COMISSÃO
EUROPEIA

Bruxelas, 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

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)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Justificação e objetivos da proposta

A União Europeia adotou uma série de medidas para aumentar a resiliência e melhorar a sua preparação em termos de cibersegurança. A primeira Estratégia da UE para a Cibersegurança[1], adotada em 2013, define objetivos estratégicos e ações concretas para se alcançar resiliência, reduzir a cibercriminalidade, desenvolver a política e as capacidades de ciberdefesa, desenvolver recursos industriais e tecnológicos e estabelecer uma política internacional coerente em matéria de ciberespaço para a UE. Nesse contexto, registaram-se desde então desenvolvimentos importantes, incluindo, em especial, o segundo mandato da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA)[2] e a adoção da **Diretiva relativa à segurança das redes e da informação**[3] («Diretiva SRI»), que constituem a base da presente proposta.

Além disso, **em 2016, a Comissão Europeia adotou uma comunicação intitulada «Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora»**[4], na qual foram anunciadas mais medidas para criar cooperação e intercâmbio de informações e conhecimentos e para aumentar a resiliência e a preparação da UE, tendo também em conta a possibilidade de incidentes em grande escala e uma eventual crise pan-europeia de cibersegurança. Neste contexto, a Comissão anunciou que iria apresentar a **avaliação** e **revisão** do Regulamento (UE) n.º 526/2013 do Parlamento Europeu e do Conselho relativo à ENISA e que revoga o Regulamento (CE) n.º 460/2004 («Regulamento ENISA»). O processo de avaliação poderia conduzir a uma eventual reforma da Agência e a uma melhoria das suas capacidades para apoiar os Estados-Membros de forma sustentável. Por conseguinte, conferir-lhe-ia um papel mais operacional e central na consecução da resiliência a nível da cibersegurança e reconheceria, no seu novo mandato, as novas responsabilidades da Agência nos termos da Diretiva SRI.

A Diretiva SRI constitui um primeiro passo essencial com vista a promover uma cultura de gestão dos riscos, introduzindo requisitos de segurança como obrigações jurídicas para os principais agentes económicos, nomeadamente operadores que prestam serviços essenciais (operadores de serviços essenciais — OSE) e fornecedores de alguns serviços digitais cruciais (prestadores de serviços digitais — PSD). Com os requisitos de segurança a serem encarados como essenciais para salvaguardar os benefícios da digitalização em curso da sociedade e atendendo à rápida proliferação dos dispositivos conectados (a Internet das coisas — IdC), a comunicação de 2016 também apresenta a ideia de criar um quadro para a certificação da segurança aplicável a produtos e serviços de TIC, a fim de aumentar a confiança e a segurança no mercado único digital. A certificação da cibersegurança das TIC torna-se particularmente relevante atendendo à cada vez maior utilização de tecnologias que exigem um elevado nível

---

1 Comunicação conjunta da Comissão Europeia e do Serviço Europeu de Ação Externa: Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido — JOIN(2013).

2 Regulamento (UE) n.º 526/2013 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.

3 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.

4 Comunicação da Comissão — Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora, COM/2016/0410 final.

de cibersegurança, tais como automóveis conectados e automatizados, saúde eletrónica ou sistemas industriais de automatização e controlo.

Estas medidas e anúncios políticos foram ainda mais reforçados pelas **conclusões do Conselho**, de 2016, que reconheceram que as «ciberameaças e as vulnerabilidades continuam a evoluir e a intensificar-se, o que obrigará a uma cooperação contínua e mais estreita, particularmente no tratamento de incidentes transfronteiras de grande escala em matéria de cibersegurança». As conclusões reafirmaram que o «regulamento ENISA constitui um dos elementos centrais de um quadro de ciberresiliência da UE»[5] e instaram a Comissão a adotar medidas suplementares para abordar a questão da certificação a nível europeu.

O estabelecimento de um sistema de certificação exigirá a criação de um sistema de governação adequado a nível da UE, designadamente mediante conhecimentos especializados disponibilizados por uma agência da UE independente. A este respeito, a presente proposta identifica naturalmente a ENISA como o organismo a nível da UE competente em matéria de cibersegurança, que deverá assumir a função de reunir e coordenar o trabalho dos organismos nacionais competentes no domínio da certificação.

