais ou ambas. Para o efeito, a ENISA pode celebrar acordos de trabalho com essas autoridades de países terceiros e organizações internacionais, sob reserva da aprovação prévia da Comissão. Esses acordos de trabalho não podem criar obrigações jurídicas à União e aos seus Estados-Membros.

2. A ENISA está aberta à participação de países terceiros que tenham celebrado acordos para o efeito com a União. Ao abrigo das disposições relevantes de tais acordos, são celebrados acordos de trabalho que determinem, nomeadamente, a natureza, o âmbito e o modo de participação desses países terceiros nos trabalhos da ENISA, e que incluam disposições relativas à participação nas iniciativas desenvolvidas pela ENISA, às contribuições financeiras e ao pessoal. No que diz respeito às questões de pessoal, esses acordos de trabalho devem, em todo o caso, respeitar o Estatuto dos Funcionários e o Regime Aplicável aos Outros Agentes.

3. O conselho de administração adota uma estratégia para as relações com os países terceiros e as organizações internacionais em matérias nas quais a ENISA é competente. A Comissão assegura que a ENISA exerça as suas atividades no âmbito do seu mandato e do quadro institucional existente mediante a celebração de acordos de trabalho adequados com o diretor executivo da ENISA.

Artigo 43.º

Regras de segurança em matéria de proteção de informações sensíveis não classificadas e de informações classificadas

Após consulta com a Comissão, a ENISA adota regras de segurança que apliquem os princípios de segurança que constam das regras de segurança da Comissão para a proteção das informações sensíveis não classificadas e das ICUE, enunciadas nas Decisões (UE, Euratom) 2015/443 e 2015/444. As regras de segurança da ENISA incluem disposições relativas ao intercâmbio, tratamento e armazenamento dessas informações.

Artigo 44.º

Acordo de sede e condições de funcionamento

1. As disposições necessárias relativas às instalações a disponibilizar à ENISA no Estado-Membro de acolhimento e às estruturas que este deve pôr à sua disposição, bem como as regras específicas aplicáveis no Estado-Membro de acolhimento ao diretor executivo, aos membros do conselho de administração, ao pessoal da ENISA e aos seus familiares, são estabelecidas num acordo de sede entre a ENISA e o Estado-Membro de acolhimento, celebrado após aprovação do conselho de administração.

2. O Estado-Membro de acolhimento da ENISA proporciona as melhores condições possíveis para assegurar o bom funcionamento da ENISA, tendo em conta a acessibilidade da localização, a existência de condições de ensino apropriadas para os filhos dos membros do seu pessoal e o acesso adequado ao mercado de trabalho, à segurança social e a cuidados médicos para os filhos e cônjuges dos membros do pessoal.

Artigo 45.º

Controlo administrativo

As atividades da ENISA são supervisionadas pelo Provedor de Justiça Europeu, nos termos do artigo 228.º do TFUE.

TÍTULO III

ENQUADRAMENTO PARA A CERTIFICAÇÃO DA CIBERSEGURANÇA

Artigo 46.º

Enquadramento europeu para a certificação da cibersegurança

1. É criado o enquadramento europeu para a certificação da cibersegurança a fim de melhorar as condições de funcionamento do mercado interno elevando o nível de cibersegurança na União e permitindo a adoção de uma abordagem harmonizada a nível da União relativamente aos sistemas europeus de certificação da cibersegurança, tendo em vista criar um mercado único digital de produtos, serviços e processos de TIC.

2. O enquadramento europeu para a certificação da cibersegurança prevê um mecanismo destinado a criar sistemas europeus de certificação da cibersegurança e a atestar que os produtos, serviços e processos de TIC que tenham sido avaliados de acordo com esses sistemas cumprem os requisitos de segurança especificados, para efeitos da proteção da disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, ou as funções ou serviços oferecidos por esses produtos, serviços e processos ou acessíveis por seu intermédio ao longo do respetivo ciclo de vida.

Artigo 47.º

Programa de trabalho evolutivo da União para a certificação europeia da cibersegurança

1. A Comissão publica um programa de trabalho evolutivo para a certificação europeia da cibersegurança (a seguir designado «programa de trabalho evolutivo da União») que aponta as prioridades estratégicas dos futuros sistemas europeus de certificação da cibersegurança.

2. O programa de trabalho evolutivo da União compreende, designadamente, uma lista dos produtos, serviços e processos de TIC ou das respetivas categorias, que podem beneficiar da inclusão no âmbito de aplicação de um sistema europeu de certificação da cibersegurança.

3. A inclusão de um determinado produto, serviço ou processo de TIC ou das respetivas categorias no programa de trabalho evolutivo da União deve ser justificada com base num ou mais dos seguintes fundamentos:

a) A disponibilidade e o desenvolvimento de sistemas nacionais de certificação da cibersegurança que abranjam uma categoria específica de produtos, serviços ou processos de TIC, em especial no que toca ao risco de fragmentação;

b) A política ou o direito aplicável na União ou no Estado-Membro;

c) A procura do mercado;

d) A evolução do cenário de ciberameaça;

e) O pedido de elaboração de um projeto de sistema específico pelo GECC.

4. A Comissão tem na devida conta os pareceres sobre o projeto de programa evolutivo da União emitidos pelo GECC e pelo grupo das partes interessadas para a certificação da cibersegurança.

5. O primeiro programa de trabalho evolutivo da União é publicado até 28 de junho de 2020. O programa de trabalho evolutivo da União é atualizado, pelo menos de três em três anos, ou com maior regularidade, se necessário.

Artigo 48.º

Pedido de sistema europeu de certificação da cibersegurança

1. A Comissão pode solicitar à ENISA a elaboração de um projeto de sistema ou a revisão de um sistema europeu de certificação da cibersegurança existente com base no programa de trabalho evolutivo da União.

2. Em casos devidamente justificados, a Comissão ou o GECC podem solicitar à ENISA a elaboração de um projeto de sistema ou a revisão de um sistema europeu de certificação da cibersegurança existente que não esteja incluído no programa de trabalho evolutivo da União. O programa de trabalho evolutivo da União é atualizado em conformidade.

Artigo 49.º

Elaboração, adoção e revisão de um sistema europeu de certificação da cibersegurança

1. Na sequência de um pedido da Comissão nos termos do artigo 48.º, a ENISA elabora um projeto de sistema que cumpra os requisitos estabelecidos nos artigos 51.º, 52.º e 54.º.

2. Na sequência de um pedido do GECC nos termos do artigo 48.º, n.º 2, a ENISA pode elaborar um projeto de sistema que cumpra os requisitos estabelecidos nos artigos 51.º, 52.º e 54.º. Caso a ENISA recuse esse pedido, deve justificar a sua recusa. Todas as decisões de recusa de tais pedidos são tomadas pelo conselho de administração.

3. Durante a elaboração das propostas de sistema, a ENISA consulta todas as partes interessadas através de um processo de consulta formal, aberto, transparente e inclusivo.

