Conselho da
União Europeia

Bruxelas, 29 de maio de 2018
(OR. en)

9350/18

Dossiê interinstitucional:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTA

de:	Presidência
para:	Conselho
n.º doc. ant.:	8834/18
n.° doc. Com.:	12183/17
Assunto:	Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à ENISA, a "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") – Orientação geral

I. INTRODUÇÃO

1. Em 13 de setembro de 2017, no contexto da sua Estratégia para o Mercado Único Digital, a Comissão adotou e transmitiu ao Conselho e ao Parlamento Europeu a proposta em epígrafe[1], cuja base jurídica é o artigo 114.º do TFUE. Esta proposta, que faz parte do chamado "pacote Cibersegurança", visa alcançar um nível elevado de cibersegurança, de ciber-resiliência e de confiança no seio da União, com vista a assegurar o normal funcionamento do mercado interno.

2. O regulamento proposto estabelece os objetivos, as atribuições e os aspetos organizativos da ENISA – a Agência da UE para a Cibersegurança – e cria um quadro para o estabelecimento de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança dos produtos e serviços de TIC na União. A proposta da Comissão é acompanhada de uma avaliação de impacto que explora um conjunto específico de oito opções políticas, que abrangem a revisão da ENISA e a certificação da segurança das TIC.

3. O regulamento proposto contém duas grandes vertentes:

   - um mandato permanente para a Agência, com um âmbito delimitado em função das necessidades no quadro das novas prioridades e instrumentos políticos, bem como um conjunto renovado de atribuições e funções da Agência, a fim de permitir um apoio efetivo e eficaz aos esforços envidados pelos Estados-Membros, pelas instituições da UE e por outras partes interessadas tendo em vista garantir um ciberespaço seguro;

   - um quadro europeu de certificação da cibersegurança para os produtos e serviços de TIC e regras relativas aos sistemas europeus de certificação da cibersegurança, que permitirão que os certificados emitidos ao abrigo desses sistemas sejam válidos e reconhecidos em todos os Estados-Membros, bem como responder à atual fragmentação do mercado.

[1] Doc. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. Em outubro de 2017, o Conselho Europeu[2] apelou a que as propostas da Comissão em matéria de cibersegurança fossem elaboradas de forma holística, entregues em tempo útil e analisadas sem demora, com base num plano de ação a definir pelo Conselho.

5. Em 12 de dezembro de 2017, o Conselho dos Assuntos Gerais adotou o plano de ação[3] para aplicação das Conclusões do Conselho[4] sobre a comunicação conjunta[5] ao Parlamento Europeu e ao Conselho intitulada "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE". O plano de ação refletia a ambição do Conselho de chegar a uma orientação geral sobre a proposta até junho de 2018.

6. No Parlamento Europeu, Angelika NIEBLER (ITRE, PPE) foi nomeada relatora. A votação da Comissão ITRE sobre o seu relatório está agendada para 19 de junho de 2018.

7. O Comité Económico e Social Europeu adotou o seu parecer em 14 de fevereiro de 2018.

II. TRABALHOS NO CONSELHO

8. A Comissão apresentou a proposta em apreço e a sua avaliação de impacto ao Grupo Horizontal das Questões do Ciberespaço (a seguir designado por "Grupo") em 26 de setembro de 2017, tendo sido seguidamente realizada uma análise da avaliação de impacto na reunião do Grupo de 20 de outubro de 2017. Os debates subsequentes centraram-se na capacidade operacional da Agência e no âmbito de interação com as autoridades nacionais competentes, bem como no impacto do quadro de certificação no mercado e na competitividade das empresas. De modo geral, a avaliação de impacto e a proposta foram ambas favoravelmente acolhidas pelas delegações.

---

2 EUCO 14/17, ponto 11.
3 Doc. 15748/17.
4 Doc. 14435/17.
5 Doc. 12211/17.

9. O Grupo começou a debater a proposta propriamente dita em novembro de 2017, durante a Presidência estónia, tendo os trabalhos prosseguido durante a Presidência búlgara. Foram realizadas 12 reuniões sobre a proposta, que resultaram na elaboração de oito versões revistas sucessivas da proposta com vista à definição de uma orientação geral no próximo Conselho TTE (Telecomunicações), que terá lugar a 8 de junho de 2018.

10. Os resultados dos debates realizados na reunião do Grupo de 14-15 de maio de 2018, bem como o texto de compromisso revisto da Presidência, constam do anexo à presente nota. Os considerandos foram adaptados para refletir as alterações no articulado. Todas as alterações em relação à proposta da Comissão estão assinaladas a **negrito** ou por [...]. As alterações em relação ao último documento do Grupo (8834/18) estão assinaladas **a negrito e sublinhadas** e todas as supressões estão indicadas por **[...]**.

III. CONCLUSÃO

11. O texto de compromisso da Presidência, constante do anexo, reflete os esforços da Presidência e dos Estados-Membros para conseguir um bom equilíbrio no texto.

12. Em 25 de maio de 2018, o Comité de Representantes Permanentes chegou a acordo sobre o texto de compromisso da Presidência, sob reserva das alterações ao artigo 19.º, n.º 5, e 48.º, n.º 5, reproduzidas em anexo.

13. Convida-se pois o Conselho a adotar uma orientação geral na reunião de 8 de junho de 2018 e a mandatar a Presidência para encetar negociações com os representantes do Parlamento Europeu e da Comissão Europeia sobre este dossiê.

ANEXO

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à ENISA, a "*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[6],

Tendo em conta o parecer do Comité das Regiões[7],

Deliberando de acordo com o processo legislativo ordinário,

[6] JO C de , p. .
[7] JO C de , p. .

Considerando o seguinte:

(1) As redes e sistemas de informação e as redes e serviços de telecomunicações desempenham um papel crucial para a sociedade e tornaram-se a espinha dorsal do crescimento económico. As tecnologias da informação e comunicação estão na base de sistemas complexos que apoiam as atividades sociais, mantêm as nossas economias a funcionar 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 parte dos cidadãos, das empresas e dos governos 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 milhões, se não mesmo milhares de milhões, de dispositivos digitais conectados sejam implantados em toda a UE durante a próxima década. Embora cada vez mais dispositivos estejam conectados à Internet, a segurança e a resiliência não são suficientemente integradas desde a conceção, conduzindo a uma insuficiência de cibersegurança. Neste contexto, a utilização reduzida da certificação leva a que haja informação insuficiente para os utilizadores empresariais e individuais sobre as características de cibersegurança de produtos e serviços de TIC, prejudicando a confiança nas soluções digitais.

(3) A digitalização e conectividade crescentes conduzem a maiores riscos de 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 mitigar o risco para a sociedade, têm de ser adotadas todas as ações necessárias para melhorar a cibersegurança na UE de modo a proteger melhor das ciberameaças as redes e sistemas de informação, as redes de telecomunicações, os produtos digitais, os serviços e dispositivos utilizados pelos cidadãos, os governos e as empresas – desde PME a operadores de infraestruturas críticas.

(4) Os ciberataques estão a aumentar e uma economia e sociedade conectadas, mais vulneráveis a ciberameaças e ciberataques, exigem defesas mais fortes. No entanto, apesar de os ciberataques terem amiúde uma natureza transfronteiriça, as respostas políticas por parte das autoridades responsáveis pela cibersegurança e as competências de aplicação da lei são predominantemente nacionais. Os ciberincidentes em grande escala são suscetíveis de perturbar a prestação de serviços essenciais na UE. Esta realidade exige uma resposta e uma gestão de crises efetivas a nível da UE, criando políticas específicas e desenvolvendo instrumentos mais abrangentes que permitam mostrar a solidariedade europeia e prestar assistência mútua. Além disso, é importante para os decisores políticos, para as empresas e para os utilizadores que se proceda a uma avaliação regular da situação da cibersegurança e da resiliência na União, com base em dados fiáveis da União, bem como a uma previsão sistemática da evolução, dos desafios e das ameaças futuras, tanto a nível da União como a nível global.

(5) 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. Os mesmos incluem a necessidade de reforçar as capacidades e o grau de preparação dos Estados-Membros e das empresas, bem como de melhorar a cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da UE. Além disso, atendendo à natureza sem fronteiras das ciberameaças, é necessário aumentar as capacidades a nível da União suscetíveis de complementar a ação dos Estados-Membros, designadamente no caso de ciberincidentes e cibercrises transfronteiriços em grande escala. São também necessários esforços adicionais para aumentar a sensibilização dos cidadãos e das empresas para as questões de cibersegurança. Além disso, a confiança no mercado único digital deve continuar a ser melhorada mediante a disponibilização de informação transparente sobre o nível de segurança de produtos e serviços de TIC. Tal pode ser facilitado por uma certificação a nível da UE que preveja requisitos de cibersegurança e critérios de avaliação comuns nos mercados e setores nacionais.

(6) Em 2004, o Parlamento Europeu e o Conselho adotaram o Regulamento (CE) n.º 460/2004[8], que cria a ENISA, a fim de contribuir para a consecução dos objetivos de garantir um elevado nível 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. Em 2008, o Parlamento Europeu e o Conselho adotaram o Regulamento (CE) n.º 1007/2008[9], que prolonga o mandato da Agência até março de 2012. O Regulamento (CE) n.º 580/2011[10] prorrogou o mandato da Agência até 13 de setembro de 2013. Em 2013, o Parlamento Europeu e o Conselho adotaram o Regulamento (UE) n.º 526/2013[11], 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, o qual prorrogou o mandato da Agência até junho de 2020.

---

8 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).

9 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).

10 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).

11 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).

(7) A União já deu passos importantes para garantir a cibersegurança e reforçar a confiança nas tecnologias digitais. Em 2013, a Estratégia da UE para a Cibersegurança foi adotada para orientar a resposta política da União às ameaças e riscos de cibersegurança. No seu esforço de proteger melhor os europeus em linha, a União adotou em 2016 o primeiro ato legislativo no domínio da cibersegurança, a Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União ("Diretiva SRI"). A Diretiva SRI instituiu requisitos relativos às capacidades nacionais no domínio da cibersegurança, criou os primeiros mecanismos para reforçar a cooperação estratégica e operacional entre Estados-Membros e introduziu 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, a água, a banca, as infraestruturas do mercado financeiro, os cuidados de saúde, as infraestruturas digitais, bem como os prestadores de serviços digitais essenciais (motores de pesquisa, serviços de computação em nuvem e mercados em linha). Foi atribuído à ENISA um papel importante de apoio à execução desta diretiva. Além disso, a luta eficaz contra a cibercriminalidade constitui uma prioridade importante da Agenda Europeia para a Segurança, contribuindo para o objetivo geral de alcançar um elevado nível de cibersegurança.

(8) É reconhecido que, desde a adoção da Estratégia da UE para a Cibersegurança, de 2013, e da última revisão do mandato da Agência, o contexto político geral se alterou significativamente, inclusive em relação a um ambiente mundial mais incerto e menos seguro. Neste contexto e no âmbito do quadro da nova política de cibersegurança da União, é necessário rever o mandato da ENISA para definir o seu papel no ecossistema alterado de cibersegurança e assegurar que contribui eficazmente para a resposta da União aos desafios de cibersegurança decorrentes deste cenário de ameaça radicalmente transformado, para o qual, conforme reconhecido pela avaliação da Agência, o mandato atual não é suficiente.

(9) A Agência criada pelo presente regulamento deverá suceder à ENISA conforme criada pelo Regulamento (UE) n.º 526/2013. A Agência deve exercer as atribuições que lhe são conferidas pelo presente regulamento e pelos atos jurídicos da União no domínio da cibersegurança mediante, entre outros aspetos, a disponibilização de conhecimentos especializados e de aconselhamento e o funcionamento como um centro de informação e conhecimentos da União. Deve promover o intercâmbio de boas práticas entre Estados-Membros e partes interessadas privadas, apresentando sugestões políticas à Comissão Europeia e aos Estados-Membros, atuando como um ponto de referência para as iniciativas políticas setoriais da União no tocante a questões de cibersegurança, promovendo a cooperação operacional entre os Estados-Membros e entre os Estados-Membros e as instituições, as agências e os organismos europeus.

(10) No quadro da Decisão 2004/97/CE, Euratom, adotada na reunião do Conselho Europeu de 13 de dezembro de 2003, os representantes dos Estados-Membros decidiram que a ENISA teria a sua sede numa cidade da Grécia a determinar pelo Governo grego. O Estado-Membro de acolhimento da Agência deve assegurar as melhores condições possíveis para o funcionamento normal e eficiente da Agência. Para poder exercer correta e eficientemente as suas atribuições, recrutar e fixar o seu pessoal e melhorar a eficiência das suas atividades de rede, é indispensável que a Agência esteja sediada num local adequado, que ofereça, nomeadamente, ligações de transporte e condições adequadas para os cônjuges e os filhos dos membros do pessoal que os acompanhem. As disposições necessárias devem ser estabelecidas num acordo entre a Agência e o Estado-Membro de acolhimento, celebrado após aprovação do conselho de administração da Agência.

(11) Atendendo aos desafios crescentes de cibersegurança que a União está a enfrentar, os recursos financeiros e humanos atribuídos à Agência devem ser aumentados para refletir o reforço do seu papel e atribuições e a sua posição crucial no ecossistema de organizações que defendem o ecossistema digital europeu.

(12) A Agência deve desenvolver e manter um elevado nível de conhecimentos especializados e servir de ponto de referência, instaurando a confiança no mercado único graças à sua independência, à qualidade do aconselhamento prestado e das informações que divulga, à transparência dos seus procedimentos e dos seus métodos de funcionamento e à sua diligência no exercício das suas atribuições. A Agência deve **apoiar** [...] os esforços nacionais e **contribuir proativamente para os esforços** da União, exercendo simultaneamente as suas atribuições em plena cooperação com as instituições, [...] agências **e organismos** da União e com os Estados-Membros. Além disso, a Agência deve tirar proveito da cooperação com o setor privado e outras partes interessadas relevantes e dos seus contributos. Um conjunto de atribuições deve determinar como a Agência deve atingir os seus objetivos, permitindo-lhe ao mesmo tempo uma certa flexibilidade de funcionamento.

(13) A Agência deve prestar assistência à Comissão por meio de aconselhamento, de pareceres e de análises sobre todas as matérias da competência da União relacionadas com a elaboração, atualização e revisão de políticas e de legislação no domínio da cibersegurança e os respetivos aspetos setoriais específicos, a fim de melhorar a pertinência das políticas e legislações da UE que tenham uma vertente de cibersegurança e de permitir a sua implementação coerente a nível nacional [...]. A Agência deve atuar como um ponto de referência de aconselhamento e conhecimentos especializados para iniciativas políticas e legislativas em setores específicos da União que envolvam questões relacionadas com a cibersegurança.

(14) A tarefa subjacente da Agência é promover a aplicação consistente do quadro jurídico relevante, nomeadamente a execução eficaz da Diretiva SRI, que é essencial para aumentar a ciber-resiliência. Atendendo à rápida evolução do cenário de ameaça à cibersegurança, é manifesto que os Estados-Membros devem ser apoiados por uma abordagem mais abrangente e transversal às políticas para reforçar a ciber-resiliência.

(15) A Agência deve prestar assistência aos Estados-Membros e às instituições, [...] agências **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 sistemas de informação. Concretamente, a Agência deve apoiar o desenvolvimento e reforço de CSIRT nacionais, com vista à consecução de um elevado nível comum da sua maturidade na União. **As atividades exercidas pela ENISA relacionadas com as capacidades operacionais dos Estados-Membros devem ser apenas complementares das medidas adotadas pelos próprios Estados-Membros a fim de dar cumprimento às suas obrigações decorrentes da Diretiva SRI, não devendo, por conseguinte, substituí-las** [...].