Na sua comunicação sobre a **Revisão intercalar da Estratégia para o Mercado Único Digital, de maio de 2017**, a Comissão especificou ainda que, até setembro de 2017, procederia à revisão do mandato da ENISA. Tal destina-se a definir o seu papel no ecossistema alterado da cibersegurança e a adotar medidas em matéria de normas de cibersegurança, de certificação e de rotulagem para tornar os sistemas baseados nas TIC, nomeadamente os objetos conectados, mais ciberseguros[6]. Nas suas **conclusões de junho de 2017[7], o Conselho Europeu** saudou a intenção da Comissão de rever a Estratégia para a Cibersegurança em setembro e de propor novas ações específicas antes do final do ano de 2017.

A proposta de regulamento prevê um conjunto abrangente de medidas que tem por base as ações anteriores e promove objetivos específicos que se reforçam mutuamente:

- Aumentar as **capacidades e o grau de preparação** dos Estados-Membros e das empresas;
- Melhorar a **cooperação e coordenação** entre Estados-Membros e instituições, agências e organismos da UE;
- Aumentar as **capacidades a nível da UE para complementar a ação dos Estados-Membros**, designadamente no caso de cibercrises transfronteiriças;
- Aumentar a **sensibilização** dos cidadãos e das empresas para as questões da cibersegurança;
- Aumentar a **transparência da garantia de cibersegurança**[8] de produtos e serviços de TIC, a fim de reforçar a confiança no mercado único digital e na inovação digital;

---

5 Conclusões do Conselho sobre o reforço do sistema de ciberresiliência da Europa e a promoção de uma indústria de cibersegurança competitiva e inovadora (15 de novembro de 2016).

6 Comunicação da Comissão sobre a revisão intercalar relativa à aplicação da Estratégia para o Mercado Único Digital, COM(2017) 228.

7 Reunião do Conselho Europeu (22 e 23 de junho de 2017) — Conclusões EUCO 8/17.

8 Entende-se por «transparência da garantia de cibersegurança»: prestar aos utilizadores informações suficientes sobre as propriedades de cibersegurança que lhes permitam determinar objetivamente o nível de segurança de um determinado produto, serviço ou processo de TIC.

- Evitar a **fragmentação dos sistemas de certificação** na UE e dos requisitos de segurança conexos, bem como dos critérios de avaliação nos Estados-Membros e setores.

A parte da exposição de motivos que se segue explica mais pormenorizadamente o fundamento subjacente à iniciativa no que diz respeito às ações propostas para a ENISA e a certificação da cibersegurança.

ENISA

A ENISA atua como um centro de conhecimentos especializados dedicado à melhoria da segurança das redes e da informação na União e ao apoio ao reforço de capacidades dos Estados-Membros.

A ENISA foi criada em 2004[9] com o intuito de contribuir para os objetivos gerais de assegurar um elevado nível de segurança das redes e da informação na UE. Em 2013, o Regulamento (UE) n.º 526/2013 instituiu um novo mandato da Agência para um período de sete anos, até 2020. A Agência tem os seus escritórios na Grécia, nomeadamente a sede administrativa em Heráclion (Creta) e as operações principais em Atenas.

A ENISA é uma pequena agência, com um orçamento reduzido e poucos funcionários, comparativamente a todas as agências da UE. Tem um mandato fixo.

A ENISA apoia as instituições europeias, os Estados-Membros e a comunidade empresarial na **análise, na resposta e sobretudo na prevenção de problemas de segurança das redes e da informação**. Para tal, realiza uma série de atividades em cinco domínios identificados na sua estratégia[10]:

- Conhecimentos especializados: prestação de informações e conhecimentos especializados sobre questões determinantes de segurança das redes e da informação.
- Política: apoio à elaboração e execução de políticas na União.
- Capacidade: apoio ao reforço das capacidades na União (por exemplo, mediante formações, recomendações, atividades de sensibilização).
- Comunidade: promover a comunidade de segurança das redes e da informação [por exemplo, apoio às equipas de resposta a emergências informáticas (CERT), coordenação dos exercícios pan-europeus de cibersegurança].
- Capacitação (por exemplo, compromissos com as partes interessadas e relações internacionais).