4. Para cada proposta de sistema, a ENISA cria um grupo *ad hoc* nos termos do artigo 20.º, n.º 4, a fim de prestar aconselhamento específico e de disponibilizar conhecimentos especializados à ENISA.

5. A ENISA coopera estreitamente com o GECC. O GECC presta à ENISA assistência e aconselhamento especializado no que respeita à elaboração do projeto de sistema e adota um parecer sobre esse projeto de sistema.

6. A ENISA tem na máxima conta o parecer do GECC antes de transmitir à Comissão o projeto de sistema elaborado nos termos dos n.ºs 3, 4 e 5. O parecer do GECC não vincula a ENISA e a sua ausência não a impede de transmitir o projeto de sistema à Comissão.

7. A Comissão, com base no projeto de sistema apresentado pela ENISA, pode adotar atos de execução que estabeleçam um sistema europeu de certificação da cibersegurança de produtos, serviços e processos de TIC que cumpram os requisitos estabelecidos nos artigos 51.º, 52.º e 54.º. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 66.º, n.º 2.

8. Pelo menos de cinco em cinco anos, a ENISA avalia os sistemas europeus de certificação da cibersegurança adotados, tendo em conta as informações que tenha recebido das partes interessadas. Se se julgar necessário, a Comissão, ou o GECC, pode solicitar à ENISA que dê início ao processo de elaboração de um projeto de sistema revisto, nos termos do artigo 48.º e do presente artigo.

Artigo 50.º

Sítio Web dos sistemas europeus de certificação da cibersegurança

1. A ENISA mantém um sítio Web especialmente concebido para disponibilizar informações sobre os sistemas europeus de certificação da cibersegurança, os certificados europeus de cibersegurança e as declarações UE de conformidade, incluindo informações sobre sistemas europeus de certificação da cibersegurança que tenham deixado de ser válidos, declarações UE de conformidade e certificados europeus de cibersegurança que tenham sido retirados e que tenham caducado e sobre o repositório de hiperligações para informações sobre cibersegurança fornecidas nos termos do artigo 55.º, bem como para publicitar esses sistemas, certificados, declarações e informações.

2. Se for o caso, o sítio Web referido no n.º 1 indica igualmente os sistemas nacionais de certificação da cibersegurança que tenham sido substituídos por um sistema europeu de certificação da cibersegurança.

Artigo 51.º

Objetivos de segurança dos sistemas europeus de certificação da cibersegurança

Os sistemas europeus de certificação da cibersegurança são concebidos de modo a alcançar, conforme aplicável, pelo menos os seguintes objetivos de segurança:

a) Proteger os dados armazenados, transmitidos ou sujeitos a qualquer outro tipo de tratamento contra o armazenamento, tratamento, acesso ou divulgação acidental ou não autorizado ao longo de todo o ciclo de vida do produto, serviço ou processo de TIC;

b) Proteger os dados armazenados, transmitidos ou sujeitos a qualquer outro tipo de tratamento contra a destruição, perda ou alteração acidental ou não autorizada ou a não disponibilização ao longo de todo o ciclo de vida do produto, serviço ou processo de TIC;

c) Garantir que as pessoas, os programas ou as máquinas autorizadas só possam aceder aos dados, serviços ou funções abrangidos pelos seus direitos de acesso;

d) Identificar e documentar as dependências e vulnerabilidades conhecidas;

e) Registar que dados, serviços ou funções foram consultados, utilizados ou sujeitos a qualquer outro tipo de tratamento, quando e por quem;

f) Garantir que seja possível verificar que dados, serviços ou funções foram consultados, utilizados ou sujeitos a qualquer outro tipo de tratamento, quando e por quem;

g) Verificar a ausência de vulnerabilidades conhecidas em produtos, serviços e processos de TIC;

h) Restabelecer a disponibilidade e o acesso aos dados, serviços e funções em tempo útil, no caso de um incidente físico ou técnico;

i) Garantir a segurança dos produtos, serviços e processos de TIC por defeito e desde a conceção;

j) Garantir que os produtos, serviços e processos de TIC sejam fornecidos ou prestados com programas e equipamentos informáticos atualizados que não contenham vulnerabilidades de conhecimento público, e que sejam dotados de mecanismos que permitam atualizações seguras.

Artigo 52.º

Níveis de garantia dos sistemas europeus de certificação da cibersegurança

1. Os sistemas europeus de certificação da cibersegurança podem especificar um ou mais dos seguintes níveis de garantia de produtos, serviços e processos de TIC: «básico», «substancial» ou «elevado». O nível de garantia é proporcional ao nível do risco associado à utilização prevista do produto, serviço ou processo de TIC, em termos de probabilidade e impacto de ocorrência de um incidente.

2. O certificado europeu de cibersegurança e a declaração UE de conformidade indicam o nível de garantia especificado no sistema europeu de certificação da cibersegurança ao abrigo do qual é emitido o certificado europeu de cibersegurança ou a declaração UE de conformidade.

3. Os requisitos de segurança que correspondem a cada nível de garantia são fornecidos no sistema europeu de certificação da segurança relevante, incluindo as funcionalidades de segurança e o rigor e a exaustividade correspondentes da avaliação a que deve ser sujeito o produto, serviço ou processo de TIC.

4. O certificado ou a declaração UE de conformidade faz referência a especificações técnicas, normas e procedimentos conexos, incluindo controlos técnicos, cuja finalidade é reduzir ou prevenir o risco de incidentes de cibersegurança.

5. Um certificado europeu de cibersegurança ou uma declaração UE de conformidade que ateste um nível de garantia «básico» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado ou dessa declaração UE de conformidade cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos básicos conhecidos de incidentes e ciberataques. As atividades de avaliação a realizar compreendem, pelo menos, uma análise da documentação técnica. Caso tal análise não seja adequada, são realizadas atividades de avaliação alternativas de efeito equivalente.

6. Um certificado europeu de cibersegurança que ateste um nível de garantia «substancial» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos conhecidos para a cibersegurança e do risco de incidentes e ciberataques levados a cabo por autores com competências e recursos limitados. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias. Caso tais atividades de avaliação não sejam adequadas, são realizadas atividades de avaliação alternativas de efeito equivalente.

7. Um certificado europeu de cibersegurança que ateste um nível de garantia «elevado» dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos de ciberataques sofisticados levados a cabo por autores com competências e recursos significativos. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias, ao nível tecnológico mais avançado, e uma avaliação da sua resistência a atacantes competentes através de ensaios de penetração. Caso tais atividades de avaliação não sejam adequadas, são realizadas atividades de avaliação alternativas de efeito equivalente.

8. Um sistema europeu de certificação da cibersegurança pode especificar vários níveis de avaliação, em função do rigor e do alcance da metodologia de avaliação utilizada. Cada nível de avaliação corresponde a um dos níveis de garantia e é definido através de uma combinação adequada de componentes de garantia.