(15-A) A Agência deve igualmente prestar assistência no desenvolvimento e na atualização de estratégias da União e, mediante pedido, dos Estados-Membros em matéria de segurança das redes e sistemas de informação, nomeadamente de cibersegurança, promover a sua divulgação e acompanhar a sua execução. A Agência deve também disponibilizar formações e material de formação a organismos públicos e, quando pertinente, "formar os formadores", com vista a assistir os Estados-Membros no desenvolvimento das suas próprias capacidades de formação.

(16) A Agência deve assistir o grupo de cooperação criado pela Diretiva SRI na execução das suas atribuições, em especial prestando conhecimentos especializados e aconselhamento e facilitando o intercâmbio de boas práticas, nomeadamente no que se refere à identificação de operadores de serviços essenciais pelos Estados-Membros, incluindo quanto a dependências transfronteiriças, referentes a riscos e incidentes.

(17) Com vista a estimular a cooperação entre o setor público e privado e dentro do setor privado, [...] **a Agência deve** apoiar **a partilha de informações nos setores e entre eles, em particular nos setores enumerados no anexo II da Diretiva (UE) 2016/1148, divulgando boas práticas e orientações sobre os instrumentos disponíveis e os procedimentos, bem como prestando orientações sobre a resolução de questões regulamentares relativas à partilha de informações, designadamente facilitando** a criação de centros de partilha e análise de informações (ISAC) a nível setorial [...].

(18) A Agência deve agregar e analisar relatórios nacionais das CSIRT e da CERT-UE **partilhados a título voluntário**, **com o intuito de ajudar os Estados-Membros a criar** [...] **procedimentos**, linguagem e terminologia comuns para o intercâmbio de informações. A Agência deve também envolver o setor privado, dentro do quadro da Diretiva SRI, que estabelece os fundamentos para o intercâmbio voluntário de informações técnicas a nível operacional [...] **no âmbito** da rede de CSIRT.

(19) A Agência deve contribuir para uma resposta a nível da UE, em caso de incidentes e crises de cibersegurança transfronteiriços em grande escala. Esta função deve **ser desempenhada de acordo com o mandato da Agência, nos termos do presente regulamento, e segundo uma abordagem a ser definida pelos Estados-Membros no contexto da Recomendação da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala. Poderá** incluir a recolha de informações relevantes e a atuação como um facilitador entre a rede de CSIRT e a comunidade técnica, bem como os decisores políticos responsáveis pela gestão de crises. Além disso, a Agência poderá apoiar o tratamento de incidentes de uma perspetiva técnica, facilitando o intercâmbio pertinente de soluções técnicas entre Estados-Membros e disponibilizando contributos para comunicações públicas. A Agência deve apoiar o processo testando modalidades dessa cooperação por intermédio de exercícios [...] **regulares** de cibersegurança.

(20) [...] **Ao prestar apoio** à **cooperação** operacional [...], a Agência deve recorrer aos conhecimentos especializados **técnicos e operacionais** da CERT-UE mediante uma cooperação estruturada [...]. [...] Sempre que pertinente, devem ser estabelecidos acordos específicos entre as duas organizações para definir a execução prática dessa cooperação **e evitar a duplicação de atividades**.

(21) Em consonância com as suas tarefas [...] **de apoio à cooperação operacional no âmbito da rede de CSIRT**, a Agência deve ser capaz de prestar apoio aos Estados-Membros**, a pedido destes,** nomeadamente aconselhando-os **sobre a forma de melhorar 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 ameaças e incidentes. **No âmbito da facilitação do tratamento técnico de incidentes com um impacto significativo ou substancial, a ENISA deve, em particular, apoiar a partilha voluntária de soluções técnicas entre os Estados-Membros ou produzir informações técnicas combinadas, designadamente soluções técnicas partilhadas pelos Estados-Membros a título voluntário.** A recomendação da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala recomenda que os Estados-Membros cooperem de boa-fé e partilhem entre si e com a ENISA informações sobre esses incidentes e crises sem atrasos injustificados. Essas informações deverão ajudar a ENISA no [...] **apoio à cooperação operacional**.

(22) Como parte da cooperação regular a nível técnico para apoiar o conhecimento da situação na União, a Agência deve elaborar regularmente **e em estreita colaboração com os Estados--Membros** o relatório sobre a situação técnica da cibersegurança na UE quanto a incidentes e ameaças, baseando-se em informações publicamente disponíveis, nas suas próprias análises e em relatórios partilhados com ela pelas CSIRT dos Estados-Membros [...] ou pelos pontos únicos de contacto da Diretiva SRI **(ambos numa base voluntária)**, pelo Centro Europeu da Cibercriminalidade (EC3) da Europol, pela CERT-UE e, sempre que pertinente, pelo Centro de Situação e de Informações da UE (INTCEN) do Serviço Europeu para a Ação Externa (SEAE). O relatório deve ser disponibilizado às instâncias pertinentes do Conselho, da Comissão, do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança e da rede de CSIRT.

(23) **O apoio prestado pela Agência a** [...] **inquéritos** técnicos *ex post* a incidentes com impacto significativo [...] mediante pedido [...] dos Estados-Membros **em causa** deve concentrar-se na prevenção de futuros incidentes [...]. **Os Estados-Membros em causa devem fornecer as informações necessárias para que a Agência possa apoiar eficazmente o inquérito técnico.**

(24) [...]

(25) Os Estados-Membros poderão convidar as empresas afetadas pelo incidente a cooperarem mediante o fornecimento de informações e assistência necessárias à Agência, sem prejuízo do seu direito de protegerem as informações comercialmente sensíveis.

(26) 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 da União, a Agência deve analisar os riscos atuais e emergentes. Para o efeito, a Agência deve, em cooperação com os Estados-Membros e, quando pertinente, com institutos de estatística e outros organismos, recolher informações pertinentes **publicamente disponíveis ou partilhadas a título voluntário**, analisar tecnologias emergentes e fornecer avaliações de tópicos específicos sobre impactos sociais, jurídicos, económicos e regulamentares previstos das inovações tecnológicas na segurança das redes e da informação, nomeadamente na cibersegurança. Além disso, a Agência deve apoiar os Estados-Membros e as instituições, agências e organismos da União na identificação de tendências emergentes e na prevenção de [...] **incidentes** de cibersegurança, mediante a análise de ameaças e incidentes.

(27) A fim de aumentar a resiliência da União, a Agência deve desenvolver excelência no tema da **ciber**segurança das **infraestruturas de apoio, designadamente, aos setores enumerados no anexo II da Diretiva SRI e das infraestruturas que são utilizadas pelos prestadores de serviços digitais enumerados no anexo III da mesma diretiva** [...], prestando aconselhamento, orientação e divulgando boas práticas. Com vista a assegurar um acesso facilitado a informação mais bem estruturada sobre riscos de cibersegurança e eventuais soluções, a Agência deve desenvolver e manter o "polo de informação" da União, um portal único que preste ao público informações sobre cibersegurança resultantes das instituições, das agências e dos organismos da UE e nacionais.

(28) A Agência deve contribuir para a sensibilização do público sobre os riscos relacionados com a cibersegurança e fornecer orientações sobre boas práticas para utilizadores individuais destinadas aos cidadãos e às organizações. A Agência deve também contribuir para promover boas práticas e soluções a nível das pessoas e organizações, recolhendo e analisando informações publicamente disponíveis relativas a incidentes significativos e coligindo relatórios destinados a prestar orientação às empresas e aos cidadãos e a melhorar o nível geral de preparação e resiliência. Além disso, a Agência deve organizar, em cooperação com os Estados-Membros e as instituições, [...] agências **e organismos** da União, ações de sensibilização e campanhas públicas de informação periódicas destinadas aos utilizadores finais, a fim de promover comportamentos individuais em linha mais seguros e de sensibilizar para as ameaças potenciais no ciberespaço, incluindo cibercrimes como os ataques de mistificação da interface, as redes de computadores zombies ou botnets e as fraudes financeiras e bancárias, bem como prestar aconselhamento sobre a autenticação de base e a proteção de dados. A Agência deve desempenhar um papel central na intensificação da sensibilização dos utilizadores finais para a segurança dos dispositivos.

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

(30) A fim de assegurar a plena realização dos seus objetivos, a Agência deve estabelecer ligações com as instituições, as agências e os organismos competentes, nomeadamente a CERT-UE, o Centro Europeu da Cibercriminalidade (EC3) da Europol, a Agência Europeia de Defesa (AED), a Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), a Agência Europeia para a Segurança da Aviação (AESA)**, a Agência do Sistema Global de Navegação por Satélite Europeu (Agência do GNSS Europeu)** e qualquer outra agência da UE que esteja envolvida na cibersegurança. Deve ainda estabelecer ligações com autoridades que lidem com a proteção de dados, a fim de partilhar conhecimentos especializados e boas práticas e prestar aconselhamento sobre aspetos de cibersegurança suscetíveis de afetarem o seu trabalho. O grupo permanente de partes interessadas da Agência deve poder incluir representantes das autoridades nacionais e da União encarregadas da aplicação da lei e da proteção de dados. Ao estabelecer ligações com os organismos encarregados da aplicação da lei sobre aspetos de segurança das redes e da informação que possam afetar o seu trabalho, a Agência deve respeitar os canais de informação existentes e as redes estabelecidas.

(31) A Agência, **ao assegurar o serviço de** [...] secretariado da rede de CSIRT, deve apoiar as CSIRT dos Estados-Membros e a CERT-UE na cooperação operacional, além de todas as atribuições relevantes da rede de CSIRT, como definido na Diretiva SRI. Além disso, a Agência deve 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 envolvam, ou sejam suscetíveis de envolver, pelo menos duas CERT, tendo simultaneamente em devida conta os procedimentos operacionais normalizados da rede de CSIRT.

(32) Com vista a aumentar o grau de preparação da União na resposta a incidentes de cibersegurança, a Agência deve organizar exercícios [...] **regulares** de cibersegurança a nível da União e, mediante pedido, apoiar os Estados-Membros e as instituições, agências e organismos da UE na organização de exercícios.

(33) A Agência deve 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 Agência deve promover a adoção da certificação da cibersegurança dentro da União, nomeadamente contribuindo para a criação e manutenção de um quadro de certificação da cibersegurança a nível da União, com vista a aumentar a transparência da garantia de cibersegurança de produtos e serviços de TIC e, desta forma, reforçar a confiança no mercado interno digital.

(34) As políticas de cibersegurança eficientes devem 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 quanto à sua aplicação eficiente. A promoção e o desenvolvimento de boas práticas em matéria de avaliação dos riscos e de soluções interoperáveis de gestão de riscos nas organizações dos setores público e privado aumentarão o nível de cibersegurança na União. Para esse efeito, a Agência deve apoiar a cooperação entre as partes interessadas a nível da União, facilitando os seus esforços no que respeita à criação e à aplicação de normas europeias e internacionais 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 sistemas de informação.

(35) A Agência deve incentivar os Estados-Membros e os prestadores de serviços a reforçarem as suas normas gerais de segurança, para que todos os utilizadores da Internet possam tomar as medidas necessárias para assegurarem a sua própria cibersegurança. Concretamente, os prestadores de serviços e os fabricantes de produtos devem retirar ou reciclar produtos e serviços que não cumpram as normas de cibersegurança. Em cooperação com as autoridades competentes, a ENISA poderá divulgar informações relativas ao nível de cibersegurança dos produtos e serviços disponibilizados no mercado interno e emitir alertas que visem os prestadores e fabricantes e solicitar-lhes que reforcem a segurança, nomeadamente a cibersegurança, dos seus produtos.

(36) A Agência deve 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, [...] agências **e organismos** da União e, se for caso disso, os Estados-Membros, a seu pedido, sobre as necessidades de investigação em matéria de [...] cibersegurança. **A fim de identificar as necessidades e prioridades de investigação, a Agência deve igualmente consultar os grupos de utilizadores pertinentes.**

(37) **As ciberameaças** [...] são problemas mundiais. É necessário reforçar a cooperação internacional a fim de melhorar as normas de **ciber**segurança, nomeadamente definindo normas comuns de comportamento, partilhando informações e promovendo 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 Agência deve apoiar um maior envolvimento e cooperação da União com os países terceiros e com as organizações internacionais, fornecendo, se for caso disso, os conhecimentos especializados e as análises necessárias às instituições, [...] agências **e organismos** competentes da União.

(38) A Agência deve ser capaz de responder a pedidos *ad hoc* de aconselhamento e assistência por parte dos Estados-Membros e das instituições, agências e organismos da UE que se enquadrem nos seus objetivos.

(39) É necessário aplicar certos princípios relativos à governação da Agência a fim de respeitar a Declaração Comum e a Abordagem Comum acordadas em julho de 2012 pelo Grupo de Trabalho Interinstitucional sobre as agências descentralizadas da União, cujo objetivo é racionalizar as atividades das agências e melhorar o seu desempenho. A Declaração Comum e a Abordagem Comum devem refletir-se também, conforme adequado, nos programas de trabalho, nas avaliações, na elaboração dos relatórios e nas práticas administrativas da Agência.

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

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

(42) O bom funcionamento da Agência implica que o seu diretor executivo seja nomeado com base no mérito e em capacidades de gestão e administrativas documentadas, bem como na competência e na experiência relevantes para a cibersegurança, e que desempenhe as suas funções com total independência. O diretor executivo deve preparar uma proposta de programa de trabalho da Agência, após consulta da Comissão, e tomar todas as medidas necessárias para garantir a boa execução do programa de trabalho. O diretor executivo deve preparar um relatório anual, **inclusive sobre a execução do programa de trabalho anual da Agência,** a apresentar ao conselho de administração, elaborar um projeto de mapa previsional das receitas e despesas da Agência e executar o orçamento. Além disso, o diretor executivo deve ter a possibilidade de criar grupos de trabalho *ad hoc* para questões específicas, designadamente de natureza científica, técnica, legal ou socioeconómica. O diretor executivo deve assegurar que os membros dos grupos de trabalho *ad hoc* sejam selecionados de acordo com os mais elevados padrões de especialização, tendo devidamente em conta a necessidade de assegurar uma representação equilibrada, se for caso disso, em função das questões específicas em causa, entre as administrações públicas dos Estados-Membros, as instituições da União e o setor privado, incluindo empresas, utilizadores e académicos especialistas em segurança das redes e da informação.

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

(44) A Agência deve dispor, a título de órgão consultivo, de um grupo permanente de partes interessadas para assegurar o diálogo regular com o setor privado, com as associações de consumidores e com outras partes interessadas pertinentes. Esse grupo permanente de partes interessadas, criado pelo conselho de administração sob proposta do diretor executivo, deve concentrar-se em questões pertinentes para as partes interessadas e submetê-las à atenção da Agência. A composição do grupo permanente de partes interessadas, que deverá ser consultado particularmente no que diz respeito ao projeto [...] de **p**rograma de **t**rabalho, e as atribuições que lhe são conferidas devem assegurar uma representação suficiente das partes interessadas no trabalho da Agência.

(45) A Agência deve dispor de regras em matéria de prevenção e gestão de conflitos de interesse. A Agência deve igualmente aplicar as disposições relevantes da União sobre o acesso do público a documentos constantes do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho[12]. O tratamento de dados pessoais por parte da Agência deve estar sujeito ao disposto no Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos organismos comunitários e à livre circulação desses dados[13]. A Agência deve respeitar as disposições aplicáveis às instituições da União e a legislação nacional relativa ao tratamento de informações, nomeadamente de informações sensíveis não classificadas e de informações classificadas da UE.