No decurso das negociações da Diretiva SRI, os colegisladores da UE decidiram atribuir funções importantes à ENISA na sua execução. Concretamente, a Agência assegura os serviços de secretariado da rede de CSIRT (criada para promover a cooperação operacional célere e eficaz entre os Estados-Membros em matéria de incidentes de cibersegurança específicos e de partilha de informações sobre riscos), sendo igualmente chamada a apoiar o grupo de cooperação no exercício das suas tarefas. Além disso, a diretiva requer que a ENISA assista os Estados-Membros e a Comissão mediante a disponibilização de conhecimentos especializados e aconselhamento e da facilitação do intercâmbio de boas práticas.

Nos termos do Regulamento ENISA, a Comissão realizou uma avaliação da Agência que inclui um estudo independente, bem como uma consulta pública. A avaliação examinou a relevância, o impacto, a eficácia, a eficiência, a coerência e o valor acrescentado da UE da Agência relativamente ao seu desempenho, governação, estrutura organizacional interna e métodos de trabalho durante o período de 2013-2016.

---

9 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).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy.

O desempenho global da ENISA foi avaliado positivamente pela maior parte dos inquiridos[11] (74 %) na consulta pública. Uma maioria de inquiridos considerou ainda que a ENISA está a alcançar os seus diferentes objetivos (pelo menos 63 % para cada um dos objetivos). Os serviços e produtos da ENISA são utilizados regularmente (mensalmente ou com maior frequência) por quase metade dos inquiridos (46 %) e são apreciados por resultarem de um organismo a nível da UE (83 %) e pela sua qualidade (62 %).

No entanto, uma grande maioria (88 %) dos inquiridos considerou que os instrumentos e mecanismos em vigor disponíveis a nível da UE são insuficientes ou apenas parcialmente adequados para responder aos desafios atuais da cibersegurança. Uma grande maioria dos inquiridos (98 %) indicou que um organismo da UE deveria responder a essas necessidades e, entre eles, a ENISA foi considerada a organização certa para o fazer por 99 % dos inquiridos. Além disso, 67,5 % dos inquiridos manifestaram a opinião de que a ENISA poderia desempenhar um papel na instituição de um quadro harmonizado para a certificação da segurança de produtos e serviços de TIC.

A avaliação geral (com base não apenas na consulta pública, mas também em diversas entrevistas individuais, inquéritos específicos suplementares e seminários) concluiu o seguinte:

- Os objetivos da ENISA continuam a ser relevantes hoje em dia. Num contexto de rápidos desenvolvimentos tecnológicos e de ameaças em evolução e atendendo aos crescentes riscos mundiais de cibersegurança, existe uma necessidade inequívoca na UE de promover e continuar a reforçar os conhecimentos especializados de alto nível em matéria de cibersegurança. Afigura-se necessário criar, nos Estados-Membros, capacidades para compreender e responder às ameaças, e as partes interessadas têm de cooperar em diferentes domínios temáticos e com diferentes instituições.
- Apesar do seu reduzido orçamento, a Agência tem sido eficiente em termos operacionais na utilização dos seus recursos e na execução das suas tarefas. Contudo, a localização dividida entre Atenas e Heráclion gerou custos administrativos suplementares.
- Em termos de eficácia, a ENISA cumpriu parcialmente os seus objetivos. A Agência contribuiu com êxito para a melhoria da segurança das redes e da informação na Europa ao proporcionar o reforço de capacidades nos 28 Estados-Membros[12], melhorando a cooperação entre os Estados-Membros e as partes interessadas em matéria de segurança das redes e da informação e disponibilizando conhecimentos especializados, desenvolvimento da comunidade e apoio à elaboração de políticas.

[11] Responderam à consulta 90 partes interessadas de 19 Estados-Membros (88 respostas e 2 posições escritas), nomeadamente autoridades nacionais de 15 Estados-Membros e 8 organizações de cúpula que representam um número significativo de empresas europeias.