Artigo 53.º

Autoavaliação da conformidade

1. Os sistemas europeus de certificação da cibersegurança podem permitir a realização de uma autoavaliação da conformidade sob a exclusiva responsabilidade do fabricante de produtos de TIC, do prestador de serviços de TIC ou do fornecedor de processos de TIC. A autoavaliação da conformidade é permitida apenas para produtos, serviços e processos de TIC com um nível de risco baixo, correspondente ao nível de garantia «básico».

2. O fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC pode emitir uma declaração UE de conformidade que indique que foi demonstrado o cumprimento dos requisitos estabelecidos no sistema. Através da emissão dessa declaração, o fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC assume a responsabilidade pela conformidade do produto, serviço ou processo de TIC com os requisitos previstos nesse sistema.

3. O fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC mantém à disposição da autoridade nacional de certificação da cibersegurança a que se refere o artigo 58.º, pelo período fixado no sistema europeu de certificação da cibersegurança em causa, a declaração UE de conformidade, a documentação técnica e todas as outras informações pertinentes relativas à conformidade dos produtos, serviços ou processos de TIC com o sistema. É apresentada à autoridade nacional de certificação da cibersegurança e à ENISA uma cópia da declaração UE de conformidade.

4. A declaração UE de conformidade é emitida a título voluntário, salvo disposição em contrário do direito da União ou dos Estados-Membros.

5. As declarações UE de conformidade são reconhecidas em todos os Estados-Membros.

Artigo 54.º

Elementos dos sistemas europeus de certificação da cibersegurança

1. Os sistemas europeus de certificação da cibersegurança compreendem, no mínimo, os seguintes elementos:

a) O objeto e o âmbito do sistema de certificação, nomeadamente o tipo ou as categorias de produtos, serviços e processos de TIC abrangidos;

b) Uma descrição clara do objetivo do sistema e do modo como as normas, os métodos de avaliação e os níveis de garantia selecionados correspondem às necessidades dos utilizadores do sistema a que se destinam;

c) Referências às normas internacionais, europeias ou nacionais aplicadas na avaliação ou, caso essas normas não estejam disponíveis ou não sejam adequadas às especificações técnicas que cumprem os requisitos estabelecidos no anexo II do Regulamento (UE) n.º 1025/2012 ou, na falta destas últimas, a especificações técnicas ou outros requisitos de cibersegurança previstos no sistema europeu de certificação de cibersegurança;

d) Um ou mais níveis de garantia, se aplicável;

e) Uma indicação que precise se a autoavaliação da conformidade é autorizada no âmbito do sistema;

f) Se aplicável, os requisitos específicos ou adicionais a que estão sujeitos os organismos de avaliação da conformidade, a fim de garantir a sua competência técnica para avaliar os requisitos de cibersegurança;

g) Os critérios e métodos de avaliação específicos, nomeadamente os tipos de avaliação a utilizar para demonstrar que são alcançados os objetivos de segurança específicos referidos no artigo 51.º;

h) Se aplicável, as informações necessárias para a certificação e que os requerentes devem fornecer ou de qualquer outro modo pôr à disposição dos organismos de avaliação da conformidade;

i) As condições de utilização de marcas ou rótulos, caso estes estejam previstos pelo sistema;

j) As regras para o controlo da conformidade dos produtos, serviços ou processos de TIC com os requisitos dos certificados europeus de cibersegurança ou da declaração UE de conformidade, incluindo mecanismos para demonstrar a conformidade permanente com os requisitos de cibersegurança especificados;

k) Se aplicável, as condições para a emissão, manutenção, continuação e renovação de um certificado europeu de cibersegurança, bem como as condições para o alargamento ou a redução do âmbito da certificação;

l) As regras relativas às consequências para os produtos, serviços e processos de TIC que tenham sido certificados ou para os quais tenha sido emitida uma declaração UE de conformidade, mas que não cumprem os requisitos do sistema;

m) As regras relativas ao modo como devem ser comunicadas e tratadas vulnerabilidades de cibersegurança não detetadas anteriormente em produtos, serviços e processos de TIC;

n) Se aplicável, as regras relativas à conservação de registos por parte dos organismos de avaliação da conformidade;

o) A identificação dos sistemas nacionais ou internacionais de certificação da cibersegurança que abranjam os mesmos tipos ou categorias de produtos, serviços e processos de TIC, requisitos de segurança, critérios e métodos de avaliação e níveis de garantia;

p) O conteúdo e formato dos certificados europeus de cibersegurança e das declarações UE de conformidade a emitir;

q) O período de disponibilidade da declaração UE de conformidade, da documentação técnica e de todas as outras informações relevantes a disponibilizar pelo fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC;

r) O prazo máximo de validade dos certificados europeus de cibersegurança emitidos ao abrigo do sistema;

s) A política de divulgação dos certificados europeus de cibersegurança emitidos, alterados e retirados ao abrigo do sistema;

t) As condições para o reconhecimento mútuo de sistemas de certificação com países terceiros;

u) Se aplicável, as regras relativas a um eventual mecanismo de avaliação pelos pares criado pelo sistema para as autoridades ou organismos que emitem certificados europeus de cibersegurança para o nível de garantia «elevado» nos termos do artigo 56.º, n.º 6. Tal mecanismo não prejudica a análise pelos pares prevista no artigo 59.º;

v) O formato e os procedimentos a seguir pelos fabricantes de produtos de TIC, prestadores de serviços de TIC ou fornecedores de processos de TIC para o fornecimento e a atualização das informações complementares sobre cibersegurança nos termos do artigo 55.º.

2. Os requisitos especificados do sistema europeu de certificação da cibersegurança são coerentes com os requisitos legais aplicáveis, em especial requisitos decorrentes do direito da União harmonizado.

3. Se um ato jurídico específico da União assim o previr, o certificado ou a declaração UE de conformidade emitidos ao abrigo de um sistema europeu de certificação da cibersegurança podem ser utilizados para demonstrar a presunção de conformidade com os requisitos do ato jurídico em questão.

4. Na falta de um direito da União harmonizado, um Estado-Membro pode também prever que um sistema europeu de certificação da cibersegurança possa ser utilizado para estabelecer a presunção de conformidade com requisitos legais.

Artigo 55.º

Informações complementares sobre cibersegurança para os produtos, serviços e processos de TIC certificados

1. O fabricante de produtos de TIC, o prestador de serviços de TIC ou o fornecedor de processos de TIC certificados ou de produtos, serviços ou processos de TIC para os quais foi emitida uma declaração UE de conformidade disponibiliza publicamente as seguintes informações complementares:

a) Orientações e recomendações para ajudar os utilizadores finais na configuração, instalação, implantação, funcionamento e manutenção seguros dos produtos de TIC ou serviços de TIC;

b) O período durante o qual é oferecido aos utilizadores finais apoio em matéria de segurança, em especial no que diz respeito à disponibilidade de atualizações relacionadas com a cibersegurança;

c) Os contactos do fabricante, do prestador ou do fornecedor e os métodos aceites para receber informações sobre vulnerabilidades comunicadas pelos utilizadores finais ou pelos investigadores em matéria de segurança;

d) Uma referência a repositórios em linha que enumerem as vulnerabilidades do conhecimento público relacionadas com o produto, serviço ou processo de TIC, e conselhos pertinentes em matéria de cibersegurança.