---

12 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).

13 JO L 8 de 12.1.2001, p. 1.

(46) A fim de assegurar a plena autonomia e independência da Agência, e de lhe permitir exercer atribuições novas ou adicionais, incluindo atribuições de emergência imprevistas, a Agência deve ser dotada de um orçamento autónomo suficiente cujas receitas provenham essencialmente de uma contribuição da União e de contribuições dos países terceiros que participam nos trabalhos da Agência. A maior parte do pessoal da Agência deve estar diretamente implicada na execução operacional do mandato da Agência. O Estado-Membro de acolhimento, ou qualquer outro Estado-Membro, deve poder contribuir voluntariamente para as receitas da Agência. O procedimento orçamental da União deve permanecer aplicável no que diz respeito a todas as subvenções imputadas ao orçamento geral da União. Além disso, o Tribunal de Contas deve proceder à auditoria das contas da Agência, a fim de assegurar a transparência e a responsabilização.

(47) [...]

(48) A certificação da cibersegurança desempenha um papel importante no aumento da confiança e segurança dos produtos e serviços de TIC. O mercado único digital, e em especial a economia dos dados e a Internet das coisas, apenas pode prosperar se houver uma confiança pública generalizada de que esses produtos e serviços fornecem um determinado nível de garantia da cibersegurança. Os automóveis conectados e automatizados, os dispositivos médicos eletrónicos, os sistemas industriais de automatização e controlo ou as redes inteligentes são apenas alguns exemplos de setores nos quais a certificação é já amplamente utilizada ou suscetível de vir a ser utilizada no futuro próximo. Os setores regulados pela Diretiva SRI são também setores nos quais a certificação da cibersegurança é crucial.

(49) Na comunicação de 2016 intitulada "Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora", a Comissão salientou a necessidade de produtos e soluções de cibersegurança de elevada qualidade, a preços acessíveis e interoperáveis. O fornecimento de produtos e serviços de TIC no mercado único continua a ser muito fragmentado geograficamente. Isto resulta de a indústria da cibersegurança na Europa se ter desenvolvido essencialmente com base na procura governamental nacional. Além disso, a falta de soluções interoperáveis (normas técnicas), práticas e mecanismos de certificação à escala da UE é outra das lacunas que afetam o mercado único da cibersegurança. Por um lado, esta situação torna difícil para as empresas europeias concorrer a nível nacional, europeu e mundial. Por outro, reduz a escolha de tecnologias de cibersegurança viáveis e utilizáveis a que as pessoas e as empresas têm acesso. De igual modo, na revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital, a Comissão salientou a necessidade de produtos e sistemas conectados seguros e indicou que a criação de um quadro europeu de segurança das TIC que defina regras sobre como organizar a certificação da segurança das TIC na União poderia preservar a confiança na Internet e resolver a fragmentação atual do mercado da cibersegurança.

(50) Atualmente, a certificação da cibersegurança de **processos,** produtos e serviços de TIC é utilizada apenas de forma limitada. Quando existe, verifica-se na sua maioria a nível do Estado-Membro ou no quadro de sistemas impulsionados pela indústria. Neste contexto, um certificado emitido por uma autoridade nacional de cibersegurança não é, em princípio, reconhecido por outros Estados-Membros. Por conseguinte, as empresas têm de certificar os seus produtos e serviços nos vários Estados-Membros onde operam, nomeadamente com vista a participar em procedimentos nacionais de adjudicação de contratos. Acresce que, embora estejam a surgir novos sistemas, parece não existir uma abordagem coerente e holística no tocante a questões horizontais de cibersegurança, designadamente no domínio da Internet das coisas. Os sistemas existentes apresentam insuficiências e diferenças consideráveis em termos de cobertura de produtos, níveis de garantia, critérios substantivos e utilização efetiva.

(51) No passado foram envidados alguns esforços para conduzir a um reconhecimento mútuo de certificados na Europa. Todavia, 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 inclui uma parte dos Estados-Membros da União. Esta circunstância limitou a eficácia do ARM do SOG-IS do ponto de vista do mercado interno.

(52) Atendendo ao que precede, afigura-se necessário criar um quadro europeu de 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 **e as declarações de conformidade da UE** dos produtos e serviços de TIC sejam reconhecidos e utilizados em todos os Estados-Membros. O quadro europeu deve ter uma dupla finalidade: por um lado, deve ajudar a aumentar a confiança nos produtos e serviços de TIC que foram certificados em conformidade com os referidos sistemas; por outro lado, deve evitar a multiplicação de certificações nacionais da cibersegurança que entrem em conflito ou que se sobreponham e, desta forma, reduzir os custos para as empresas que operam no mercado único digital. Os sistemas devem ser não discriminatórios e assentes em normas internacionais e/ou **[...] europeias**, salvo se tais normas forem ineficazes ou inadequadas para satisfazer os objetivos legítimos da União a este respeito.

(53) Devem ser atribuídas competências à Comissão para adotar sistemas europeus de certificação da cibersegurança relativamente a grupos específicos de **processos,** produtos e serviços de TIC. Esses sistemas devem ser implementados e supervisionados por autoridades nacionais de certificação [...] **da cibersegurança** e os certificados emitidos no âmbito de tais sistemas devem ser válidos e reconhecidos em toda a União. Os sistemas de certificação operados pela indústria ou outras organizações privadas devem ser excluídos do âmbito de aplicação do regulamento. Contudo, os organismos que operem tais sistemas poderão propor à Comissão que os considere como base para a aprovação de sistemas europeus.

(54) As disposições do presente regulamento devem aplicar-se sem prejuízo da legislação da União que prevê regras específicas em matéria de certificação de produtos e serviços de TIC. Designadamente, o Regulamento Geral sobre a Proteção de Dados ("RGPD") estabelece disposições para a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com esse regulamento. Esses procedimentos de certificação e selos e marcas de proteção de dados devem permitir que os titulares dos dados avaliem rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa. O presente regulamento aplica-se sem prejuízo da certificação das operações de tratamento de dados, nomeadamente quando essas operações estejam integradas em produtos e serviços, ao abrigo do RGPD.

(55) O objetivo dos sistemas europeus de certificação da cibersegurança deve ser garantir que os **processos**, produtos e serviços de TIC certificados ao abrigo desses sistemas cumprem os requisitos especificados [...] **com vista a** [...] **proteger** a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados, transmitidos ou tratados, as funções conexas ou os serviços oferecidos por esses produtos, processos, serviços e sistemas ou acessíveis por via deles **ao longo do respetivo ciclo de vida**, na aceção do presente regulamento. É impossível definir pormenorizadamente no presente regulamento os requisitos de cibersegurança relativos a todos os **processos,** produtos e serviços de TIC. Os **processos,** produtos e serviços de TIC e as necessidades de cibersegurança conexas são de tal forma diversos que é muito difícil apresentar requisitos de cibersegurança globais que sejam genericamente aplicáveis. Por conseguinte, é necessário adotar uma noção lata e geral de cibersegurança para efeitos de certificação, complementada por um conjunto de objetivos de cibersegurança específicos que devem ser tidos em conta durante a conceção dos sistemas europeus de certificação da cibersegurança. As modalidades com as quais esses objetivos serão alcançados em **processos,** produtos e serviços de TIC específicos devem depois ser estabelecidas em pormenor a nível do sistema de certificação individual adotado pela Comissão, nomeadamente mediante referência a normas ou especificações técnicas**, sempre que não estejam disponíveis normas adequadas.**

(55-A) As especificações técnicas a utilizar num sistema europeu de certificação da cibersegurança devem ser identificadas respeitando os princípios estabelecidos no anexo II do Regulamento (UE) 1025/2012. Poderão no entanto ser considerados necessários alguns desvios em relação a estes princípios, 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. Os motivos para os desvios em causa devem ser divulgados ao público.

(55-B) A avaliação certificada da conformidade é o processo destinado a avaliar se foram preenchidos os requisitos especificados para um determinado processo, produto ou serviço de TIC. É realizada por um terceiro independente, que não o fabricante do produto ou o prestador do serviço. A emissão de um certificado é efetuada na sequência da avaliação positiva de um determinado processo, produto ou serviço de TIC. Deve ser considerada como a confirmação de que a respetiva avaliação foi efetuada corretamente. Consoante o nível de garantia, o sistema europeu de cibersegurança deve prever se o certificado é emitido por uma entidade pública ou privada. A avaliação de conformidade e a certificação, por si só, não podem garantir que os produtos e serviços de TIC certificados são ciberseguros. Consistem antes num procedimento e numa metodologia técnica para atestar que os produtos e serviços de TIC foram ensaiados e que cumprem determinados requisitos de cibersegurança estabelecidos noutros diplomas, por exemplo, conforme especificado em normas técnicas.

(55-C) A escolha, pelos utilizadores dos certificados, do nível adequado de certificação e dos requisitos de segurança conexos deve basear-se numa análise do risco de utilização do processo, produto ou serviço de TIC. O nível de garantia deve ser, por conseguinte, proporcional ao nível do risco associado à utilização prevista do processo, produto ou serviço de TIC.

(55-D) Os sistemas europeus de certificação da cibersegurança poderão prever a realização de uma avaliação da conformidade sob a exclusiva responsabilidade do fabricante ou fornecedor de produtos e serviços de TIC (autoavaliação da conformidade). Nesses casos, é suficiente que o próprio fabricante ou fornecedor efetue todos os controlos a fim de garantir a conformidade dos processos, produtos ou serviços de TIC com o sistema de certificação. Este tipo de avaliação da conformidade deve ser considerado adequado para produtos e serviços de TIC de baixa complexidade (por exemplo, com uma conceção e um mecanismo de produção simples) que apresentem um baixo nível de risco para o interesse público. Além disso, apenas os produtos e serviços de TIC correspondentes ao nível de garantia básico poderão vir a ser objeto da autoavaliação da conformidade.

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

(55-F) O fabricante ou fornecedor de produtos e serviços de TIC que realize uma autoavaliação da conformidade deve elaborar e assinar a declaração de conformidade da UE no âmbito do procedimento de avaliação da conformidade. A declaração de conformidade da UE é o documento que atesta que determinado produto ou serviço de TIC preenche os requisitos do sistema. Ao elaborar e assinar a declaração de conformidade da UE, o fabricante ou fornecedor assume a responsabilidade pela conformidade do produto ou serviço de TIC com os requisitos legais do sistema. Deve ser apresentada à autoridade nacional de certificação da cibersegurança e à ENISA uma cópia da declaração de conformidade da UE.

(55-G) O fabricante ou fornecedor de produtos e serviços de TIC deve manter, por um período definido no sistema europeu de certificação da cibersegurança em causa, à disposição da autoridade nacional de certificação da cibersegurança competente a declaração de conformidade [...] da UE e a documentação técnica com todas as informações pertinentes relativas à conformidade dos produtos ou serviços de TIC com um sistema. A documentação técnica deve especificar os requisitos aplicáveis e abranger, na medida em que for relevante para a avaliação, a conceção, o fabrico e o funcionamento do produto ou serviço de TIC. A documentação técnica deve ser compilada de modo a permitir a avaliação da conformidade de um produto ou serviço de TIC com os requisitos pertinentes.

(55-H) Os Estados-Membros e as organizações de partes interessadas devem poder propor ao grupo europeu para a certificação da cibersegurança a elaboração de uma proposta de sistema. As organizações de partes interessadas são organizações de representantes da indústria ou dos consumidores, incluindo representantes das organizações de PME com um interesse justificado no desenvolvimento de um determinado sistema europeu de certificação da cibersegurança. As propostas dos Estados-Membros e das organizações de partes interessadas devem ser examinadas à luz dos critérios definidos pelo grupo europeu para a certificação da cibersegurança, segundo orientações baseadas nos princípios da transparência, abertura, imparcialidade, consenso, eficácia, relevância e coerência.

(56) Devem ser atribuídas competências à Comissão **e ao grupo** para pedir à ENISA que prepare **sem demora injustificada** propostas de sistemas destinados a **processos**, produtos ou serviços de TIC específicos. Devem ser atribuídas competências à Comissão para adotar, com base na proposta de sistema apresentada 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 devem especificar um conjunto mínimo de elementos relativos ao objeto, âmbito de aplicação e funcionamento do sistema individual. Os mesmos devem incluir, entre outros, o âmbito de aplicação e objeto da certificação da cibersegurança, designadamente as categorias de **processos,** produtos e serviços 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 métodos de avaliação, bem como o nível previsto de garantia (básico, substancial e/ou elevado) **e os níveis de avaliação, se for caso disso**.

(56-A) A garantia dada por um sistema europeu de certificação é o motivo para confiar em que um processo, 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 quadro que rege os processos, produtos e serviços de TIC certificados, um sistema europeu de certificação da cibersegurança poderá especificar níveis de garantia para os certificados europeus de cibersegurança e as declarações de conformidade da UE emitidos ao abrigo desse mesmo sistema. Cada certificado poderá corresponder a um dos níveis de garantia – básico, substancial ou elevado –, ao passo que a declaração de conformidade da UE apenas poderá corresponder ao nível de garantia básico. Os níveis de garantia determinam o nível de esforço necessário para [...] a avaliação e caracterizam-se por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é mitigar ou prevenir incidentes de cibersegurança. Cada nível de garantia deve ser coerente entre os diferentes domínios setoriais nos quais é aplicada a certificação.

(56-B) Um sistema europeu de certificação da cibersegurança poderá especificar vários níveis de avaliação em função do rigor e alcance da metodologia de avaliação utilizada, que deve corresponder a um dos níveis de garantia e estar associada a uma combinação adequada de componentes de garantia. Para todos os níveis de garantia, o produto ou serviço de TIC deve conter um conjunto de funcionalidades de segurança, tal como definidas 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/amontoadas *stack*/*heap*. Estas funcionalidades devem ser elaboradas e mantidas seguindo abordagens de desenvolvimento centradas na segurança e utilizando as ferramentas conexas, para assegurar que são incorporados mecanismos eficazes (tanto de *software* como de *hardware*) de forma fiável. Para o nível de garantia básico, a avaliação deve ser orientada, no mínimo, pelos seguintes componentes de garantia: a avaliação deve incluir, pelo menos, uma análise da documentação técnica do produto ou serviço 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 ou serviço de TIC também deve ser objeto de análise técnica. Nos casos em que um sistema europeu de certificação da cibersegurança preveja uma autoavaliação da conformidade, deve ser suficiente que o fabricante ou fornecedor realize uma autoavaliação sobre a conformidade dos processos, produtos ou serviços de TIC com o sistema de certificação. Para o nível de garantia substancial, a avaliação deve, para além do nível de garantia básico, ser orientada, pelo menos, pela verificação da conformidade das funcionalidades de segurança do produto ou serviço de TIC com a respetiva documentação técnica. Para o nível de garantia elevado, a avaliação deve, para além do nível de garantia substancial, ser orientada, pelo menos, por um ensaio de eficiência que avalie a resistência das funcionalidades de segurança do produto ou serviço de TIC contra atores com competências e recursos significativos que levem a cabo ciberataques elaborados.

(56-C) Ao elaborar uma proposta de sistema, a ENISA deve consultar todas as partes interessadas relevantes, tais como as organizações europeias de normalização, as autoridades nacionais competentes, as organizações baseadas em acordos de reconhecimento mútuo, designadamente o ARM do SOG-IS, as PME, as organizações de consumidores, bem como as partes interessadas ambientais e sociais.