[12] Foi pedido aos inquiridos da consulta pública que comentassem o que entendiam ser as principais realizações da ENISA durante o período de 2013-2016. Os inquiridos de todos os grupos (55 no total, nomeadamente 13 de autoridades nacionais, 20 do setor privado e 22 de «outros») consideraram que as principais realizações da ENISA eram as seguintes: 1) A coordenação dos exercícios «Cyber Europe»; 2) A prestação de apoio às CERT/CSIRT por via de formação e seminários que promovem a coordenação e os intercâmbios; 3) As publicações da ENISA (orientações e recomendações, relatórios sobre o cenário de ameaças, estratégias para a comunicação de incidentes e gestão de crises, etc.) que foram consideradas úteis para criar e atualizar quadros de segurança nacionais, bem como para servirem de referência a decisores políticos e profissionais da cibernética; 4) A assistência na promoção da Diretiva SRI; 5) Os esforços para aumentar a sensibilização em matéria de cibersegurança por via do mês da cibersegurança.

Em termos gerais, a ENISA concentrou-se diligentemente na execução do seu programa de trabalho e atuou como um parceiro de confiança para as partes interessadas, num domínio que só recentemente foi reconhecido como tendo uma relevância transfronteiriça tão forte.

- A ENISA conseguiu produzir um impacto, pelo menos até certo ponto, no vasto domínio da segurança das redes e da informação, mas não conseguiu desenvolver plenamente um nome de marca forte nem ganhar visibilidade suficiente para ser reconhecida como «o» centro de conhecimentos especializados na Europa. Tal explica-se pelo mandato alargado da ENISA, que não está equipada com recursos proporcionalmente suficientes. Além disso, a ENISA continua a ser a única agência da UE com um mandato fixo, o que limita a sua capacidade de desenvolver uma visão a longo prazo e de apoiar as partes interessadas de um modo sustentável. Isto contrasta igualmente com as disposições da Diretiva SRI, que confiam à ENISA funções sem termo. Por último, a avaliação concluiu que esta eficácia limitada pode explicar-se, em parte, pela forte dependência de conhecimentos especializados externos, em detrimento dos internos, e pelas dificuldades no recrutamento e conservação de pessoal especializado.
- Finalmente, a avaliação concluiu que o valor acrescentado da ENISA assenta primeiramente na capacidade da Agência de melhorar a cooperação, principalmente entre Estados-Membros, e particularmente com comunidades relacionadas com a segurança das redes e da informação (em especial, entre as CSIRT). Não existe outro interveniente a nível da UE que apoie um âmbito tão lato de partes interessadas em matéria de segurança das redes e da informação. No entanto, devido à necessidade de conferir prioridades às suas atividades de modo estritamente rigoroso, o programa de trabalho da ENISA é, na sua maioria, guiado pelas necessidades dos Estados-Membros. Consequentemente, não aborda suficientemente as necessidades de outras partes interessadas, em especial a indústria. Isso também tornou a Agência reativa à satisfação das necessidades das principais partes interessadas, impedindo-a de alcançar um impacto maior. Por conseguinte, o valor acrescentado proporcionado pela Agência variou de acordo com as necessidades divergentes das partes interessadas e na medida em que a Agência foi capaz de dar resposta às mesmas (por exemplo, Estados-Membros grandes face a pequenos; Estados-Membros face à indústria).

Resumindo, os resultados das consultas e avaliação das partes interessadas sugeriram que os recursos e o mandato da ENISA têm de ser adaptados para que esta possa desempenhar uma função adequada na resposta aos desafios atuais e futuros.

À luz destas conclusões, a presente proposta revê o mandato em vigor da ENISA e estabelece um conjunto renovado de tarefas e funções, com vista a apoiar eficaz e eficientemente os esforços dos Estados-Membros, das instituições da UE e de outras partes interessadas destinados a garantir um ciberespaço seguro na União Europeia. O novo mandato proposto pretende atribuir à Agência um papel mais forte e mais central, nomeadamente no apoio aos Estados-Membros na execução da Diretiva SRI e no combate mais ativo (capacidade operacional) a ameaças específicas, e torná-la num centro de conhecimentos especializados que apoia os Estados-Membros e a Comissão em matéria de certificação de cibersegurança. Nos termos desta proposta:

- Será atribuído um mandato permanente à ENISA que, assim, estará colocada num patamar mais estável para o futuro. O mandato, os objetivos e as atribuições devem continuar a estar sujeitos a revisão regular.