2. As informações referidas no n.º 1 são disponibilizadas em formato eletrónico, permanecem disponíveis e são atualizadas conforme necessário pelo menos até caducar o certificado europeu de cibersegurança ou a declaração UE de conformidade correspondentes.

Artigo 56.º

Certificação da cibersegurança

1. Presume-se que os produtos, serviços e processos de TIC que tenham sido certificados ao abrigo de um sistema europeu de certificação da cibersegurança adotado nos termos do artigo 49.º cumprem os requisitos desse sistema.

2. A certificação de cibersegurança é voluntária, salvo disposição em contrário no direito da União ou dos Estados-Membros.

3. A Comissão avalia regularmente a eficiência e a utilização dos sistemas europeus de certificação da cibersegurança adotados e se algum sistema europeu de certificação da cibersegurança específico deve passar a ser obrigatório por força do direito aplicável da União, a fim de assegurar um nível adequado de cibersegurança dos produtos, serviços e processos de TIC na União e melhorar o funcionamento do mercado interno. A primeira dessas avaliações deve ser realizada até 31 de dezembro de 2023 e as avaliações subsequentes devem ser efetuadas pelo menos de dois em dois anos. Baseado no resultado dessas avaliações, a Comissão identifica os produtos, serviços e processos de TIC abrangidos por um sistema de certificação existente que devem ser abrangidos por um sistema de certificação obrigatório.

A Comissão concentra-se prioritariamente nos setores enumerados no anexo II da Diretiva (UE) 2016/1148, que são avaliados o mais tardar dois anos após a adoção do primeiro sistema europeu de certificação da cibersegurança.

Ao preparar a avaliação, a Comissão:

a) Toma em consideração o impacto das medidas para os fabricantes de produtos de TIC, os prestadores de serviços de TIC e os fornecedores de processos de TIC e para os utilizadores em termos de custos dessas medidas, e os benefícios societais ou económicos decorrentes do reforço previsto do nível de segurança para os produtos, serviços e processos visados;

b) Tem em conta a existência e a aplicação do direito aplicável do Estado-Membro e do país terceiro;

c) Procede a uma consulta aberta, transparente e inclusiva de todas as partes interessadas e Estados-Membros;

d) Toma em consideração os prazos de aplicação, as medidas e os períodos de transição, tendo especialmente em conta o eventual impacto da medida para os fabricantes de produtos de TIC, os prestadores de serviços de TIC e os fornecedores de processos de TIC, incluindo as PME;

e) Propõe a forma mais célere e eficaz de efetuar a transição dos sistemas de certificação voluntários para os obrigatórios.

4. Os organismos de avaliação da conformidade a que se refere o artigo 60.º emitem certificados europeu de cibersegurança, nos termos do presente artigo, atestando um nível de garantia «básico» ou «substancial», com base nos critérios incluídos no sistema europeu de certificação da cibersegurança adotado pela Comissão, nos termos do artigo 49.º.

5. Em derrogação do n.º 4, em casos devidamente justificados um sistema europeu de certificação da cibersegurança pode prever que os certificados europeus de cibersegurança ao abrigo desse sistema só possam ser emitidos por um organismo público. Esse organismo deve ser um dos seguintes:

a) Uma autoridade nacional de certificação da cibersegurança a que se refere o artigo 58.º, n.º 1; ou

b) Um organismo público acreditado como organismo de avaliação da conformidade nos termos do artigo 60.º, n.º 1.

6. Nos casos em que um sistema europeu de certificação da cibersegurança adotado nos termos do artigo 49.º exija um nível de garantia «elevado», o certificado europeu de cibersegurança ao abrigo desse sistema só pode ser emitido por uma autoridade nacional de certificação da cibersegurança ou, nos casos a seguir indicadas, por um organismo de avaliação:

a) Mediante aprovação prévia pela autoridade nacional de certificação da cibersegurança para cada certificado europeu de cibersegurança individual emitido por um organismo de avaliação da conformidade; ou

b) Com base numa delegação geral prévia do poder de emitir esses certificados europeus de certificação da cibersegurança pela autoridade nacional de certificação da cibersegurança no organismo de avaliação da conformidade.

7. As pessoas singulares ou coletivas que submetem os seus produtos, serviços ou processos de TIC à certificação disponibilizam à autoridade nacional de certificação da cibersegurança a que se refere o artigo 58.º, quando essa autoridade for o organismo que emite o certificado europeu de certificação da cibersegurança ou o organismo de avaliação da conformidade a que se refere o artigo 60.º, todas as informações necessárias para efetuar a certificação.

8. O titular de um certificado europeu de cibersegurança informa a autoridade ou o organismo referido no n.º 7 de quaisquer vulnerabilidades ou irregularidades posteriormente detetadas relativas à segurança do produto, serviço ou processo de TIC certificado que possam ter um impacto na conformidade do produto, serviço ou processo de TIC com os requisitos relacionados com a certificação. Essa autoridade ou organismo transmite essas informações sem demora injustificada à autoridade nacional de certificação da cibersegurança.

9. Os certificados europeus de cibersegurança são emitidos pelo período definido pelo sistema europeu de certificação da cibersegurança em causa e podem ser renovados, desde que continuem a ser cumpridos os requisitos aplicáveis.

10. Os certificados europeus de cibersegurança emitidos ao abrigo do presente artigo são reconhecidos em todos os Estados-Membros.

Artigo 57.º

Sistemas e certificados nacionais de certificação da cibersegurança

1. Sem prejuízo do disposto no n.º 3 do presente artigo, os sistemas nacionais de certificação da cibersegurança e os procedimentos conexos relativos aos produtos, serviços e processos de TIC abrangidos por um sistema europeu de certificação da cibersegurança deixam de produzir efeitos a partir da data estabelecida no ato de execução adotado ao abrigo do artigo 49.º, n.º 7. Os sistemas nacionais de certificação da cibersegurança e os procedimentos conexos relativos aos produtos de TIC, serviços de TIC e processos de TIC que não sejam abrangidos por um sistema europeu de certificação da cibersegurança continuam a existir.

2. Os Estados-Membros não podem introduzir novos sistemas nacionais de certificação da cibersegurança relativos aos produtos, serviços e processos de TIC abrangidos por um sistema europeu de certificação da cibersegurança em vigor.

3. Os certificados em vigor emitidos ao abrigo de sistemas nacionais de certificação da cibersegurança e abrangidos por um sistema europeu de certificação da cibersegurança permanecem válidos até à respetiva data de caducidade.

4. A fim de evitar a fragmentação do mercado interno, os Estados-Membros comunicam à Comissão e ao GECC a intenção de elaborar novos sistemas nacionais de certificação da cibersegurança.