(56-D) A ENISA deve manter um sítio Web para disponibilizar informações sobre os sistemas europeus de certificação da cibersegurança e publicitá-los, o qual deve incluir, nomeadamente, os pedidos de elaboração de uma proposta de sistema europeu de certificação da cibersegurança e as informações recebidas durante o processo de consulta realizado pela ENISA durante a fase de elaboração. Esse sítio Web deve igualmente disponibilizar informações sobre os certificados e as declarações de conformidade da UE emitidos nos termos do presente regulamento.

(57) O recurso à certificação europeia da cibersegurança **e à declaração de conformidade da UE** deve manter-se voluntário, salvo disposição em contrário na legislação da União ou nacional **adotada nos termos do direito da União**. **Na ausência de legislação harmonizada, os Estados-Membros podem adotar regulamentação técnica nacional, em conformidade com a Diretiva (UE) 2015/1535, que preveja a certificação obrigatória nos termos de um sistema europeu de certificação da cibersegurança. Os Estados-Membros poderão recorrer também à certificação europeia da cibersegurança no contexto da adjudicação de contratos públicos e da Diretiva 2014/24/UE.** [...]

(57-A) 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 e serviços de TIC abrangidos por um sistema europeu de certificação da cibersegurança devem cessar de produzir efeitos a contar da data estipulada pela Comissão por meio do ato de execução. Além disso, os Estados-Membros não devem introduzir novos sistemas nacionais de certificação que incluam sistemas de certificação da cibersegurança de produtos e serviços de TIC já abrangidos por um sistema europeu de certificação da cibersegurança existente. No entanto, os Estados-Membros não devem ser impedidos de adotar ou manter sistemas nacionais de certificação para efeitos de segurança nacional.

(58) Assim que um sistema europeu de certificação da cibersegurança for adotado, os fabricantes de produtos de TIC ou os prestadores de serviços de TIC devem poder apresentar uma candidatura para a certificação dos seus produtos ou serviços a um organismo de avaliação da conformidade da sua escolha. Os organismos de avaliação da conformidade devem ser acreditados por um organismo de acreditação se cumprirem determinados requisitos estabelecidos no presente regulamento. A acreditação deve ser emitida por um período máximo de cinco anos e pode ser renovada nas mesmas condições, desde que o organismo de avaliação da conformidade cumpra os requisitos. Os organismos de acreditação devem **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 violem o presente regulamento.

(59) **[...]** Os Estados-Membros **[...] devem** designar uma **ou mais** autoridades de [...] certificação da cibersegurança para supervisionar o cumprimento **das obrigações decorrentes do presente regulamento. Caso um Estado-Membro o considere adequado, essas atribuições podem igualmente ser conferidas a autoridades já existentes. Os Estados--Membros devem também poder decidir, por acordo mútuo com outro Estado--Membro, designar uma ou mais autoridades supervisoras no território desse outro Estado-Membro. A autoridade deve, nomeadamente, controlar e fazer cumprir as obrigações dos fabricantes ou fornecedores de produtos e serviços de TIC estabelecidos no respetivo território, no que respeita à declaração de conformidade da UE, prestar assistência aos organismos nacionais de acreditação no controlo e supervisão das atividades dos organismos de avaliação da conformidade, disponibilizando-lhes conhecimentos especializados e informações pertinentes, autorizar os organismos de avaliação da conformidade a exercer as suas atribuições sempre que preencham os requisitos adicionais estabelecidos no sistema e acompanhar os desenvolvimentos pertinentes no domínio da certificação da cibersegurança** [...]. As autoridades [...] nacionais de certificação da **cibersegurança** devem tratar as reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados **por elas emitidos ou os certificados emitidos por organismos de avaliação da conformidade com nível de garantia elevado** [...], investigar, tanto quanto for necessário, o conteúdo 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, incluindo pela partilha de informações sobre a eventual não conformidade de produtos e serviços de TIC com os requisitos do presente regulamento ou de sistemas de certificação da cibersegurança específicos.

(60) Com vista a assegurar a aplicação consistente do quadro europeu de certificação da cibersegurança, deve ser criado um grupo europeu para a certificação da cibersegurança ("grupo") composto por **representantes das** autoridades nacionais de certificação [...] **da cibersegurança ou outras autoridades nacionais competentes**. As principais atribuições do grupo devem ser: aconselhar e assistir a Comissão no seu trabalho, a fim de assegurar uma execução e uma aplicação coerentes do quadro europeu de certificação da cibersegurança; assistir e cooperar estreitamente com a Agência na preparação de propostas de sistemas de certificação da cibersegurança; recomendar que a Comissão peça à Agência que prepare uma proposta de sistema europeu de certificação da cibersegurança; adotar pareceres dirigidos **à Agencia relacionados com as propostas de sistemas e dirigidos** à Comissão relacionados com a manutenção e revisão dos sistemas europeus de certificação da cibersegurança existentes.

(60-A) O grupo deve facilitar o intercâmbio de boas práticas e conhecimentos especializados entre as autoridades nacionais de certificação da cibersegurança responsáveis pela autorização dos organismos de avaliação da conformidade e pela emissão de certificados. O grupo deve apoiar o desenvolvimento de um mecanismo de revisão pelos pares no contexto da elaboração de uma proposta de sistema e da sua implementação para os organismos que emitem certificados europeus de cibersegurança para o nível de garantia elevado. Tais revisões pelos pares devem, em particular, avaliar se os organismos em causa dispõem dos conhecimentos especializados adequados e exercem as suas atribuições de forma harmonizada. Os resultados das revisões pelos pares devem ser disponibilizados ao público. Os organismos em causa poderão adotar medidas adequadas para adaptar as suas práticas e conhecimentos especializados.

(61) A fim de sensibilizar para os futuros sistemas de cibersegurança da UE e de facilitar a sua aceitação, a Comissão Europeia poderá 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 e serviços de TIC certificados.

(61-A) A fim de facilitar mais o comércio e reconhecendo que as cadeias de abastecimento de TIC são mundiais, podem ser celebrados pela União, em conformidade com o artigo 218.º do TFUE, acordos de reconhecimento mútuo relativos aos certificados emitidos por sistemas de certificação criados no contexto do quadro europeu de certificação da cibersegurança. A Comissão, tendo em conta o aconselhamento prestado pela ENISA e pelo grupo europeu para a certificação da cibersegurança, pode recomendar a abertura de negociações pertinentes. Cada sistema deve prever condições específicas de reconhecimento mútuo com países terceiros.

(62) [...]

(63) [...]

(64) A fim de assegurar condições uniformes para a execução do presente regulamento, devem ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento. Essas competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011.

(65) O procedimento de exame deve ser seguido no que concerne a adoção de atos de execução relativos: aos sistemas europeus de certificação da cibersegurança de produtos e serviços de TIC; às modalidades para realização de **inquéritos** por parte da Agência; às circunstâncias, aos formatos e aos procedimentos de notificação de organismos de avaliação da conformidade acreditados pelas autoridades nacionais de certificação [...] **da cibersegurança** à Comissão.

(66) As atividades da Agência devem ser avaliadas de forma independente. A avaliação deve ter em consideração a consecução dos objetivos por parte da Agência, os seus métodos de trabalho e a pertinência das suas atribuições. A avaliação deve também avaliar o impacto, a eficácia e a eficiência do quadro europeu de certificação da cibersegurança.

(67) O Regulamento (UE) n.º 526/2013 deve ser revogado.

(68) Atendendo a que os objetivos do presente regulamento não podem ser suficientemente alcançados pelos Estados-Membros, mas podem ser mais bem alcançados a nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo,

ADOTARAM O PRESENTE REGULAMENTO:

TÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e âmbito de aplicação

1. Com vista a assegurar o normal funcionamento do mercado interno e a alcançar, em simultâneo, 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, a "Agência da União Europeia para a Cibersegurança", a seguir designada por "Agência"; e

b) Um quadro para o estabelecimento de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança de **processos,** produtos e serviços de TIC na União. Este quadro é aplicável sem prejuízo de disposições específicas em matéria de certificação de caráter voluntário ou obrigatório constantes de outros atos da União.

2. **O presente regulamento não prejudica as competências dos Estados-Membros em matéria de cibersegurança nem, em caso algum, as 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 as pessoas afetadas;

2) "Rede e sistema de informação": um sistema 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": um enquadramento na aceção do artigo 4.º, ponto 3, da Diretiva (UE) 2016/1148;

4) "Operador de serviços essenciais": uma entidade pública ou privada na aceção do artigo 4.º, ponto 4, da Diretiva (UE) 2016/1148;

5) "Prestador de serviços digitais": uma pessoa coletiva que presta um serviço digital na aceção do artigo 4.º, ponto 6, da Diretiva (UE) 2016/1148;

6) "Incidente": um evento na aceção do artigo 4.º, ponto 7, da Diretiva (UE) 2016/1148;

7) "Tratamento de incidentes": um procedimento na aceção do artigo 4.º, ponto 8, da Diretiva (UE) 2016/1148;

8) "Ciberameaça": uma potencial circunstância ou evento que possa **prejudicar, perturbar ou** afetar negativamente **de qualquer outra forma** as redes e os sistemas de informação, os seus utilizadores e as pessoas afetadas.

9) "Sistema europeu de certificação da cibersegurança": o conjunto abrangente de regras, requisitos técnicos, normas e procedimentos definidos a nível da União e aplicáveis à certificação **ou à avaliação da conformidade** de **processos,** produtos e serviços de tecnologias da informação e comunicação (TIC) abrangidos pelo âmbito de aplicação desse sistema específico;

9-A) "Sistema nacional de certificação da cibersegurança": um conjunto abrangente de regras, requisitos técnicos, normas e procedimentos desenvolvidos e adotados por uma autoridade pública nacional aplicáveis à certificação ou à avaliação da conformidade de processos, produtos e serviços de TIC abrangidos pelo âmbito de aplicação desse sistema específico;

10) "Certificado europeu de cibersegurança": um documento [...] que ateste que um determinado **processo,** produto ou serviço de TIC [...] **foi avaliado para determinar a sua conformidade com** requisitos **de segurança** específicos estabelecidos por um sistema europeu de certificação da cibersegurança;

11) "Produto [...] de TIC": um elemento ou grupo de elementos de redes e sistemas de informação;

11-A) "Serviço de TIC": um serviço que consista total ou principalmente na transmissão, no armazenamento, na extração ou no tratamento de informações por meio de redes e sistemas de informação;

11-B) "Processo de TIC": um conjunto de atividades realizadas com o intuito de conceber, desenvolver, oferecer e manter um produto ou serviço de TIC;

12) "Acreditação": a acreditação na aceção do artigo 2.º, ponto 10, do Regulamento (CE) n.º 765/2008;

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

14) "Avaliação da conformidade": a avaliação da conformidade na aceção do artigo 2.º, ponto 12, do Regulamento (CE) n.º 765/2008;

15) "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;

16) "Norma": uma norma na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 1025/2012**;**

16-A) "Especificação técnica": um documento que define os requisitos técnicos a satisfazer por um processo, produto ou serviço de TIC;

16-B) "Nível de garantia": um motivo para confiar em que um processo, produto ou serviço de TIC cumpre os requisitos de segurança de um determinado sistema europeu de certificação da cibersegurança e que indica a que nível esse processo, produto ou serviço de TIC foi avaliado; o nível de garantia não mede a segurança de um processo, produto ou serviço de TIC em si mesmo.

TÍTULO II

ENISA – a "*Agência da União Europeia para a Cibersegurança*"

CAPÍTULO I

MANDATO E */.../* OBJETIVOS */.../*

Artigo 3.º

Mandato

1. A Agência exerce as atribuições que lhe são conferidas pelo presente regulamento com o objetivo de contribuir para um elevado nível de cibersegurança [...] **em toda a** União, **particularmente através do apoio aos Estados-Membros e às instituições, agências e organismos da União para reforçar a cibersegurança**. **A Agência atua como um ponto de referência para as instituições, agências e organismos da União no que se refere ao aconselhamento e aos conhecimentos especializados sobre cibersegurança.**

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

2-A. No exercício das suas atribuições, a Agência atua de forma independente e tem em máxima conta os conhecimentos especializados nacionais das autoridades competentes dos Estados-Membros, evitando, ao mesmo tempo, a duplicação de atividades.

3. [...]

Artigo 4.º

Objetivos

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

2. A Agência presta assistência às instituições, agências e organismos da União, bem como aos Estados-Membros, na elaboração e execução de políticas **da União** relacionadas com a cibersegurança, **incluindo políticas setoriais sobre cibersegurança**.

3. A Agência apoia o reforço das capacidades e do grau de preparação em toda a União, prestando assistência às **instituições, agências e organismos** da União, **bem como** aos Estados-Membros e às partes interessadas públicas e privadas a fim de aumentar a proteção das suas redes e sistemas de informação, desenvolver e **melhorar a ciber-resiliência e as capacidades de resposta e desenvolver** capacidades e competências no domínio da cibersegurança [...].

4. A Agência promove a cooperação e a coordenação a nível da União entre os Estados-Membros, as instituições, agências e organismos da União, e as partes interessadas [...] **públicas e privadas pertinentes**, em questões relacionadas com a cibersegurança.

5. A Agência **contribui para aumentar** [...] as capacidades em matéria de cibersegurança a nível da União a fim de [...] **prestar assistência** aos Estados-Membros na prevenção e resposta a ciberameaças, nomeadamente em caso de incidentes transfronteiriços.

6. A Agência promove o recurso à certificação, **com vista a evitar a fragmentação dos sistemas de certificação na UE. Em particular, a Agência contribui** [...] para a criação e a manutenção de um quadro de certificação da cibersegurança a nível da União em conformidade com o título III do presente regulamento, com vista a aumentar a transparência da garantia de cibersegurança de produtos e serviços de TIC e, por conseguinte, reforçar a confiança no mercado interno digital.

7. A Agência promove um elevado nível de sensibilização dos cidadãos e das empresas para as questões relacionadas com a cibersegurança.

CAPÍTULO I-A
ATRIBUIÇÕES

Artigo 5.º

[...] ***Elaboração e a execução da política e do direito da União***

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

1. Prestando assistência e aconselhamento, nomeadamente emitindo pareceres independentes e realizando trabalhos preparatórios relativos à elaboração e à revisão da política e do direito da União no domínio da cibersegurança, bem como de iniciativas legislativas e políticas setoriais que envolvam questões relacionadas com a cibersegurança;

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, incluindo por meio de pareceres, orientações, aconselhamento e divulgação de boas práticas sobre questões como a gestão dos riscos, a comunicação de incidentes e a partilha de informações, bem como facilitando o intercâmbio de boas práticas entre as autoridades competentes neste domínio;

3. Contribuindo para os trabalhos do grupo de cooperação, em conformidade com o artigo 11.º da Diretiva (UE) 2016/1148, fornecendo conhecimentos especializados e assistência;

4. Apoiando:

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

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

5. Apoiando a análise periódica das atividades políticas da União, fornecendo um relatório anual sobre o estado de execução do respetivo quadro jurídico, no que diz respeito:

   a) Às notificações de incidentes nos Estados-Membros que os pontos únicos de contacto apresentaram ao grupo de cooperação, em conformidade com o artigo 10.º, n.º 3, da Diretiva (UE) 2016/1148;

   b) Às notificações de violações da segurança e de perda de integridade relativas aos prestadores de serviços de confiança que as entidades supervisoras forneceram à Agência, em conformidade com o artigo 19.º, n.º 3, do Regulamento (UE) n.º 910/2014;

   c) Às notificações de [...] **incidentes de** segurança transmitidas pelas empresas que disponibilizam redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público que as autoridades competentes forneceram à Agência, em conformidade com o artigo 40.º da [diretiva que estabelece o Código Europeu das Comunicações Eletrónicas].