- O mandato proposto esclarece ainda a função da ENISA enquanto agência da UE para a cibersegurança e ponto de referência no ecossistema de cibersegurança da UE, atuando em estreita colaboração com todos os demais organismos pertinentes desse ecossistema.
- A organização e governação da Agência, que foram avaliadas positivamente no decurso da avaliação, serão ligeiramente revistas, em especial para garantir que as necessidades da comunidade mais alargada de partes interessadas estão mais bem refletidas no trabalho da Agência.
- É delineado o âmbito sugerido do mandato, reforçando as áreas nas quais a Agência demonstrou um claro valor acrescentado e aditando as novas áreas nas quais é necessário apoio, atendendo às novas prioridades e instrumentos políticos, designadamente a Diretiva SRI, a revisão da Estratégia da UE para a Cibersegurança, o futuro plano de ação da UE para a cibersegurança, a cooperação na gestão de cibercrises e a certificação da segurança das TIC:
    - **Desenvolvimento e execução de políticas da UE:** a ENISA será incumbida de contribuir pró-ativamente para o desenvolvimento de políticas no domínio da segurança das redes e da informação, bem como de outras iniciativas políticas com elementos de cibersegurança em diferentes setores (por exemplo, energia, transportes, finanças). Para o efeito, terá um forte papel consultivo, que poderá desempenhar mediante o fornecimento de pareceres independentes e de trabalhos preparatórios para a elaboração e a atualização da política e da legislação. A ENISA também apoiará a política e a legislação da UE nos domínios das comunicações eletrónicas, da identificação eletrónica e dos serviços de confiança, com o intuito de promover um nível reforçado de cibersegurança. Na fase de execução, em especial no contexto do grupo de cooperação SRI, a ENISA ajudará os Estados-Membros a alcançar uma abordagem coerente na execução da Diretiva SRI entre fronteiras e setores, bem como de outras políticas e atos legislativos pertinentes. A fim de apoiar a revisão regular das políticas e da legislação no domínio da cibersegurança, a ENISA também comunicará regularmente o estado da execução do quadro jurídico da UE.
    - **Reforço das capacidades:** a ENISA contribuirá para a melhoria das capacidades e dos conhecimentos especializados das autoridades públicas nacionais e da UE, nomeadamente em matéria de resposta a incidentes e de supervisão de medidas regulamentares relacionadas com a cibersegurança. A Agência será também chamada a contribuir para a criação de centros de partilha e análise de informações (ISAC) em vários setores mediante a disponibilização de boas práticas e orientação sobre instrumentos e procedimentos disponíveis, bem como pela resposta adequada a questões regulamentares relacionadas com a partilha de informações.
    - **Conhecimento, informação e sensibilização:** a ENISA tornar-se-á o polo de informações da UE. Tal implicará a promoção e partilha de boas práticas e iniciativas na UE, reunindo informações sobre cibersegurança provenientes das instituições, agências e organismos nacionais e da UE. A Agência disponibilizará igualmente aconselhamento, orientação e boas práticas em matéria de segurança de infraestruturas críticas. Além disso, na sequência de incidentes de cibersegurança transfronteiriços significativos, a ENISA coligirá relatórios destinados a prestar orientação a empresas e cidadãos na UE. Este

fluxo de trabalho envolverá igualmente a organização regular de ações de sensibilização em coordenação com as autoridades dos Estados-Membros.