Artigo 58.º

Autoridades nacionais de certificação da cibersegurança

1. Cada Estado-Membro designa uma ou mais autoridades nacionais de certificação da cibersegurança no seu território ou, com o acordo de outro Estado-Membro, designa uma ou mais autoridades nacionais de certificação da cibersegurança estabelecidas nesse outro Estado-Membro como responsáveis pelas atribuições de supervisão no Estado-Membro que procede à designação.

2. Os Estados-Membros informam a Comissão da identidade das autoridades nacionais de certificação da cibersegurança designadas. Se designarem mais do que uma autoridade, os Estados-Membros informam igualmente a Comissão das atribuições conferidas a cada uma.

3. Sem prejuízo do disposto no artigo 56.º, n.º 5, alínea a), e no artigo 56.º, n.º 6, as autoridades nacionais de certificação da cibersegurança são independentes das entidades que supervisionam, no que se refere à organização, às decisões de financiamento, à estrutura jurídica e à tomada de decisões.

4. Os Estados-Membros garantem que as atividades das autoridades nacionais de certificação da cibersegurança relacionadas com a emissão de certificados europeus de cibersegurança a que se refere o artigo 56.º, n.º 5, alínea a), e o artigo 56.º, n.º 6, estejam rigorosamente separadas das suas atividades de supervisão previstas no presente artigo, e que sejam exercidas independentemente uma da outra.

5. Os Estados-Membros asseguram que as autoridades nacionais de certificação da cibersegurança disponham dos recursos adequados ao exercício das suas competências e à realização eficaz e eficiente das suas atribuições.

6. A fim de permitir a aplicação efetiva do presente regulamento, é conveniente que as autoridades nacionais de certificação da cibersegurança participem de uma forma ativa, eficaz, eficiente e segura no GECC.

7. Compete às autoridades nacionais de certificação da cibersegurança:

a) Supervisionar e fazer aplicar as regras incluídas nos sistemas europeus de certificação da cibersegurança, nos termos do artigo 54.º, n.º 1, alínea j), para efetuar o controlo da conformidade dos produtos, serviços e processos de TIC com os requisitos dos certificados europeus de cibersegurança emitidos nos respetivos territórios, em cooperação com outras autoridades de fiscalização de mercado competentes;

b) Controlar o cumprimento das obrigações do fabricante de produtos de TIC, do prestador de serviços de TIC ou do fornecedor de processos de TIC estabelecidos nos respetivos territórios e que efetuem a autoavaliação da conformidade e fazer executar essas obrigações, em especial, as obrigações estabelecidas no artigo 53.º, n.ºs 2 e 3, e no respetivo sistema europeu de certificação da cibersegurança;

c) Sem prejuízo do disposto no artigo 60.º, n.º 3, prestar ativamente assistência e apoio aos organismos nacionais de acreditação no controlo e na supervisão das atividades dos organismos de avaliação da conformidade para efeitos do presente regulamento;

d) Controlar e supervisionar as atividades dos organismos públicos a que se refere o artigo 56.º, n.º 5;

e) Se aplicável, autorizar os organismos de avaliação da conformidade nos termos do artigo 60.º, n.º 3, e restringir, suspender ou retirar a autorização existente caso esses organismos violem o disposto no presente regulamento;

f) Tratar as reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados europeus de cibersegurança emitidos pela autoridade nacional de certificação da cibersegurança ou a certificados europeus de cibersegurança emitidos por organismos de avaliação da conformidade nos termos do artigo 56.º, n.º 6, ou em relação a declarações UE de conformidade emitidas ao abrigo do artigo 53.º, e investigar, na medida do necessário, o objeto das reclamações e informar os autores das reclamações do andamento e do resultado da investigação num prazo razoável;

g) Fornecer à ENISA e ao GECC um relatório anual de síntese das atividades realizadas, nos termos das alíneas b), c) e d) do presente número ou do n.º 8;

h) Cooperar com outras autoridades nacionais de certificação da cibersegurança ou outras autoridades públicas, inclusive através da partilha de informações sobre a eventual não conformidade de produtos, serviços e processos de TIC com os requisitos do presente regulamento ou de sistemas europeus de certificação da cibersegurança específicos; e

i) Acompanhar factos novos relevantes no domínio da certificação da cibersegurança.

8. Cada autoridade nacional de certificação da cibersegurança dispõe, no mínimo, das competências para:

a) Solicitar aos organismos de avaliação da conformidade, aos titulares de certificados europeus de cibersegurança e aos emitentes de declarações UE de conformidade que lhe forneçam as informações de que necessite para o exercício das suas competências;

b) Conduzir investigações, sob a forma de auditorias, aos organismos de avaliação da conformidade, aos titulares de certificados europeus de cibersegurança e aos emitentes de declarações de conformidade da UE, a fim de verificar se cumprem o disposto no presente título;

c) Tomar as medidas adequadas, de acordo com o direito nacional, a fim de garantir que os organismos de avaliação da conformidade, os titulares de certificados europeus de cibersegurança, e os emitentes de declarações UE de conformidade cumprem o disposto no presente regulamento ou num sistema europeu de certificação da cibersegurança;

d) Obter acesso a todas as instalações dos organismos de avaliação da conformidade ou dos titulares de certificados europeus de cibersegurança com o objetivo de conduzir investigações de acordo com o direito processual da União ou dos Estados-Membros em causa;

e) Retirar, de acordo com o direito nacional, os certificados europeus de cibersegurança emitidos pelas autoridades nacionais de certificação da cibersegurança, ou os certificados europeus de cibersegurança emitidos pelos organismos de avaliação da conformidade nos termos do artigo 56.º, n.º 6, que não cumpram o disposto no presente regulamento ou num sistema europeu de certificação da cibersegurança;

f) Aplicar sanções, de acordo com o direito nacional, como previsto no artigo 65.º, e exigir a cessação imediata da violação das obrigações estabelecidas no presente regulamento.

9. As autoridades nacionais de certificação da cibersegurança cooperam entre si e com a Comissão e, em particular, partilham informações, experiências e boas práticas em matéria de certificação da cibersegurança e de questões técnicas relacionadas com a cibersegurança dos produtos de TIC, serviços de TIC e de processos de TIC.

Artigo 59.º

Análise pelos pares

1. A fim de alcançar a equivalência das normas na União no que se refere aos certificados europeus de cibersegurança emitidos e às declarações UE de conformidade, as autoridades nacionais de certificação da cibersegurança são sujeitas a análise pelos pares.

2. A análise pelos pares deve ser realizada com base em critérios e procedimentos de avaliação sólidos e transparentes, especialmente no que se refere aos requisitos estruturais, de recursos humanos e processuais, à confidencialidade e às reclamações.