Artigo 6.º

[...] ***Reforço das capacidades***

1. A Agência presta assistência:

a) Aos Estados-Membros, nos seus esforços para melhorar a prevenção, a deteção e a análise de [...] **ciberameaças** e incidentes de cibersegurança e a sua capacidade de resposta aos mesmos, fornecendo-lhes os conhecimentos especializados necessários;

b) Às instituições, [...] agências **e organismos** da União, nos seus esforços para melhorar a prevenção, a deteção e a análise de [...] **ciberameaças** e incidentes de cibersegurança e a sua capacidade de resposta aos mesmos, **em particular** por meio do apoio adequado às equipas de resposta a emergências informáticas para as instituições, agências e organismos da União (CERT-UE);

c) Aos Estados-Membros, a seu pedido, no desenvolvimento de equipas nacionais de resposta a incidentes de segurança informática (CSIRT), em conformidade com o artigo 9.º, n.º 5, da Diretiva (UE) 2016/1148;

d) Aos Estados-Membros, a seu pedido, no desenvolvimento de estratégias nacionais de segurança das redes e dos sistemas de informação, em conformidade com o artigo 7.º, n.º 2, da Diretiva (UE) 2016/1148. A Agência também favorece a divulgação e **acompanha [...] a** execução dessas estratégias em toda a União, a fim de promover as melhores práticas;

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

f) Às CSIRT nacionais e da União, aumentando o 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;

g) Aos Estados-Membros, organizando **regularmente** [...] os exercícios de cibersegurança [...] a nível da União a que se refere o artigo 7.º, n.º 6, e emitindo recomendações políticas com base no processo de avaliação dos exercícios e das lições tiradas dos mesmos;

h) Aos organismos públicos competentes, disponibilizando formação em matéria de cibersegurança, se for caso disso, em cooperação com as partes interessadas;

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

2. A Agência **apoia a partilha de informações nos setores e entre eles** [...], em particular nos setores enumerados no anexo II da Diretiva (UE) 2016/1148, divulgando boas práticas e orientações sobre os instrumentos disponíveis e os procedimentos, bem como sobre a resolução de questões regulamentares relativas à partilha de informações.

Artigo 7.º

[...] ***Cooperação operacional a nível da União***

1. A Agência apoia a cooperação operacional entre **os Estados-Membros, as instituições, agências e** organismos [...] **da União** e as partes interessadas.

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

a) O intercâmbio de competências técnicas e de boas práticas,

b) A prestação de aconselhamento e de orientações sobre questões pertinentes relacionadas com a cibersegurança;

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

3. A Agência assegura os serviços de secretariado da rede de CSIRT, em conformidade com o artigo 12.º, n.º 2, da Diretiva (UE) 2016/1148, e, **nessa qualidade,** [...] facilita a partilha de informações e a cooperação entre os seus membros.

4. A Agência **apoia** [...] a cooperação operacional no âmbito da rede de CSIRT, prestando apoio aos Estados-Membros **a seu pedido**, nomeadamente:

a) Aconselhando-os sobre a forma de melhorar as suas capacidades de prevenção, deteção e resposta a incidentes;

b) [...] **Facilitando o tratamento** técnico [...] de incidentes com um impacto significativo ou substancial, **em particular, através do apoio à partilha voluntária de soluções técnicas entre Estados-Membros**;

c) Analisando vulnerabilidades [...] e incidentes**;**

c-A) Prestando apoio aos inquéritos técnicos *ex post* relativos a incidentes com um impacto significativo ou substancial nos termos da Diretiva (UE) 2016/1148.

No exercício destas atribuições, a Agência e a CERT-UE encetam uma cooperação estruturada, de modo a beneficiar de sinergias **e a evitar a duplicação de atividades** [...].

5. [...]

[...]

6. A Agência organiza **regularmente** [...] exercícios de cibersegurança a nível da União, e apoia, a seu pedido, os Estados-Membros e as instituições, agências e organismos da UE na organização de exercícios. **Tais exercícios a nível da União podem incluir elementos técnicos, operacionais ou estratégicos** [...]. **De dois em dois anos, é organizado um exercício em larga escala que inclui todos esses elementos.** A Agência contribui também, se for caso disso, para exercícios de cibersegurança setoriais e ajuda a organizá-los, juntamente com [...] **as organizações competentes que podem também** participar [...] nos exercícios de cibersegurança a nível da União.

7. A Agência**, em estreita colaboração com os Estados-Membros,** elabora regularmente um relatório sobre a situação técnica da cibersegurança na UE quanto a incidentes e ameaças, baseando-se em informações de fonte aberta, nas suas próprias análises e em relatórios partilhados, entre outros: pelas CSIRT dos Estados-Membros [...] ou pelos pontos únicos de contacto da Diretiva SRI (**ambos numa base voluntária** [...]), pelo Centro Europeu da Cibercriminalidade (EC3) da Europol e pela CERT-UE.

8. A Agência contribui para desenvolver 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 relatórios provenientes de fontes nacionais **partilhados numa base voluntária**, com vista a contribuir para estabelecer um conhecimento comum da situação;

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

c) [...] **Mediante pedido dos Estados-Membros, facilitando** o tratamento técnico de um incidente ou crise, **em particular**, [...] **através do apoio** à partilha **voluntária** de soluções técnicas entre Estados-Membros;

d) Apoiando as **instituições, agências e organismos da UE e, mediante pedido, os Estados-Membros na** comunicação pública relativa a incidentes ou crises;

e) **Apoiando os Estados-Membros, a pedido dos mesmos, no ensaio** [...] dos planos de cooperação destinados a responder a esses incidentes ou crises.

Artigo 8.º

*[...] **Mercado, certificação da cibersegurança e normalização***

A Agência:

a) Apoia e promove a elaboração e a execução da política da União em matéria de certificação da cibersegurança de **processos,** produtos e serviços de TIC, tal como estabelecido no título III do presente regulamento:

1) Elaborando propostas de sistemas europeus de certificação da cibersegurança de **processos,** produtos e serviços de TIC, em **cooperação com a indústria e em** conformidade com o artigo 44.º do presente regulamento;

2) Prestando assistência à Comissão, ao assegurar os serviços de secretariado do grupo europeu para a certificação da cibersegurança, em conformidade com o artigo 53.º do presente regulamento;

3) Compilando e publicando orientações e desenvolvendo boas práticas em matéria de requisitos de cibersegurança de produtos e serviços de TIC, em cooperação com as autoridades nacionais [...] de certificação **da cibersegurança** e a indústria;

3-A) Recomendando especificações técnicas adequadas para o recurso ao desenvolvimento de sistemas europeus de certificação da cibersegurança, tal como referido no artigo 47.º, n.º 1, alínea b), nos casos em que não estejam disponíveis normas;

3-B) Contribuindo para um reforço de capacidades suficiente relacionado com os processos de avaliação e certificação através da compilação e publicação de orientações e da prestação de apoio aos Estados-Membros, mediante pedido dos mesmos;

b) Facilita a elaboração e a adoção de normas europeias e internacionais em matéria de gestão dos riscos e de segurança dos **processos,** produtos e serviços [...] de TIC**;**

b-A) Elabora, em colaboração com os Estados-Membros, recomendações e orientações relativas aos domínios técnicos relacionados com os requisitos de segurança para os operadores de serviços essenciais e os prestadores de serviços digitais, bem como relativas a normas já existentes, incluindo normas nacionais dos Estados-Membros, em conformidade com o artigo 19.º, n.º 2, da Diretiva (UE) 2016/1148;

c) Analisa periodicamente as principais tendências do mercado da cibersegurança, tanto na perspetiva da oferta como da procura, e divulga os seus resultados com vista à promoção do mercado da cibersegurança na União.

Artigo 9.º

[...] ***Conhecimento*** *e* [...] ***informação*** [...]

A Agência:

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

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

c) Fornece, em cooperação com peritos das autoridades dos Estados-Membros, recomendações, orientações e boas práticas para a segurança das redes e 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) Reúne, organiza e disponibiliza ao público, por intermédio de um portal dedicado, informações sobre cibersegurança fornecidas pelas instituições, agências e organismos da União **e, numa base voluntária, pelos Estados-Membros e pelas partes interessadas privadas e públicas**;

e) [...]

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

g) [...]

Artigo 9.º-A

Sensibilização e educação

A Agência:

a) Sensibiliza o público para os riscos de cibersegurança, e fornece orientações sobre boas práticas para utilizadores individuais destinadas aos cidadãos e às organizações;

b) Organiza, em cooperação com os Estados-Membros, as instituições, agências e organismos da União e a indústria, campanhas de sensibilização periódicas, a fim de aumentar a cibersegurança e a sua visibilidade na União;

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

d) Apoia uma coordenação mais estreita e o intercâmbio de boas práticas entre os Estados-Membros em matéria de educação e sensibilização para a cibersegurança facilitando a criação e manutenção de uma rede de pontos de contacto nacionais em matéria de educação.

Artigo 10.º

[...] ***Investigação e inovação***

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

a) Presta aconselhamento à 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 ameaças atuais e emergentes, nomeadamente no que respeita às tecnologias de informação e comunicação novas e emergentes, e utilizar de forma eficaz as tecnologias de prevenção dos riscos;

b) Participa, se a Comissão nela delegar as competências necessárias para tal, na fase de execução de programas de financiamento da investigação e inovação ou é beneficiária dos mesmos.

Artigo 11.º

[...] ***Cooperação internacional***

A Agência contribui para os esforços de cooperação da União com países terceiros e organizações internacionais para promover a cooperação internacional em matéria de cibersegurança:

a) Implicando-se, se adequado, como observador na organização de exercícios internacionais, analisando os resultados desses exercícios e prestando informações sobre os mesmos ao conselho de administração;

b) Facilitando, [...] **nos quadros de cooperação internacional pertinentes,** o intercâmbio de boas práticas [...];

c) Disponibilizando, mediante pedido, conhecimentos especializados à Comissão**;**

c-A) Prestando, em colaboração com o grupo europeu para a certificação da cibersegurança criado nos termos do artigo 53.º, aconselhamento e apoio à Comissão sobre questões relacionadas com acordos para o reconhecimento mútuo de certificados de cibersegurança com países terceiros.

CAPÍTULO II
ORGANIZAÇÃO DA AGÊNCIA

Artigo 12.º

Estrutura

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

a) Um conselho de administração, que exerce as funções definidas no artigo 14.º;

b) Uma comissão executiva, que exerce as funções definidas no artigo 18.º;

c) Um diretor executivo, que exerce as responsabilidades definidas no artigo 19.º;

d) Um grupo permanente de partes interessadas, que exerce as funções definidas no artigo 20.º**;**

d-A) Uma rede de agentes de ligação nacionais, que exerce as funções definidas no artigo 20.º-A.

SECÇÃO 1
CONSELHO DE ADMINISTRAÇÃO

Artigo 13.º

Composição do conselho de administração

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

2. Cada membro do conselho de administração tem um suplente que o representa 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 competências de gestão, administrativas e orçamentais relevantes. A Comissão e os Estados-Membros procurarão 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 procurarão assegurar uma representação equilibrada entre homens e mulheres no conselho de administração.

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

Artigo 14.º

Funções do conselho de administração

1. Compete ao conselho de administração:

a) Definir a orientação geral das atividades da Agência e assegurar que esta trabalhe de acordo com as regras e os princípios estabelecidos no presente regulamento. Compete-lhe igualmente assegurar a coerência do trabalho da Agência com as atividades realizadas pelos Estados-Membros, assim como a nível da União;

b) Adotar o projeto de documento único de programação da Agência a que se refere o artigo 21.º, antes de este ser apresentado à Comissão para que emita o seu parecer;

c) Adotar, tendo em conta o parecer da Comissão, o documento único de programação da Agência, por maioria de dois terços dos membros e em conformidade com o artigo 17.º;

c-A) Supervisionar a execução da programação anual e plurianual incluída no documento único de programação;

d) Adotar, por maioria de dois terços dos membros, o orçamento anual da Agência e exercer outras funções respeitantes ao orçamento, de acordo com o capítulo III;

e) Avaliar e adotar o relatório anual consolidado sobre as atividades da Agência e enviar esse relatório e respetiva avaliação, até 1 de julho do ano seguinte, ao Parlamento Europeu, ao Conselho, à Comissão e ao Tribunal de Contas. O relatório anual inclui as contas e descreve como a Agência cumpriu os seus indicadores de desempenho. O relatório é tornado público;

f) Adotar as regras financeiras aplicáveis à Agência, em conformidade com o artigo 29.º;

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

h) Adotar normas de prevenção e gestão de conflitos de interesses relativamente aos seus membros;

i) 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 internos ou externos;

j) Adotar o respetivo regulamento interno;

k) Exercer, de acordo com o disposto no n.º 2, em relação ao pessoal da Agência, os poderes atribuídos pelo Estatuto dos Funcionários da União Europeia à entidade competente para proceder a nomeações e pelo Regime Aplicável aos Outros Agentes da União Europeia à autoridade investida do poder de celebrar contratos ("poderes da autoridade investida do poder de nomeação");

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

m) Nomear o diretor executivo e, sendo caso disso, prorrogar o seu mandato ou exonerá-lo, em conformidade com o artigo 33.º do presente regulamento;

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

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

p) Autorizar a celebração de acordos de cooperação, em conformidade com os artigos 7.º e 39.º.

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

3. Se circunstâncias excecionais assim o impuserem, o conselho de administração pode, mediante a adoção de uma decisão, 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 que não o diretor executivo.

Artigo 15.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, por um período de quatro anos, 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 expiram automaticamente na mesma data. O vice-presidente substitui automaticamente o presidente na sua falta ou impedimento.

Artigo 16.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 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, sem direito a voto.

4. Os membros do grupo permanente de partes interessadas podem participar, a convite do presidente, nas reuniões do conselho de administração, sem direito a voto.

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

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

Artigo 17.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, bem como para a prorrogação do seu mandato ou para a sua exoneração.

3. Cada membro dispõe de um voto. Em caso de ausência de um membro, o seu suplente pode exercer o respetivo direito de voto.

4. O presidente participa na votação.

5. O diretor executivo não participa na votação.

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

SECÇÃO 2
COMISSÃO EXECUTIVA

Artigo 18.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 internos e externos.

   c) Prestar assistência e aconselhamento ao diretor executivo, sem prejuízo das responsabilidades a este atribuídas e definidas no artigo 19.º, na execução das decisões do conselho de administração sobre questões administrativas e orçamentais, em conformidade com o artigo 19.º.

3. A comissão executiva é composta por cinco membros nomeados de entre os membros do conselho de administração, entre os quais o presidente do conselho de administração, que pode também presidir à comissão executiva, e um dos representantes da Comissão. 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. Esse 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. [...]