- **Atribuições relacionadas com o mercado (normalização, certificação de cibersegurança):** a ENISA exercerá várias funções que apoiam especificamente o mercado interno e constituirá um «observatório do mercado» de cibersegurança, analisando as tendências importantes do mercado da cibersegurança, a fim de melhor fazer corresponder a oferta à procura, e apoiando o desenvolvimento de políticas da UE nos domínios da normalização e da certificação de segurança das TIC. No que diz concretamente respeito à normalização, facilitará a criação e adoção de normas de cibersegurança. A ENISA também exercerá as atribuições previstas no contexto do futuro quadro para certificação (ver secção infra).
- **Investigação e inovação:** a ENISA contribuirá com os seus conhecimentos especializados por via do aconselhamento às autoridades nacionais e da UE sobre a fixação de prioridades em matéria de investigação e desenvolvimento, nomeadamente no contexto da parceria público-privada contratual (PPPc) para a cibersegurança. O aconselhamento da ENISA sobre investigação alimentará o Centro Europeu de Investigação e de Competências em matéria de Cibersegurança ao abrigo do próximo quadro financeiro plurianual. A ENISA também estará envolvida, sempre que a Comissão o solicite, na execução dos programas de financiamento da UE para investigação e inovação.
- **Cooperação operacional e gestão de crises:** este fluxo de trabalho deve ter por base o reforço das capacidades operacionais preventivas existentes, em especial a atualização dos exercícios pan-europeus de cibersegurança (Cyber Europe), realizando-os anualmente, e um papel de apoio na cooperação operacional assumindo os serviços de secretariado da rede de CSIRT (tal como previsto nas disposições da Diretiva SRI), assegurando, entre outros aspetos, o bom funcionamento da infraestrutura informática e dos canais de comunicação da rede de CSIRT. Neste contexto, será necessária uma cooperação estruturada com a CERT-UE, o Centro Europeu da Cibercriminalidade (EC3) e outros organismos competentes da UE. Além disso, a cooperação estruturada com a CERT-UE, em estreita proximidade física, deverá conduzir a uma função de prestação de assistência técnica em caso de incidentes significativos e de apoio à análise de incidentes. Os Estados-Membros que a solicitem receberão assistência para lidar com incidentes e apoio à análise de vulnerabilidades, artefactos e incidentes, a fim de reforçarem a sua própria capacidade preventiva e de resposta.
- A ENISA também desempenhará um papel no **plano de ação da UE para a cibersegurança** apresentado como parte deste pacote e que estabelece a recomendação da Comissão aos Estados-Membros para uma resposta coordenada, a nível da UE, a incidentes de cibersegurança transfronteiriços em grande escala e crises de cibersegurança[13]. A ENISA facilitará a cooperação entre Estados-Membros individuais na resposta a situações de emergência,

[13] O plano de ação aplicar-se-á a incidentes de cibersegurança que causem uma perturbação mais extensa do que aquela com que um Estado-Membro possa lidar sozinho ou que afetem dois ou mais Estados-Membros com um impacto ou importância política de tal ordem abrangente e significativa que exijam coordenação e resposta política tempestivas a nível político da União.

mediante a análise e agregação de relatórios de situação nacionais, baseados em informações disponibilizadas à Agência a título voluntário pelos Estados-Membros e outras entidades.

- **Certificação da cibersegurança de produtos e serviços de TIC**

A fim de criar e preservar confiança e segurança, os produtos e serviços de TIC têm de incorporar diretamente funcionalidades de segurança nas fases incipientes da sua conceção e desenvolvimento técnicos (segurança desde a conceção). Além disso, os clientes e utilizadores devem ser capazes de verificar o nível de garantia de segurança dos produtos e serviços que obtêm ou adquirem.

A certificação, que consiste na avaliação formal de produtos, serviços e processos realizada por um organismo independente e acreditado relativamente a um conjunto definido de critérios ou normas e na emissão de um certificado que ateste a conformidade, desempenha um papel importante no aumento da confiança e segurança dos produtos e serviços. Embora as avaliações de segurança sejam um domínio bastante técnico, a certificação serve a finalidade de informar e tranquilizar os compradores e utilizadores sobre as propriedades de segurança dos produtos e serviços de TIC que adquirem ou utilizam. Conforme referido anteriormente, isto é particularmente relevante para os novos sistemas baseados nas tecnologias digitais e que exigem um elevado nível de segurança, tais como os automóveis conectados, a saúde eletrónica, os sistemas industriais de automatização e controlo (IACS)[14] ou as redes inteligentes.

Presentemente, o cenário da certificação de cibersegurança de produtos e serviços de TIC na UE é deveras fragmentado. Existe uma série de iniciativas internacionais, tais como os designados Critérios Comuns (CC) para a Avaliação da Segurança das Tecnologias da Informação (ISO 15408), que se tratam de uma norma internacional para avaliação da segurança informática. Baseiam-se na avaliação por parte de um terceiro e preveem sete níveis de avaliação da garantia (Evaluation Assurance Levels) (EAL). Os CC e a Metodologia Comum para a Avaliação da Segurança das Tecnologias da Informação (CEM) que os acompanha constituem a base técnica para um acordo internacional, o Acordo de Reconhecimento dos Critérios Comuns (ARCC), que assegura que os certificados dos CC são reconhecidos por todos os signatários do ARCC. Contudo, na versão atual do ARCC, apenas as avaliações até ao EAL 2 são mutuamente reconhecidas. Além disso, apenas 13 Estados-Membros assinaram o acordo.