3. A análise pelos pares avalia os seguintes elementos:

a) Se aplicável, se as atividades da autoridade nacional de certificação da cibersegurança relacionadas com a emissão de certificados europeus de cibersegurança, nos termos do artigo 56.º, n.º 5, alínea a), e n.º 6, estão rigorosamente separadas das atividades de supervisão previstas no artigo 58.º, e se essas atividades são exercidas independentemente uma da outra;

b) Os procedimentos destinados a supervisionar e controlar a aplicação das regras relativas ao controlo da conformidade dos produtos, serviços e processos de TIC com os certificados europeus de cibersegurança nos termos do artigo 58.º, n.º 7, alínea a);

c) Os procedimentos destinados a controlar o cumprimento das obrigações dos fabricantes de produtos de TIC, dos prestadores de serviços de TIC e dos fornecedores de processos de TIC nos termos do artigo 58.º, n.º 7, e a fazer executar essas obrigações;

d) Os procedimentos destinados a controlar, autorizar e supervisionar as atividades dos organismos de avaliação da conformidade;

e) Se aplicável, se o pessoal das autoridades ou organismos que emitem certificados atestando um nível de garantia «elevado» nos termos do artigo 56.º, n.º 6 possuem os conhecimentos especializados adequados.

4. A análise pelos pares é realizada pelo menos por duas autoridades nacionais de certificação da cibersegurança de outros Estados-Membros e pela Comissão, no mínimo, uma vez de cinco em cinco anos. A ENISA pode participar na análise pelos pares.

5. A Comissão pode adotar atos de execução que estabeleçam um plano para as análises pelos pares que cubra um período de pelo menos cinco anos, e defina os critérios para a composição da equipa de análise pelos pares, a metodologia a seguir na análise, o calendário, a frequência e outras tarefas relacionadas com a análise pelos pares. Ao adotar esses atos de execução, a Comissão tem devidamente em conta as opiniões do GECC. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 66.º, n.º 2.

6. Os resultados das análises pelos pares são examinados pelo GECC, que elabora sínteses que podem ser disponibilizadas ao público e que, se necessário, emite orientações ou recomendações relativas a ações ou medidas a tomar pelas entidades em causa.

Artigo 60.º

Organismos de avaliação da conformidade

1. Os organismos de avaliação da conformidade são acreditados pelos organismos nacionais de acreditação designados nos termos do Regulamento (CE) n.º 765/2008. A acreditação só é emitida se o organismo de avaliação da conformidade cumprir os requisitos estabelecidos no anexo do presente regulamento.

2. Caso seja emitido um certificado europeu de cibersegurança por uma autoridade nacional de certificação da cibersegurança nos termos do artigo 56.º, n.º 5, alínea a), e n.º 6, o organismo de certificação da autoridade nacional de certificação da cibersegurança é acreditado como organismo de avaliação da conformidade nos termos do n.º 1 do presente artigo.

3. Caso os sistemas europeus de certificação da cibersegurança estabeleçam requisitos específicos ou suplementares nos termos do artigo 54.º, n.º 1, alínea f), só os organismos de avaliação da conformidade que cumpram esses requisitos podem ser autorizados pela autoridade nacional de certificação da cibersegurança a executar tarefas no âmbito destes sistemas.

4. A acreditação dos organismos de avaliação da conformidade referida no n.º 1 é emitida por um prazo máximo de cinco anos e pode ser renovada nas mesmas condições, desde que o organismo de avaliação da conformidade continue a cumprir os requisitos estabelecidos no presente artigo. Os organismos nacionais de acreditação tomam todas as medidas adequadas num prazo razoável para restringir, suspender ou revogar a acreditação de um organismo de avaliação da conformidade que tenha sido emitida nos termos do n.º 1, se as condições para a acreditação não tiverem sido cumpridas ou deixarem de ser cumpridas, ou se o organismo de avaliação da conformidade violar o disposto no presente regulamento.

Artigo 61.º

Notificação

1. As autoridades nacionais de certificação da cibersegurança notificam a Comissão, relativamente a cada sistema europeu de certificação da cibersegurança, dos organismos de avaliação da conformidade acreditados e, se for o caso, autorizados nos termos do artigo 60.º, n.º 3 para efeitos da emissão de certificados europeus de cibersegurança atestando os níveis de garantia especificados, conforme referido no artigo 52.º. As autoridades nacionais de certificação da cibersegurança notificam a Comissão sem demora injustificada, de quaisquer alterações posteriores.

2. Um ano após a entrada em vigor de um sistema europeu de certificação da cibersegurança, a Comissão publica no *Jornal Oficial da União Europeia* uma lista dos organismos de avaliação da conformidade notificados no âmbito desse sistema.

3. Se receber uma notificação após o termo do prazo referido no n.º 2, a Comissão publica as alterações da lista dos organismos de avaliação da conformidade notificados no *Jornal Oficial da União Europeia* num prazo de dois meses a contar da data da receção da notificação.

4. As autoridades nacionais de certificação da cibersegurança podem apresentar à Comissão um pedido para que retire da lista referida no n.º 2 um organismo de avaliação da conformidade notificado pela autoridade em causa. A Comissão publica as alterações correspondentes da referida lista no *Jornal Oficial da União Europeia* no prazo de um mês a contar da data de receção do pedido da autoridade nacional de certificação da cibersegurança.

5. A Comissão pode adotar atos de execução para estabelecer as circunstâncias, os formatos e os procedimentos da notificação referida no n.º 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 66.º, n.º 2.

Artigo 62.º

Grupo europeu para a certificação da cibersegurança

1. É criado o grupo europeu para a certificação da cibersegurança (a seguir designado «GECC»).

2. O grupo é composto por representantes das autoridades nacionais de certificação da cibersegurança ou representantes de outras autoridades nacionais competentes. Um membro do GECC não pode representar mais de dois Estados-Membros.

3. Podem ser convidados a assistir às reuniões do GECC e a participar nos seus trabalhos as partes e os terceiros interessados relevantes.

4. O GECC tem as seguintes atribuições:

a) Aconselhar e assistir a Comissão no seu trabalho de assegurar a execução e aplicação coerentes do presente título, nomeadamente no que se refere ao programa de trabalho evolutivo da União, às questões da política de certificação da cibersegurança, à coordenação das abordagens políticas e à elaboração de sistemas europeus de certificação da cibersegurança;

b) Assistir, aconselhar e cooperar com a ENISA no que se refere à elaboração de propostas de sistemas, nos termos do artigo 49.º;

c) Adotar pareceres sobre as propostas de sistemas elaboradas pela ENISA, nos termos do artigo 49.º;

d) Solicitar à ENISA que elabore projetos de sistemas nos termos do artigo 48.º, n.º 2;

e) Adotar pareceres dirigidos à Comissão relativos à manutenção e revisão de sistemas europeus de certificação da cibersegurança em vigor;

f) Analisar a evolução relevante no domínio da certificação da cibersegurança e proceder ao intercâmbio de informações e de boas práticas em matéria de sistemas de certificação da cibersegurança;

g) Facilitar a cooperação entre as autoridades nacionais de certificação da cibersegurança a que se refere o presente título mediante o reforço de capacidades e o intercâmbio de informações, nomeadamente através do estabelecimento de métodos eficientes de intercâmbio de informações relativas a todas a questões no domínio da certificação da cibersegurança;

h) Apoiar a aplicação dos mecanismos de avaliação pelos pares, de acordo com as regras estabelecidas por um sistema europeu de certificação da cibersegurança nos termos do artigo 54.º, n.º 1, alínea u);

i) Facilitar o alinhamento dos sistemas europeus de certificação da cibersegurança pelas normas reconhecidas a nível internacional, nomeadamente avaliando os sistemas europeus de certificação da cibersegurança existentes e, se necessário, formulando recomendações à atenção da ENISA para que colabore com os organismos internacionais de normalização competentes, a fim de sanar insuficiências ou lacunas nas normas existentes reconhecidas internacionalmente.