SECÇÃO 3
DIRETOR EXECUTIVO

Artigo 19.º

Responsabilidades do diretor executivo

1. A Agência 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 relatórios ao Parlamento Europeu 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 Agência;

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 Agência**, incluindo a execução do programa de trabalho anual,** e apresentá-lo ao conselho de administração para avaliação e adoção;

f) Preparar um plano de ação para o seguimento das 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 para o seguimento das conclusões dos relatórios das auditorias internas ou externas, assim como dos inquéritos do Organismo Europeu de Luta Antifraude (OLAF), e apresentar relatórios sobre os progressos realizados à Comissão, duas vezes por ano, e, regularmente, ao conselho de administração;

h) Elaborar o projeto de regras financeiras aplicáveis à Agência;

i) Elaborar o projeto de mapa previsional de receitas e despesas da Agência 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 for caso disso, mediante a aplicação de sanções administrativas e financeiras efetivas, proporcionadas e dissuasivas;

k) Elaborar uma estratégia antifraude da Agência 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;

l-A) Manter um diálogo regular com as instituições, agências e organismos da União no que se refere às suas atividades em matéria de cibersegurança para garantir a coerência no desenvolvimento e na aplicação da política da UE;

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

4. Se necessário, e no quadro do mandato e em conformidade com os objetivos e atribuições da Agência, o diretor executivo pode criar grupos de trabalho *ad hoc* compostos por peritos, nomeadamente peritos das autoridades competentes dos Estados-Membros. O conselho de administração deve ser antecipadamente informado do facto. Os procedimentos relativos, nomeadamente, à composição e ao funcionamento dos grupos de trabalho e à nomeação dos peritos que os constituem pelo diretor executivo serão especificados no regulamento interno da Agência.

5. **Se necessário, de modo a assegurar o exercício eficaz e eficiente das atribuições da Agência 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 deve **solicitar o parecer do(s) Estado(s)-Membro(s) em causa, incluindo o Estado-Membro onde se encontra a sede da Agência, e** obter 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 em causa, a questão é levada ao Conselho para debate.** A decisão deve especificar o âmbito das atividades a realizar pela delegação local, de modo a evitar custos desnecessários e a duplicação de funções administrativas da Agência. [...] **O número de membros do pessoal em todas as delegações locais deve ser mantido num nível mínimo e não pode exceder, no total, 40 % do [...] pessoal localizado no Estado-Membro onde se encontra a sede da Agência. O número de membros do pessoal em cada delegação local não pode exceder 10 % do [...] pessoal localizado no Estado-Membro onde se encontra a sede da Agência.**

SECÇÃO 4
GRUPO PERMANENTE DE PARTES INTERESSADAS

Artigo 20.º

Grupo permanente de partes interessadas

1. O conselho de administração, agindo sob proposta do diretor executivo, cria um grupo permanente de partes interessadas composto por peritos reconhecidos que representam as partes interessadas, nomeadamente empresas de TIC, fornecedores de redes ou serviços de comunicações eletrónicas disponibilizados ao público, **operadores de serviços essenciais,** associações de consumidores, peritos académicos no domínio da cibersegurança e representantes das autoridades competentes nacionais notificadas nos termos da [diretiva que estabelece o Código Europeu das Comunicações Eletrónicas] e das autoridades supervisoras responsáveis pela aplicação da lei e pela proteção dos dados.

2. Os procedimentos relativos ao grupo permanente de partes interessadas, nomeadamente quanto à composição e ao número e nomeação dos seus membros pelo conselho de administração, quanto à proposta a apresentar pelo diretor executivo e quanto ao funcionamento do grupo serão especificados no regulamento interno da Agência e tornados públicos.

3. O grupo permanente de partes interessadas é presidido pelo diretor executivo ou por qualquer outra pessoa nomeada, caso a caso, pelo diretor executivo.

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

5. O grupo permanente de partes interessadas aconselha a Agência no exercício das suas atividades. O grupo aconselha, em particular, o diretor executivo na elaboração da proposta de programa de trabalho da Agência, e no que respeita à comunicação com as partes interessadas sobre todas as questões ligadas ao programa de trabalho.

5-A. O grupo permanente de partes interessadas informa regularmente o conselho de administração das suas atividades.

SECÇÃO 4-A
REDE DE AGENTES DE LIGAÇÃO NACIONAIS

Artigo 20.º-A

Rede de agentes de ligação nacionais

1. O conselho de administração, deliberando sob proposta do diretor executivo, cria uma rede de agentes de ligação nacionais composta por representantes dos Estados--Membros.

2. A rede de agentes de ligação nacionais é composta por representantes de todos os Estados-Membros. Cada Estado-Membro nomeia um representante. As reuniões da rede podem realizar-se em diferentes configurações de peritos.

3. Em particular, a rede de agentes de ligação nacionais facilita o intercâmbio de informações entre a ENISA e os Estados-Membros. Apoia, nomeadamente, a ENISA na comunicação das suas atividades, conclusões e recomendações às partes interessadas pertinentes em toda a UE.

4. Os agentes de ligação nacionais servem de pontos de contacto focais a nível nacional para facilitar a cooperação entre a ENISA e os peritos nacionais no contexto da execução do programa de trabalho da ENISA.

5. Ainda que os agentes de ligação nacionais devam cooperar estreitamente com os representantes do conselho de administração dos respetivos países, a rede em si mesma não deve duplicar o trabalho do conselho de administração nem o de outras instâncias da UE.

6. As funções e os procedimentos da rede de agentes de ligação nacionais são especificados no regulamento interno da Agência e tornados públicos.

SECÇÃO 5
FUNCIONAMENTO

Artigo 21.º

Documento único de programação

1. A Agência 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 humanos e financeiros, em conformidade com o artigo 32.º do Regulamento Delegado (UE) n.º 1271/2013 da Comissão[14] 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 envia-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 definitivo após a aprovação final do orçamento geral da União, devendo, se necessário, ser ajustado em conformidade.

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 funções que tenham sido acrescentadas, modificadas ou suprimidas em comparação com o exercício financeiro anterior.

---

[14] 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).

6. O conselho de administração altera o programa de trabalho anual adotado sempre que seja cometida à Agência 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 56.º.

Artigo 22.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 Agência estabelecerá, no seu regulamento interno, as disposições de execução das regras relativas às declarações de interesses referidas nos n.ºs 1 e 2.

Artigo 23.º

Transparência

1. A Agência executa as suas atividades com um elevado nível de transparência e em conformidade com o artigo 25.º.

2. A Agência 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 Agência publica as declarações de interesses feitas nos termos do artigo 22.º.

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

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

Artigo 24.º

Confidencialidade

1. Sem prejuízo do disposto no artigo 25.º, a Agência não divulga a terceiros informações por si tratadas ou recebidas em relação às quais tenha sido apresentado um pedido fundamentado de tratamento confidencial, parcial ou total.

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

3. A Agência estabelecerá, 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 Agência, o conselho de administração autoriza a Agência a tratar informações classificadas. Nesse caso, o conselho de administração adota, de comum acordo com os serviços da Comissão, regras internas de funcionamento que respeitem os princípios de segurança estabelecidos nas Decisões (UE, Euratom) 2015/443[15] e 2015/444[16] da Comissão. Essas regras incluem disposições relativas ao intercâmbio, tratamento e armazenamento de informações classificadas.

---

15 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).

16 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).

Artigo 25.º

Acesso a documentos

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

2. O conselho de administração adota disposições de execução do Regulamento (CE) n.º 1049/2001 no prazo de seis meses a contar da criação da Agência.

3. As decisões tomadas pela Agência 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 III
ELABORAÇÃO E ESTRUTURA DO ORÇAMENTO

Artigo 26.º

Elaboração do orçamento

1. O diretor executivo elabora anualmente um projeto de mapa previsional de receitas e despesas da Agência 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 referido no n.º 1, o mapa previsional de receitas e despesas da Agência para o exercício orçamental seguinte.

3. Até 31 de janeiro de cada ano, o conselho de administração envia o mapa previsional referido no n.º 2, que faz parte do projeto de documento único de programação, à Comissão e aos países terceiros com os quais a União tenha celebrado acordos em conformidade com o artigo 39.º.

4. Com base no referido mapa previsional, a Comissão inscreve no projeto de orçamento da União as previsões que considere necessárias no que respeita ao quadro de pessoal e o montante da subvenção a cargo do orçamento geral, e apresenta-o ao Parlamento Europeu e ao Conselho em conformidade com os artigos 313.º e 314.º do TFUE.

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

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

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

Artigo 27.º

Estrutura do orçamento

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

   a) Uma subvenção do orçamento da União;

   b) Receitas afetadas ao financiamento de despesas específicas, em conformidade com as regras financeiras referidas no artigo 29.º;

   c) Financiamento da União sob a forma de acordos de contribuição ou subvenções *ad hoc*, em conformidade com as regras financeiras referidas no artigo 29.º e com as disposições dos instrumentos relevantes de apoio às políticas da União;

d) Contribuições de países terceiros que participem nos trabalhos da Agência, como previsto no artigo 39.º;

e) Eventuais contribuições voluntárias dos Estados-Membros, em numerário ou em espécie; os Estados-Membros que efetuem contribuições voluntárias não podem reivindicar quaisquer direitos ou serviços específicos em contrapartida dessas contribuições.

2. As despesas da Agência 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 28.º

Execução do orçamento

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

2. O auditor interno da Comissão exerce, em relação à Agência, os mesmos poderes que lhe são conferidos em relação aos serviços da Comissão.

3. Até 1 de março seguinte ao termo de cada exercício financeiro (1 de março do ano N+1), o contabilista da Agência comunica as contas provisórias ao contabilista da Comissão e ao Tribunal de Contas.

4. Depois de receber as observações do Tribunal de Contas sobre as contas provisórias da Agência, o contabilista da Agência elabora as contas definitivas da mesma sob a sua responsabilidade.

5. O diretor executivo apresenta as contas definitivas ao conselho de administração para que emita um parecer.

6. Até 31 de março do ano N+1, o diretor executivo envia 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 transmite as contas definitivas, acompanhadas do parecer do conselho de administração, ao Parlamento Europeu, ao Conselho, ao contabilista da Comissão e ao Tribunal de Contas Europeu.

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

9. O diretor executivo publica as contas definitivas até 15 de novembro do ano seguinte.

10. Até 30 de setembro do ano N+1, o diretor executivo envia uma resposta às observações do Tribunal de Contas 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, tal como previsto no artigo 165.º, n.º 3, do Regulamento Financeiro.

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

Artigo 29.º

Regras financeiras

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

Artigo 30.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[17], a Agência deve aderir, no prazo de seis meses a partir da data em que se tornar operacional, ao Acordo Interinstitucional de 25 de maio de 1999 relativo aos inquéritos internos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF), e 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 ou no local, todos os beneficiários de subvenções, contratantes e subcontratantes que tenham recebido fundos da União por intermédio da Agência.

[17] 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).

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 do Parlamento Europeu e do Conselho e no Regulamento (Euratom, CE) n.º 2185/96 do Conselho[18], 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, a fim de determinar a existência de fraudes, corrupção ou outras atividades ilícitas que afetem os interesses financeiros da União no âmbito de uma subvenção ou de um contrato financiado pela Agência.

4. Sem prejuízo do disposto nos n.ºs 1, 2 e 3, os acordos de cooperação com países terceiros e organizações internacionais, os contratos, as convenções e as decisões de subvenção da Agência devem incluir disposições que confiram expressamente ao Tribunal de Contas e ao OLAF poderes para realizarem essas auditorias e inquéritos, no respeito das respetivas competências.

CAPÍTULO IV
PESSOAL DA AGÊNCIA

Artigo 31.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, aplicam-se ao pessoal da Agência.

---

18 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).

Artigo 32.º

Privilégios e imunidades

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

Artigo 33.º

Diretor executivo

1. O diretor executivo é contratado como agente temporário da Agência, 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 com o diretor executivo, a Agência 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 **quatro** [...] anos. No termo desse período, a Comissão procede a uma avaliação que tenha em conta a avaliação do trabalho realizado pelo diretor executivo e as futuras atribuições e desafios da Agência.

6. O conselho de administração adota as suas decisões sobre a nomeação, a prorrogação do mandato ou a exoneração do diretor executivo por maioria de dois terços dos seus membros com direito de voto.

7. O conselho de administração, deliberando sob 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 não superior a **quatro** [...] 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. Um 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 [...].

Artigo 34.º

Peritos nacionais destacados e outro pessoal

1. A Agência pode recorrer a peritos nacionais destacados ou a outro pessoal não contratado pela Agência. 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 Agência.

CAPÍTULO V
DISPOSIÇÕES GERAIS

Artigo 35.º

Estatuto jurídico da Agência

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

2. A Agência 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 Agência é representada pelo seu diretor executivo.

Artigo 36.º

Responsabilidade da Agência

1. A responsabilidade contratual da Agência 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 Agência.

3. Em matéria de responsabilidade extracontratual, a Agência procede à reparação, de acordo com os princípios gerais comuns às legislações dos Estados-Membros, dos danos causados por si ou pelos seus agentes no exercício das suas funções.

4. O Tribunal de Justiça da União Europeia é competente em qualquer litígio relativo à reparação desses danos.

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

Artigo 37.º

Regime linguístico

1. O Regulamento n.º 1 do Conselho é aplicável à Agência[19]. Os Estados-Membros e os outros organismos por eles designados podem dirigir-se à Agência e receber resposta na língua oficial das instituições da União da sua escolha.

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

Artigo 38.º

Proteção de dados pessoais

1. O tratamento de dados pessoais pela Agência está sujeito às disposições do Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho[20].

2. O conselho de administração adota as disposições de execução a que se refere o artigo 24.º, n.º 8, do Regulamento (CE) n.º 45/2001. O conselho de administração pode adotar medidas adicionais necessárias para a aplicação do Regulamento (CE) n.º 45/2001 pela Agência.

---

19 Regulamento n.º 1 que estabelece o regime linguístico da Comunidade Europeia da Energia Atómica (JO 17 de 6.10.1958, p. 401).

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

Artigo 39.º

Cooperação com países terceiros e organizações internacionais

1. A Agência 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 Agência pode, mediante aprovação prévia da Comissão, estabelecer acordos de cooperação com essas autoridades de países terceiros e organizações internacionais. Esses acordos não podem criar obrigações jurídicas à União e aos seus Estados-Membros.

2. A Agência 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, serão celebrados acordos que determinem, nomeadamente, a natureza, o âmbito e o modo de participação desses países nos trabalhos da Agência, incluindo disposições relativas à participação nas iniciativas desenvolvidas pela Agência, às contribuições financeiras e ao pessoal. No que diz respeito às questões de pessoal, esses acordos devem respeitar, em todo o caso, o Estatuto dos Funcionários.

3. O conselho de administração adota uma estratégia para as relações com países terceiros ou organizações internacionais em matérias nas quais a Agência é competente. A Comissão assegura que a Agência funciona no âmbito do seu mandato e do quadro institucional existente mediante a celebração de um acordo de trabalho adequado com o diretor executivo da agência.

Artigo 40.º

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

A Agência, em consulta com a Comissão, adota regras de segurança próprias que apliquem os princípios de segurança que constam das regras de segurança da Comissão para a proteção das informações classificadas da União Europeia (ICUE) e das informações sensíveis não classificadas, enunciadas nas Decisões (UE, Euratom) 2015/443 e 2015/444 da Comissão. Essas regras abrangem, nomeadamente, disposições relativas ao intercâmbio, ao tratamento e ao armazenamento dessas informações.

Artigo 41.º

Acordo de sede e condições de funcionamento

1. As disposições necessárias relativas às instalações a disponibilizar à Agência 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 Agência e aos membros das suas famílias, são estabelecidas num acordo de sede entre a Agência e o Estado-Membro de acolhimento, celebrado após a aprovação do conselho de administração, no prazo máximo de [2 anos a contar da entrada em vigor do presente regulamento].