As autoridades de certificação de 12 Estados-Membros celebraram um acordo de reconhecimento mútuo relativo aos certificados emitidos em conformidade com o acordo com base nos Critérios Comuns[15]. Além disso, existe atualmente, ou está a ser criado, um conjunto de iniciativas de certificação das TIC nos Estados-Membros. Embora sejam importantes, estas

---

[14] A DG JRC publicou um relatório que propõe um conjunto inicial de requisitos europeus comuns e orientações amplas relacionadas com a certificação da cibersegurança dos componentes dos IACS. Acessível em: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf.

[15] O Grupo de Altos Funcionários para a Segurança dos Sistemas de Informação (SOG-IS) inclui 12 Estados-Membros e a Noruega e desenvolveu alguns perfis de proteção para um número limitado de produtos tais como a assinatura digital, o tacógrafo digital e os cartões inteligentes. Os participantes trabalham em conjunto para coordenar a normalização dos perfis de proteção dos CC e coordenam o desenvolvimento de perfis de proteção. Muitas vezes, os Estados-Membros solicitam a certificação SOG-IS para efeitos de concursos públicos nacionais.

iniciativas criam o risco de fragmentação do mercado e levantam questões de interoperabilidade. Consequentemente, uma empresa poderá ter de se submeter a vários procedimentos de certificação em diferentes Estados-Membros para poder colocar o seu produto em diversos mercados. Por exemplo, um fabricante de contadores inteligentes que pretenda vender os seus produtos em três Estados-Membros, como, por exemplo, Alemanha, França e Reino Unido, necessita atualmente de cumprir os requisitos de três sistemas de certificação distintos, neste caso, o Commercial Product Assurance (CPA) no Reino Unido, a Certification de Sécurité de Premier Niveau (CSPN) em França e um perfil de proteção específico baseado nos Critérios Comuns na Alemanha.

Esta situação conduz a custos mais elevados e constitui um encargo administrativo considerável para as empresas que operam em vários Estados-Membros. Embora o custo da certificação possa variar consideravelmente em função do produto/serviço em causa, do nível de avaliação da garantia pretendido e/ou de outras componentes, regra geral, tende a ser bastante considerável para as empresas. Para o certificado BSI «Smart Meter Gateway», por exemplo, o custo é superior a um milhão de EUR (nível mais elevado de ensaio e garantia, abrange não só um produto, mas também toda a infraestrutura à sua volta). No Reino Unido, o custo da certificação dos contadores inteligentes é de quase 150 000 EUR. Em França, o custo é similar ao do Reino Unido, a saber, cerca de 150 000 EUR ou mais.

As principais partes interessadas públicas e privadas reconheceram que, na ausência de um sistema de certificação da cibersegurança a nível da UE, as empresas têm em muitas circunstâncias de ser certificadas individualmente em cada Estado-Membro, o que conduz à fragmentação do mercado. Mais importante, na ausência de legislação de harmonização da UE para os produtos e serviços de TIC, as diferenças nas normas e práticas de certificação da cibersegurança nos Estados-Membros são suscetíveis de criar, na prática, 28 mercados de segurança distintos na UE, cada um dos quais com os seus próprios requisitos técnicos, metodologias de ensaio e procedimentos de certificação da cibersegurança. Estas práticas divergentes a nível nacional são suscetíveis de causar, caso não seja tomada uma ação adequada a nível da UE, um obstáculo considerável à realização do mercado único digital, retardando ou impedindo os seus efeitos positivos conexos no crescimento e no emprego.