5. Com a assistência da ENISA, a Comissão preside ao GECC e assegura a prestação dos seus serviços de secretariado ao GECC, tal como previsto no artigo 8.º, n.º 1, alínea e).

Artigo 63.º

Direito de apresentar reclamação

1. As pessoas singulares ou coletivas têm o direito de apresentar uma reclamação junto da entidade emissora dos certificados europeus de cibersegurança ou, no caso de a reclamação se referir a um certificado europeu de cibersegurança emitido por um organismo de avaliação da conformidade agindo nos termos do artigo 56.º, n.º 6, junto da autoridade nacional de certificação da cibersegurança competente.

2. A autoridade ou o organismo ao qual tiver sido apresentada a reclamação informa o seu autor do andamento e do resultado da mesma, e informa-o do direito a um recurso judicial efetivo nos termos do artigo 64.º.

Artigo 64.º

Direito a um recurso judicial efetivo

1. Não obstante os recursos administrativos ou vias extrajudiciais, as pessoas singulares e coletivas têm direito a um recurso judicial efetivo no que respeita:

a) Às decisões adotadas pela autoridade ou por um organismo referido no artigo 63.º, n.º 1, inclusive, se aplicável, em relação à emissão indevida, à omissão de emissão de certificados ou ao reconhecimento de certificados europeus de cibersegurança na posse das referidas pessoas singulares e coletivas;

b) À omissão de ação relativamente a uma reclamação apresentada junto de uma autoridade ou de um organismo referido no artigo 63.º, n.º 1.

2. Os recursos ao abrigo do presente artigo são interpostos perante os tribunais do Estado-Membro onde está situada a autoridade ou o organismo contra o qual são interpostos.

Artigo 65.º

Sanções

Os Estados-Membros estabelecem as regras relativas às sanções aplicáveis em caso de violação do disposto no presente título e nos sistemas europeus de certificação da cibersegurança e tomam as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Os Estados-Membros notificam, sem demora, a Comissão dessas regras e medidas, e notificam-na de qualquer alteração subsequente das mesmas.

TÍTULO IV

DISPOSIÇÕES FINAIS

Artigo 66.º

Procedimento de comité

1. A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º, n.º 4, alínea b), do Regulamento (UE) n.º 182/2011.

Artigo 67.º

Avaliação e revisão

1. Até 28 de junho de 2024, e, daí em diante, de cinco em cinco anos, a Comissão avalia o impacto, a eficácia e a eficiência da ENISA e dos seus métodos de trabalho, a eventual necessidade de alterar o mandato da ENISA e as consequências financeiras dessa alteração. A avaliação tem em conta todas as informações comunicadas à ENISA em resposta às suas atividades. Se entender que manter a ENISA, tendo em conta os seus objetivos, mandato e atribuições, deixou de se justificar, a Comissão pode propor que o presente regulamento seja alterado no que diz respeito às disposições relativas à ENISA.

2. A avaliação visa igualmente o impacto, a eficácia e a eficiência das disposições do título III do presente regulamento, no que respeita aos objetivos de assegurar um nível adequado de cibersegurança dos produtos, serviços e processos de TIC na União e de melhorar o funcionamento do mercado interno.

3. A avaliação deve verificar se são necessários requisitos de cibersegurança essenciais para o acesso ao mercado interno, a fim de impedir que produtos, serviços e processos de TIC que não cumpram os requisitos básicos de cibersegurança entrem no mercado da União.

4. Até 28 de junho de 2024 e, daí em diante, de cinco em anos, a Comissão envia o relatório da avaliação, acompanhado das suas conclusões, ao Parlamento Europeu, ao Conselho e ao conselho de administração. As conclusões desse relatório são publicadas.

Artigo 68.º

Revogação e sucessão

1. O Regulamento (UE) n.º 526/2013 é revogado com efeitos a partir de 27 de junho de 2019.

2. As remissões para o Regulamento (UE) n.º 526/2013 e as referências para a ENISA, tal como criada por esse regulamento, entendem-se como remissões para o presente regulamento e como referências para a ENISA, tal como criada pelo presente regulamento.

3. A ENISA tal como criada pelo presente regulamento sucede à ENISA tal como criada pelo Regulamento (UE) n.º 526/2013 no que respeita a todos os direitos de propriedade, acordos, obrigações legais, contratos de trabalho, compromissos financeiros e responsabilidades. As decisões do conselho de administração e da comissão executiva adotadas nos termos do Regulamento (UE) n.º 526/2013 permanecem válidas, desde que cumpram com o presente regulamento.

4. A ENISA é criada por um período indeterminado a partir de 27 de junho de 2019.

5. O diretor executivo nomeado ao abrigo do artigo 24.º, n.º 4, do Regulamento (UE) n.º 526/2013 permanece em funções e exerce as suas atribuições de diretor executivo da ENISA, nos termos do artigo 20.º do presente regulamento, durante o período remanescente do mandato do diretor executivo. As demais condições do seu contrato permanecem inalteradas.

6. Os membros do conselho de administração e respetivos suplentes nomeados ao abrigo do artigo 6.º do Regulamento (UE) n.º 526/2013 permanecem em funções e exercem as funções do conselho de administração, nos termos do artigo 15.º do presente regulamento, durante o período remanescente do seu mandato.

Artigo 69.º

Entrada em vigor

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

2. Os artigos 58.º, 60.º, 61.º, 63.º, 64.º e 65.º são aplicáveis a partir de 28 de junho de 2021.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Estrasburgo, em 17 de abril de 2019.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*
A. TAJANI	G. CIAMBA

ANEXO

REQUISITOS A CUMPRIR PELOS ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE

Os organismos de avaliação da conformidade que pretendam ser acreditados devem cumprir os seguintes requisitos:

1. Os organismos de avaliação da conformidade devem estar constituídos nos termos do direito nacional e ser dotados de personalidade jurídica.

2. Os organismos de avaliação da conformidade devem ser organismos terceiros independentes da organização ou dos produtos, serviços ou processos de TIC que avaliam.