2. O Estado-Membro de acolhimento da Agência proporciona [...] condições [...] para assegurar o bom funcionamento da Agência, incluindo a acessibilidade da localização, condições de ensino apropriadas para os filhos dos membros do pessoal e acesso adequado ao mercado de trabalho, à segurança social e a cuidados médicos para os filhos e cônjuges.

Artigo 42.º

Controlo administrativo

As atividades da Agência são supervisionadas pelo Provedor de Justiça Europeu, em conformidade com o artigo 228.º do TFUE.

TÍTULO III
QUADRO DE CERTIFICAÇÃO DA CIBERSEGURANÇA

Artigo 43.º

Quadro [...] europeu de certificação da cibersegurança

1. **É criado o quadro europeu de certificação da cibersegurança, a fim de melhorar as condições de funcionamento do mercado interno aumentando o nível de cibersegurança na União. O quadro estabelece uma governação que possibilita uma abordagem harmonizada dos sistemas europeus de certificação da cibersegurança a nível da UE, com vista a criar um mercado único digital para processos, produtos e serviços de TIC.**

2. **O quadro europeu de certificação da cibersegurança define um mecanismo destinado a criar** [...] sistemas europeus de certificação da cibersegurança [...] **e a** atestar que os **processos,** produtos e serviços de TIC que foram [...] **avaliados** em conformidade com esses sistemas cumprem os requisitos **de segurança** especificados [...] **com vista a proteger** a disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, ou as funções ou serviços oferecidos por esses produtos, processos [...] **e** serviços [...] ou acessíveis por via deles **ao longo do respetivo ciclo de vida**.

Artigo 44.º

Elaboração e adoção de um sistema europeu de certificação da cibersegurança

1. Na sequência de um pedido da Comissão **ou do grupo europeu para a certificação da cibersegurança (a seguir designado por "grupo") criado nos termos do artigo 53.º**, a ENISA elabora uma proposta de sistema europeu de certificação da cibersegurança que cumpra os requisitos estabelecidos nos artigos 45.º, 46.º e 47.º do presente regulamento.

1-A. A elaboração de uma proposta de sistema europeu de certificação da cibersegurança pode ser proposta ao grupo pelos Estados-Membros ou pelas organizações de partes interessadas. O grupo avalia as propostas dos Estados-Membros ou das organizações de partes interessadas em função dos critérios por si definidos nas orientações previstas no artigo 53.º, n.º 3, alínea c-A), e pode solicitar à ENISA que elabore uma proposta de sistema europeu de certificação da cibersegurança.

2. Durante a elaboração das propostas de sistema a que se refere o n.º 1 do presente artigo, a ENISA consulta todas as partes interessadas pertinentes **através de processos de consulta transparentes** e coopera estreitamente com o grupo. O grupo presta à ENISA assistência e aconselhamento especializado [...] no que concerne a elaboração da proposta de sistema **e adota um parecer sobre essa proposta de sistema antes da sua apresentação à Comissão.** [...] **A ENISA assegura que as propostas de sistema são coerentes com a norma harmonizada aplicável utilizada na acreditação do organismo de avaliação da conformidade.**

3. A ENISA **tem em máxima conta o parecer do grupo antes de transmitir** [...] à Comissão a proposta de sistema [...] elaborada em conformidade com o n.º 2 do presente artigo.

4. A Comissão, com base na proposta de sistema apresentada pela ENISA, pode adotar atos de execução, nos termos do artigo 55.º, n.º 2, que estabeleçam sistemas europeus de certificação da cibersegurança de **processos,** produtos e serviços de TIC que cumpram os requisitos estabelecidos nos artigos 45.º, 46.º e 47.º do presente regulamento.

5. [...]

Artigo 44.º-A

Manutenção dos sistemas europeus de certificação da cibersegurança

1. A Agência mantém um sítio Web específico para disponibilizar informações sobre os sistemas europeus de certificação da cibersegurança, os certificados e as declarações de conformidade da UE emitidas nos termos do artigo 47.º-A, bem como para publicitar esses sistemas, certificados e declarações.

2. Pelo menos de cinco em cinco anos, a Agência reanalisa, em estreita colaboração com o grupo, os sistemas europeus de certificação da cibersegurança adotados, tendo em conta as informações recebidas das partes interessadas. Se for considerado necessário, a Comissão ou o Grupo pode solicitar à Agência que dê início ao processo de elaboração de uma proposta de sistema revista, nos termos do artigo 44.º, n.ºs 2 e 3.

Artigo 45.º

Objetivos de segurança dos sistemas europeus de certificação da cibersegurança

Um sistema europeu de certificação da cibersegurança é concebido de modo a [...] **alcançar**, conforme aplicável, **pelo menos** os seguintes objetivos de segurança:

a) Proteger 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 processo, produto ou serviço**;

b) Proteger dados armazenados, transmitidos ou sujeitos a qualquer outro tipo de tratamento contra a destruição, perda ou alteração acidental ou não autorizada [...] **ou a falta de disponibilidade ao longo de todo o ciclo de vida do processo, produto ou serviço**;

c) [...] As pessoas, programas ou máquinas autorizadas poderem aceder exclusivamente aos dados, serviços ou funções abrangidos pelos seus direitos de acesso;

d) Registar que dados, funções ou serviços foram [...] **acedidos, utilizados ou sujeitos a qualquer outro tipo de tratamento**, quando e por quem;

e) [...] Ser possível verificar que dados, serviços ou funções foram acedidos, [...] utilizados **ou sujeitos a qualquer outro tipo de tratamento**, quando e por quem;

f) Restabelecer a disponibilidade e o acesso a dados, serviços e funções de forma atempada, no caso de um incidente físico ou técnico;

g) [...] Os **processos,** produtos e serviços de TIC serem equipados com *software* **e *hardware*** atualizados que não contêm vulnerabilidades **que sejam do conhecimento público** e serem dotados de mecanismos que permitam atualizações seguras [...]**;**

g-A) Os processos, produtos e serviços de TIC serem desenvolvidos, fabricados e fornecidos de acordo com os requisitos de segurança estabelecidos no sistema específico.

Artigo 46.º

Níveis de garantia dos sistemas europeus de certificação da cibersegurança

1. Um sistema europeu de certificação da cibersegurança pode especificar um ou mais dos seguintes níveis de garantia: básico, substancial e/ou elevado, para **processos,** produtos e serviços de TIC. **O nível de garantia é proporcional ao nível do risco associado à utilização prevista do processo, produto ou serviço de TIC.**

2. Os níveis de garantia básico, substancial e elevado [...] **correspondem a um certificado ou uma declaração de conformidade da UE, emitido no âmbito de um sistema europeu de certificação da cibersegurança, que determina, para cada nível de garantia, os respetivos requisitos de segurança, incluindo as funcionalidades de segurança e o nível de esforço necessário para avaliar um processo, produto ou serviço de TIC. O certificado ou a declaração de conformidade da UE caracteriza-se por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é prevenir ou reduzir o risco dos seguintes incidentes de cibersegurança:**

a) **Um certificado europeu de cibersegurança ou uma declaração de conformidade da UE que corresponde a um** nível de garantia **"**básico**" garante que os processos, produtos e serviços de TIC cumprem os respetivos requisitos de segurança, incluindo as funcionalidades de segurança, e que foram avaliados a um nível que visa minimizar os riscos básicos conhecidos de ciberincidentes e ciberataques. As atividades de avaliação incluem, pelo menos, uma análise da documentação técnica; quando tal não for aplicável, incluem atividades alternativas de efeito equivalente** [...];

b) **Um certificado europeu de cibersegurança que corresponde a um** nível de garantia **"**substancial**"** garante **que os processos, produtos e serviços de TIC cumprem os respetivos requisitos de segurança, incluindo as funcionalidades de segurança, e que foram avaliados a um nível que visa minimizar os riscos cibernéticos conhecidos e os ciberincidentes e ciberataques devidos a atores com competências e recursos limitados. As atividades de avaliação incluem, pelo menos: a análise da não aplicabilidade de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para verificar se os processos, produtos ou serviços de TIC aplicam corretamente a funcionalidade de segurança necessária; quando tal não for aplicável, incluem atividades alternativas de efeito equivalente;**

c) **Um certificado europeu de cibersegurança que corresponde a um** nível de garantia **"**elevado**"** [...] garante **que os processos, produtos e serviços de TIC cumprem os respetivos requisitos de segurança, incluindo as funcionalidades de segurança, e que foram avaliados a um nível que visa minimizar os riscos de ciberataques sofisticados perpetrados por atores com competências e recursos significativos. As atividades de avaliação incluem, pelo menos: a análise da não aplicabilidade de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para verificar se os processos, produtos ou serviços de TIC aplicam corretamente a funcionalidade de segurança necessária, ao nível tecnológico mais avançado, e a avaliação da sua resistência a atacantes competentes através de ensaios de penetração; quando tal não for aplicável, incluem atividades alternativas de efeito equivalente.**

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

Artigo 47.º

Elementos dos sistemas europeus de certificação da cibersegurança

1. Um sistema europeu de certificação da cibersegurança inclui**, no mínimo,** os seguintes elementos:

a) Objeto e âmbito **do sistema** de certificação, nomeadamente os tipos ou categorias de **processos,** produtos e serviços de TIC abrangidos**, bem como uma explicação da forma como o sistema de certificação satisfaz as necessidades do grupo-alvo previsto**;

b) [...] Referência às [...] normas internacionais**, europeias ou nacionais seguidas na avaliação**. **Quando não estão disponíveis normas, é feita uma referência a** especificações técnicas **que cumpram os requisitos estabelecidos no anexo II do Regulamento 1025/2012 ou, na ausência das mesmas, a especificações técnicas ou outros requisitos de cibersegurança definidos no sistema;**

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

c-A) Se for caso disso, requisitos específicos ou adicionais aplicáveis aos organismos de avaliação da conformidade, a fim de garantir a sua competência técnica para avaliar os requisitos de cibersegurança;

d) Critérios e métodos de avaliação específicos, nomeadamente os tipos de avaliação, utilizados para demonstrar que os objetivos específicos referidos no artigo 45.º são alcançados;

e) **Se aplicável,** informações necessárias para a certificação que os requerentes devem fornecer **ou disponibilizar de qualquer outra forma** aos organismos de avaliação da conformidade;

f) Condições de utilização de marcas ou rótulos, caso estes estejam previstos pelo sistema;

g) Regras para o controlo da conformidade com os requisitos dos certificados **ou da declaração de conformidade da UE**, incluindo mecanismos para demonstrar a conformidade permanente com os requisitos de cibersegurança especificados [...];

h) **Se aplicável,** condições para a concessão **e a renovação de um certificado**, **bem como para a** manutenção, continuação, alargamento **ou** redução do âmbito da certificação;

i) Regras relativas às consequências da não conformidade de produtos e serviços de TIC certificados **ou objeto de autoavaliação** com os requisitos [...] **do sistema**;

j) Regras relativas ao modo como devem ser comunicadas e tratadas vulnerabilidades de cibersegurança em **processos,** produtos e serviços de TIC não detetadas anteriormente;

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

l) Identificação dos sistemas nacionais **ou internacionais** de certificação da cibersegurança que abranjam os mesmos tipos ou categorias de **processos,** produtos e serviços de TIC**, requisitos de segurança e critérios e métodos de avaliação**;

m) Conteúdo do certificado emitido **ou declaração de conformidade da UE;**

m-A) Período de armazenamento da declaração de conformidade da UE e da documentação técnica com todas as informações pertinentes fornecidas pelo fabricante ou fornecedor de produtos e serviços de TIC;

m-B [...]) Prazo máximo de validade dos certificados;

m-C [...]) Política de divulgação de certificados concedidos, alterados e retirados;

m-D [...]) Condições para o reconhecimento mútuo de sistemas de certificação com países terceiros;

m-E [...]) Se aplicável, regras relativas a um mecanismo de revisão pelos pares para os organismos que emitem certificados europeus de cibersegurança para [...] o nível de garantia elevado nos termos do artigo 48.º, n.º 4-A.

2. Os requisitos especificados do sistema não podem contradizer quaisquer requisitos legais aplicáveis, em especial requisitos decorrentes da legislação harmonizada da União.

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

4. Na ausência de legislação harmonizada da União, a legislação de 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 47.º-A

Autoavaliação da conformidade

1. Os sistemas europeus de certificação da cibersegurança podem permitir a realização de uma avaliação da conformidade sob a exclusiva responsabilidade do fabricante ou fornecedor de produtos e serviços de TIC. Tal avaliação da conformidade é aplicável apenas aos produtos e serviços de TIC de baixo risco correspondentes ao nível de garantia básico.

2. O fabricante ou fornecedor de produtos e serviços de TIC pode emitir uma declaração de conformidade da UE que indique que foi demonstrado o cumprimento dos requisitos estabelecidos no sistema. Ao elaborar tal declaração, o fabricante ou fornecedor de produtos e serviços de TIC assume a responsabilidade pela conformidade do produto ou serviço de TIC com os requisitos estabelecidos no sistema.

3. O fabricante ou fornecedor de produtos e serviços de TIC mantém, por um período definido no sistema europeu de certificação da cibersegurança em causa, à disposição da autoridade nacional de certificação da cibersegurança a que se refere o artigo 50.º, n.º 1, a declaração de conformidade da UE e a documentação técnica com todas as informações pertinentes relativas à conformidade dos produtos ou serviços de TIC com um sistema. É apresentada à autoridade nacional de certificação da cibersegurança e à ENISA uma cópia da declaração de conformidade da UE.

4. A declaração de conformidade da UE é emitida a título voluntário, salvo se especificado em contrário no direito da União ou dos Estados-Membros.

5. As declarações de conformidade da UE emitidas ao abrigo do presente artigo são reconhecidas em todos os Estados-Membros.

Artigo 48.º

Certificação da cibersegurança

1. Os **processos,** produtos e serviços de TIC que tenham sido certificados ao abrigo de um sistema europeu de certificação da cibersegurança adotado nos termos do artigo 44.º são considerados conformes com os requisitos desse sistema.

2. A certificação é voluntária, salvo se especificado em contrário no direito da União **ou dos Estados-Membros**.

3. Os organismos de avaliação da conformidade a que se refere o artigo 51.º emitem um certificado europeu de cibersegurança nos termos do presente artigo**, correspondente ao nível de garantia básico ou substancial**, com base nos critérios incluídos no sistema europeu de certificação da cibersegurança adotado nos termos do artigo 44.º.

4. Em derrogação do n.º 3, em casos devidamente justificados, um determinado sistema europeu **de certificação** da cibersegurança pode prever que o certificado europeu de cibersegurança resultante desse sistema apenas possa ser emitido por um organismo público. Esse organismo [...] será um dos seguintes:

   a) Uma autoridade nacional **de certificação da cibersegurança** [...] a que se refere o artigo 50.º, n.º 1;

   b) Um organismo **público** acreditado como organismo de avaliação da conformidade nos termos do artigo 51.º, n.º 1;

   c) [...]

4-A. Nos casos em que um sistema europeu de certificação da cibersegurança nos termos do artigo 44.º exija um nível de garantia elevado, o certificado só pode ser emitido por uma autoridade nacional de certificação da cibersegurança a que se refere o artigo 50.º, n.º 1, ou, nas condições a seguir indicadas, por um organismo de avaliação da conformidade a que se refere o artigo 51.º:

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

b) Mediante delegação geral prévia desta atribuição pela autoridade nacional de certificação da cibersegurança no organismo de avaliação da conformidade.

5. As pessoas singulares ou coletivas que submetem os seus **processos,** produtos ou serviços de TIC ao processo de certificação [...] **disponibilizam** ao organismo de avaliação da conformidade a que se refere o artigo 51.º **ou à autoridade nacional de certificação da cibersegurança a que se refere o artigo 50.º**, **quando essa autoridade for o organismo que emite o certificado,** todas as informações necessárias para efetuar o procedimento de certificação.

5-A. O titular de um certificado informa o organismo que emite o certificado de quaisquer vulnerabilidades ou irregularidades relativas à segurança do processo, produto ou serviço de TIC certificado detetadas posteriormente, que possam influenciar os requisitos relacionados com a certificação. O organismo transmite essas informações sem demora injustificada à autoridade nacional de certificação da cibersegurança.

6. Os certificados são emitidos [...] **pelo período definido pelo sistema de certificação em causa** e podem ser renovados [...], desde que continuem a ser cumpridos os requisitos pertinentes.

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

Artigo 49.º

Sistemas e certificados nacionais de certificação da cibersegurança

1. Sem prejuízo do disposto no n.º 3, os sistemas nacionais de certificação da cibersegurança e os procedimentos conexos relativos a **processos**, produtos e serviços 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 44.º, n.º 4. Os sistemas nacionais de certificação da cibersegurança e os procedimentos conexos relativos a **processos**, produtos e serviços de TIC não abrangidos por um sistema europeu de certificação da cibersegurança continuam a produzir efeitos.

2. Os Estados-Membros não podem introduzir novos sistemas nacionais de certificação da cibersegurança relativos a **processos,** produtos e serviços 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 expiração.

Artigo 50.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, por acordo mútuo com outro Estado-Membro, designa uma ou mais autoridades 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 [...] designadas e das atribuições que lhes são conferidas**.

3. **Sem prejuízo do disposto no artigo 48.º, n.º 4, alínea a), e n.º 4-A**, 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.

3-A. Os Estados-Membros garantem que as atividades da autoridade nacional de certificação da cibersegurança relacionadas com a emissão de certificados em conformidade com o artigo 48.º, n.º 4, alínea a), e n.º 4-A, respeitam uma separação rigorosa de funções e responsabilidades relativamente às atividades de supervisão previstas no presente artigo, e que as duas atividades são exercidas de forma independente uma da outra.

4. Os Estados-Membros asseguram que as autoridades nacionais [...] de certificação da **cibersegurança** dispõem de recursos adequados ao exercício das suas competências e à realização, de forma eficaz e eficiente, das atribuições que lhes são conferidas.

5. A fim de permitir a execução efetiva do presente regulamento, é conveniente que estas autoridades participem no grupo europeu para a certificação da cibersegurança instituído nos termos do artigo 53.º, de uma forma ativa, eficaz, eficiente e segura.

6. Compete às autoridades nacionais [...] de certificação da **cibersegurança**:

a) [...]

a-A) Controlar e fazer cumprir as obrigações do fabricante ou fornecedor de produtos e serviços de TIC estabelecido nos respetivos territórios definidas no artigo 47.º-A, n.ºs 2 e 3, e no sistema europeu de certificação da cibersegurança correspondente;

b) [...] **Sem prejuízo do disposto no artigo 51.º, n.º 1-B, prestar assistência aos organismos nacionais de acreditação no controlo e supervisão** das atividades dos organismos de avaliação da conformidade para efeitos do presente regulamento [...];

b-A) Controlar e supervisionar as atividades dos organismos a que se refere o artigo 48.º, n.º 4;

b-B) Autorizar os organismos de avaliação da conformidade a que se refere o artigo 51.º, n.º 1-B, e restringir, suspender ou retirar a autorização existente em caso de não conformidade com os requisitos do presente regulamento;

c) Tratar as reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados emitidos pela [...] **autoridade nacional de certificação da cibersegurança ou, em conformidade com o artigo 48.º, n.º 4-A, pelos organismos de avaliação da conformidade**, investigar, tanto quanto for necessário, o conteúdo das reclamações e informar os respetivos autores do andamento e do resultado da investigação num prazo razoável;

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

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

7. 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 de conformidade da UE** que lhe forneçam as informações de que necessite para o desempenho das suas funções;

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 a sua conformidade com o disposto no título III;

c) Tomar as medidas adequadas, em conformidade com o direito nacional, a fim de garantir que os organismos de avaliação da conformidade**,** [...] os titulares de certificados **e os emitentes de declarações de conformidade da UE** estão conformes com o presente regulamento ou com um sistema europeu de certificação da cibersegurança;

d) Obter acesso a todas as instalações dos organismos de avaliação da conformidade e dos titulares de certificados europeus de cibersegurança com o objetivo de conduzir investigações, em conformidade com o direito processual da União ou do respetivo Estado-Membro;

e) Retirar, em conformidade com o direito nacional, os certificados **emitidos pela autoridade nacional de certificação da cibersegurança ou, em conformidade com o artigo 48.º, n.º 4-A, pelos organismos de avaliação da conformidade,** que não estejam em conformidade com o presente regulamento ou um sistema europeu de certificação da cibersegurança;

f) Aplicar sanções, tal como previsto no artigo 54.º, em conformidade com o direito nacional, e exigir a cessação imediata da violação das obrigações estabelecidas no presente regulamento.

8. 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 de **processos,** produtos e serviços de TIC.

Artigo 51.º

Organismos de avaliação da conformidade

1. O organismo nacional de acreditação designado nos termos do Regulamento (CE) n.º 765/2008 só acredita os organismos de avaliação da conformidade se estes cumprirem os requisitos estabelecidos no anexo do presente regulamento.

1-A. Nos casos em que é emitido um certificado europeu de cibersegurança por uma autoridade nacional de certificação da cibersegurança nos termos do artigo 48.º, n.º 4, alínea a), e n.º 4-A, 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.

1-B. Se aplicável, os organismos de avaliação da conformidade são autorizados pela autoridade nacional de certificação da cibersegurança a exercer as atribuições desta última sempre que cumpram os requisitos específicos ou adicionais estabelecidos no sistema europeu de certificação nos termos do artigo 47.º, n.º 1, alínea c-A).

2. A acreditação é emitida por um período máximo de cinco anos e pode ser renovada nas mesmas condições, desde que o organismo de avaliação da conformidade cumpra os requisitos estabelecidos no presente artigo. Os organismos de acreditação **tomam todas as medidas adequadas num prazo razoável para restringir, suspender** ou revogar a acreditação de um organismo de avaliação da conformidade conferida nos termos do n.º 1 do presente artigo, 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 violem o presente regulamento.

Artigo 52.º

Notificação

1. As autoridades nacionais [...] de certificação da **cibersegurança** notificam a Comissão, relativamente a cada sistema europeu de certificação da cibersegurança adotado ao abrigo do artigo 44.º, dos organismos de avaliação da conformidade acreditados **– e, se aplicável, autorizados em conformidade com o artigo 51.º, n.º 1-B –** para emitirem certificados com os níveis de garantia especificados conforme referido no artigo 46.º, bem como, sem demora injustificada, de quaisquer alterações posteriores dos mesmos.

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

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

4. Uma autoridade nacional [...] de certificação da **cibersegurança** pode apresentar à Comissão um pedido para que retire da lista referida no n.º 2 do presente artigo um organismo de avaliação da conformidade notificado pelo Estado-Membro em causa. A Comissão publica no Jornal Oficial da União Europeia as correspondentes alterações da lista no prazo de um mês a contar da data de receção do pedido da autoridade nacional [...] de certificação da **cibersegurança**.

5. A Comissão pode, por intermédio de atos de execução, definir as circunstâncias, os formatos e os procedimentos da notificação referida no n.º 1 do presente artigo. Os referidos atos de execução são adotados nos termos do procedimento de exame a que se refere o artigo 55.º, n.º 2.

Artigo 53.º

Grupo europeu para a certificação da cibersegurança

1. É criado o grupo europeu para a certificação da cibersegurança (a seguir designado por "grupo").

2. O grupo é composto por **representantes das** autoridades nacionais [...] de certificação da **cibersegurança ou representantes de outras autoridades nacionais competentes**. [...] **Nenhum membro do grupo pode representar mais de um Estado-Membro.**

3. O grupo tem as seguintes atribuições:

   a) Aconselhar e assistir a Comissão no seu trabalho de assegurar a execução e aplicação coerente do presente título, nomeadamente no que se refere 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, em conformidade com o artigo 44.º do presente regulamento;

   b-A) Adotar pareceres sobre as propostas de sistemas, em conformidade com o artigo 44.º do presente regulamento;

   c) [...] **Solicitar** à Agência que elabore uma proposta de sistema europeu de certificação da cibersegurança, em conformidade com o artigo 44.º do presente regulamento;

   c-A) Elaborar e adotar orientações sobre os critérios para a avaliação das propostas de elaboração de uma proposta de sistema apresentadas [...] ao grupo em conformidade com o artigo 44.º, n.º 1-A;

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

e) Analisar os desenvolvimentos relevantes no domínio da certificação da cibersegurança e proceder ao intercâmbio de boas práticas em matéria de sistemas de certificação da cibersegurança;

f) Facilitar a cooperação entre as autoridades nacionais [...] de certificação da **cibersegurança** a que se refere o presente título mediante o **reforço de capacidades,** o intercâmbio de informações, nomeadamente pelo estabelecimento de métodos eficientes de intercâmbio de informações relativas a todas as questões no domínio da certificação da cibersegurança**;**

f-A) Apoiar a aplicação do mecanismo de revisão pelos pares em conformidade com a regras estabelecidas por um sistema europeu de certificação da cibersegurança nos termos do artigo 47.º, n.º 1, alínea m-D), do presente regulamento.

4. A Comissão preside ao grupo **na qualidade de moderador** e assegura os seus serviços de secretariado, com a assistência da ENISA, tal como previsto no artigo 8.º, alínea a).

Artigo 53.º-A

***Direito de apresentar uma reclamação junto da autoridade* [...] *nacional* de *certificação* da cibersegurança**

1. As pessoas singulares ou coletivas têm o direito de apresentar uma reclamação junto da autoridade nacional de certificação da cibersegurança relativamente a certificados emitidos pela mesma autoridade ou, nos termos do artigo 48.º, n.º 4-A, por organismos de avaliação da conformidade.

2. A autoridade nacional de certificação da cibersegurança à qual tiver sido apresentada a reclamação informa o autor da reclamação sobre o andamento e o resultado da mesma, inclusive sobre a possibilidade de recurso judicial nos termos do artigo 53.º-B.

Artigo 53.º-B

Direito a um recurso judicial efetivo

1. As pessoas singulares ou coletivas têm direito a um recurso judicial efetivo contra uma decisão juridicamente vinculativa a seu respeito tomada por uma autoridade nacional de certificação da cibersegurança.

2. As pessoas singulares ou coletivas têm o direito a um recurso judicial efetivo caso a autoridade nacional de certificação da cibersegurança não trate uma reclamação.

3. Os recursos judiciais contra uma autoridade nacional de certificação da cibersegurança são interpostos nos tribunais do Estado-Membro onde a autoridade está estabelecida.

Artigo 54.º

Sanções

Os Estados-Membros estabelecem as regras relativas às sanções aplicáveis em caso de violação do disposto neste 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, [até .../ sem demora], a Comissão dessas regras e medidas, e notificam-na igualmente de qualquer alteração subsequente das mesmas.

TÍTULO IV
DISPOSIÇÕES FINAIS

Artigo 55.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 56.º

Avaliação e revisão

1. O mais tardar cinco anos após a data referida no artigo 58.º, e posteriormente de cinco em cinco anos, a Comissão avalia o impacto, a eficácia e a eficiência da Agência e dos seus métodos de trabalho, bem como a eventual necessidade de alterar o mandato da Agência e as consequências financeiras dessa alteração. Essa avaliação tem em conta todas as informações comunicadas à Agência em resposta às suas atividades. Se entender que a manutenção da Agência, 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 concerne as disposições relativas à Agência.

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

3. A Comissão envia o relatório de avaliação, acompanhado das suas conclusões, ao Parlamento Europeu, ao Conselho e ao conselho de administração. As conclusões do relatório de avaliação são tornadas públicas.

Artigo 57.º

Revogação e sucessão

1. O Regulamento (CE) n.º 526/2013 é revogado com efeitos a partir de [...].

2. As referências ao Regulamento (CE) n.º 526/2013 e à ENISA consideram-se como sendo referências ao presente regulamento e à Agência.

3. A Agência sucede à Agência criada pelo Regulamento (CE) 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 em vigor do conselho de administração e da comissão executiva permanecem válidas, desde que não estejam em conflito com as disposições do presente regulamento.

4. A Agência é criada por um período indeterminado que se inicia em [...].

5. O diretor executivo nomeado ao abrigo do artigo 24.º, n.º 4, do Regulamento (CE) n.º 526/2013 será o diretor executivo da Agência durante o restante do seu mandato.

6. Os membros e respetivos suplentes do conselho de administração nomeados ao abrigo do artigo 6.º do Regulamento (CE) n.º 526/2013 serão os membros e respetivos suplentes do conselho de administração da Agência durante o restante do seu mandato.

Artigo 58.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.

1-A. O presente regulamento é aplicável a partir de […], exceto no que respeita aos artigos 50.º, 51.º, 52.º, 53.º-A, 53.º-B e 54.º, que são aplicáveis a partir de [24 meses após a data da sua publicação no Jornal Oficial da União Europeia].

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

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*

ANEXO

REQUISITOS QUE OS ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE DEVEM CUMPRIR

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 ou serviços de tecnologias da informação e comunicação (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 ou serviços 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 ou serviços de TIC a avaliar, nem o representante autorizado de qualquer uma dessas partes. Esta exigência não obsta à utilização de produtos avaliados que sejam necessários às atividades do organismo de avaliação da conformidade, nem à utilização desses produtos 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 ou na manutenção desses produtos ou serviços de TIC, nem representar as partes envolvidas nessas atividades. Os referidos organismos não podem exercer qualquer atividade suscetível de comprometer a independência do seu julgamento ou a sua integridade no desempenho das atividades de avaliação da conformidade para as quais sejam notificados. Esta disposição é aplicável, nomeadamente, aos serviços de consultoria.

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

7. 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.

8. 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 por eles mesmos ou em seu nome e sob a sua responsabilidade.

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

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

   b) Descrições dos procedimentos de avaliação da conformidade que assegurem 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 de outras atividades;

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

10. 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.

11. O pessoal encarregado de 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 que efetua e a devida autoridade para as efetuar;

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

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

12. Deve ser garantida a imparcialidade dos organismos de avaliação da conformidade, dos seus quadros superiores e do pessoal avaliador.

13. A remuneração dos quadros superiores e do pessoal avaliador dos organismos de avaliação da conformidade não pode depender do número de avaliações realizadas nem do seu resultado.

14. 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.

15. O pessoal dos organismos de avaliação da conformidade deve estar sujeito a sigilo profissional no que se refere a todas as informações obtidas no cumprimento das suas tarefas no âmbito do presente regulamento ou de qualquer disposição do direito nacional que lhe dê aplicação, exceto em relação às autoridades competentes do Estado-Membro em que exerce as suas atividades.

16. Os organismos de avaliação da conformidade devem cumprir os requisitos da norma **pertinente harmonizada ao abrigo do Regulamento (CE) 765/2008 para a acreditação de organismos de avaliação da conformidade que certifiquem processos, produtos ou serviços [...].**

17. Os organismos de avaliação da conformidade devem assegurar que os laboratórios de ensaio utilizados para fins de avaliação da conformidade cumprem os requisitos da norma **pertinente harmonizada ao abrigo do Regulamento (CE) 765/2008 na acreditação de laboratórios que realizem ensaios** [...].