3. Os organismos que pertençam a organizações empresariais ou associações profissionais que representem empresas envolvidas nas atividades de conceção, fabrico, fornecimento, montagem, utilização ou manutenção de produtos, serviços ou processos de TIC por si avaliados podem ser considerados organismos de avaliação da conformidade, desde que demonstrem a respetiva independência e a inexistência de conflitos de interesses.

4. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem ser o projetista, o fabricante, o fornecedor, o instalador, o comprador, o proprietário, o utilizador ou o responsável pela manutenção dos produtos, serviços ou processos de TIC a avaliar, ou o representante autorizado de uma dessas partes. Esta proibição não obsta à utilização de produtos de TIC avaliados que sejam necessários às atividades do organismo de avaliação da conformidade, nem à utilização desses produtos de TIC para fins pessoais.

5. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem intervir diretamente na conceção, no fabrico ou na construção, na comercialização, na instalação, na utilização nem na manutenção dos produtos, serviços ou processos de TIC que são objeto da avaliação. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem exercer qualquer atividade suscetível de comprometer a independência do seu julgamento ou a sua integridade no exercício das atividades de avaliação da conformidade. Essa proibição é aplicável, nomeadamente, aos serviços de consultoria.

6. Se os organismos de avaliação da conformidade forem propriedade de entidades ou instituições públicas, ou geridos por tais entidades ou instituições, devem ser garantidas e documentadas a independência e a inexistência de conflitos de interesses entre a autoridade nacional de certificação de cibersegurança e o organismo de avaliação da conformidade.

7. Os organismos de avaliação da conformidade devem assegurar que as atividades das suas filiais ou subcontratantes não afetem a confidencialidade, a objetividade ou a imparcialidade das respetivas atividades de avaliação da conformidade.

8. Os organismos de avaliação da conformidade e o seu pessoal devem executar as atividades de avaliação da conformidade com a maior integridade profissional e a maior competência técnica necessária no domínio específico em causa, e não podem estar sujeitos a quaisquer pressões ou incentivos, incluindo de natureza financeira, suscetíveis de influenciar o seu julgamento ou os resultados das suas atividades de avaliação da conformidade, em especial por parte de pessoas ou grupos de pessoas interessadas nos resultados dessas atividades.

9. Os organismos de avaliação da conformidade devem ter capacidade para executar todas as tarefas de avaliação de conformidade que lhes sejam atribuídas ao abrigo do presente regulamento, quer essas tarefas sejam executadas pelos próprios organismos de avaliação da conformidade ou em seu nome e sob a sua responsabilidade. A subcontratação ou consulta a pessoal externo deve ser devidamente documentada, não pode envolver intermediários e deve estar subordinada a um acordo escrito que abranja, entre outros aspetos, a confidencialidade e os conflitos de interesses. O organismo de avaliação da conformidade em causa assume a responsabilidade plena pelas tarefas executadas.

10. Para cada procedimento de avaliação da conformidade e para cada tipo, categoria ou subcategoria de produtos, serviços ou processos de TIC, os organismos de avaliação da conformidade devem sempre dispor de:

    a) Pessoal com conhecimentos técnicos e experiência suficiente e adequada para executar as tarefas de avaliação da conformidade;

    b) Descrições dos procedimentos pelos quais deve ser avaliada a conformidade a fim de assegurar a sua transparência e a sua reprodutibilidade. Devem dispor de uma política e de procedimentos adequados que distingam as tarefas que executam na qualidade de organismos notificados nos termos do artigo 61.º das suas outras atividades;

c) Procedimentos que permitam o exercício das suas atividades, tendo devidamente em conta a dimensão, o setor e a estrutura das empresas, o grau de complexidade da tecnologia do produto, serviço ou processo de TIC em causa e a natureza do processo de produção em massa ou em série.

11. Os organismos de avaliação da conformidade devem dispor dos meios necessários para a boa execução das tarefas técnicas e administrativas relacionadas com as atividades de avaliação da conformidade e ter acesso a todos os equipamentos e instalações necessários.

12. O pessoal responsável por executar as atividades de avaliação da conformidade deve dispor de:

a) Uma sólida formação técnica e profissional, que abranja todas as atividades de avaliação da conformidade;

b) Um conhecimento satisfatório dos requisitos das avaliações de conformidade que efetua e a autoridade necessária para as efetuar;

c) Um conhecimento e compreensão adequados dos requisitos e das normas de ensaio aplicáveis;

d) Aptidão necessária para redigir os certificados, registos e relatórios comprovativos da realização das avaliações de conformidade.

13. Deve ser garantida a imparcialidade dos organismos de avaliação da conformidade, dos seus quadros superiores, das pessoas responsáveis por executar as atividades de avaliação da conformidade e dos subcontratantes.

14. A remuneração dos quadros superiores e das pessoas responsáveis por executar as atividades de avaliação da conformidade não pode depender do número de avaliações de conformidade realizadas nem do seu resultado.

15. Os organismos de avaliação da conformidade devem subscrever um seguro de responsabilidade civil, salvo se essa responsabilidade for assumida pelo Estado-Membro nos termos do direito nacional, ou se o próprio Estado-Membro for diretamente responsável pelas avaliações da conformidade.

16. Os organismos de avaliação da conformidade e o seu pessoal, os seus comités, as suas filiais, os seus subcontratantes, e qualquer outro organismo associado ou o pessoal externo de organismos de avaliação da conformidade, devem manter a confidencialidade e respeitar o sigilo profissional no que se refere a todas as informações obtidas no cumprimento das suas tarefas de avaliação da conformidade no âmbito do presente regulamento ou de qualquer disposição do direito nacional que lhe dê aplicação, salvo nos casos em que a divulgação seja exigida pelo direito da União ou do Estado-Membro ao qual essas pessoas estão sujeitas, e exceto em relação às autoridades competentes do Estado-Membro em que exercem as suas atividades. Os direitos de propriedade intelectual devem ser protegidos. Os organismos de avaliação da conformidade devem dispor de procedimentos documentados referentes aos requisitos do presente ponto.

17. Com exceção do ponto 16, os requisitos estabelecidos no presente anexo em nada obstam ao intercâmbio de informações técnicas e de orientações regulamentares entre organismos de avaliação da conformidade e pessoas que apresentem, ou ponderem apresentar, pedidos de certificação.

18. Os organismos de avaliação da conformidade devem funcionar de acordo com um conjunto de condições coerentes, justas e razoáveis, tendo em conta os interesses das PME no que respeita às taxas.

19. Os organismos de avaliação da conformidade devem cumprir os requisitos da norma aplicável harmonizada, nos termos do Regulamento (CE) n.º 765/2008 para a acreditação de organismos de avaliação da conformidade que certifiquem produtos, serviços ou processos de TIC.

20. Os organismos de avaliação da conformidade devem assegurar que os laboratórios de ensaio utilizados para fins de avaliação da conformidade cumpram os requisitos da norma aplicável harmonizada, nos termos do Regulamento (CE) n.º 765/2008 para a acreditação de laboratórios que realizem ensaios.