Com base nos desenvolvimentos supracitados, a proposta de regulamento estabelece um quadro europeu de certificação da cibersegurança («**Quadro**») de produtos e serviços de TIC e especifica as funções e tarefas essenciais da ENISA no domínio da certificação da cibersegurança. A presente proposta estabelece um quadro geral de regras que regem os sistemas europeus de certificação da cibersegurança. A proposta não introduz diretamente sistemas de certificação operacionais, criando antes um mecanismo (quadro) para a criação de sistemas de certificação específicos destinados a produtos/serviços de TIC específicos (os «sistemas europeus de certificação da cibersegurança»). A criação de sistemas europeus de certificação da cibersegurança de acordo com o Quadro permitirá que os certificados emitidos nos termos dos mesmos sejam válidos e reconhecidos em todos os Estados-Membros e responder à atual fragmentação do mercado.

O objetivo geral de um sistema europeu de certificação da cibersegurança é atestar que os produtos e serviços de TIC que foram certificados em conformidade com esse sistema cumprem os requisitos de cibersegurança especificados. Tal incluiria, por exemplo, a sua capacidade para proteger os dados (armazenados, transmitidos ou tratados de qualquer outro modo) contra armazenamento, tratamento, acesso, divulgação, destruição acidental ou não autorizado, e a perda ou alteração acidental. Os sistemas de certificação da cibersegurança da UE utilizarão normas existentes em relação aos requisitos técnicos e procedimentos de

avaliação que os produtos necessitam de cumprir e não desenvolverão eles próprios as normas técnicas[16]. Por exemplo, uma certificação a nível da UE para produtos como os cartões inteligentes, que atualmente são ensaiados relativamente a normas de CC internacionais ao abrigo do sistema SOG-IS (e descritos anteriormente), significaria tornar este sistema válido em toda a UE.

Além de descrever um conjunto específico de objetivos de segurança a serem tidos em conta na conceção de um sistema europeu de certificação da cibersegurança específico, a proposta estipula qual deve ser o conteúdo mínimo desses sistemas. Esses sistemas terão de definir, entre outros aspetos, um número de elementos específicos que definem o âmbito e objeto da certificação da cibersegurança. Tal inclui a identificação das categorias de produtos e serviços abrangidas, a especificação pormenorizada dos requisitos de cibersegurança (por exemplo, por referência às normas ou especificações técnicas relevantes), os critérios e métodos de avaliação específicos e o nível de garantia que se destinam a assegurar (ou seja, básico, substancial ou elevado).

A ENISA, com a assistência, aconselhamento especializado e estreita cooperação do grupo europeu para a certificação da cibersegurança (ver infra), preparará os sistemas europeus de certificação da cibersegurança, que a Comissão adotará por intermédio de atos de execução. Quando for identificada a necessidade de um sistema de certificação da cibersegurança, a Comissão solicitará à ENISA que prepare um sistema destinado a produtos ou serviços de TIC específicos. A ENISA trabalhará no sistema em estreita cooperação com as autoridades nacionais supervisoras da certificação representadas no Grupo. Os Estados-Membros e o Grupo poderão propor à Comissão que solicite à ENISA a preparação de um sistema específico.

A certificação pode ser um processo muito dispendioso, o que, por sua vez, pode conduzir a preços mais elevados para os clientes e consumidores. A necessidade de certificar poderá também variar consideravelmente em função do contexto específico de utilização dos produtos e serviços e do ritmo rápido da evolução tecnológica. O recurso à certificação europeia da cibersegurança deve, portanto, manter-se voluntário, salvo disposição em contrário na legislação da União que estabeleça requisitos de segurança para produtos e serviços de TIC.

A fim de assegurar a harmonização e evitar a fragmentação, os sistemas ou procedimentos nacionais de certificação da cibersegurança de produtos e serviços de TIC abrangidos por um sistema europeu de certificação da cibersegurança deixarão de ser aplicáveis a partir da data fixada no ato de execução que adota o sistema. Além disso, os Estados-Membros não devem introduzir novos sistemas nacionais de certificação da cibersegurança de produtos e serviços de TIC abrangidos por um sistema europeu de certificação da cibersegurança existente.

Assim que um sistema europeu de certificação da cibersegurança for adotado, os fabricantes de produtos de TIC ou os prestadores de serviços de TIC poderão 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 especificados. A acreditação será emitida por um período máximo de cinco anos e poderá ser renovada nas mesmas condições, desde que o organismo de avaliação da conformidade cumpra os requisitos. Os organismos de acreditação revogarão a acreditação de um organismo

[16] No caso de normas europeias, isto faz-se por intermédio das organizações de normalização europeias e é aprovado pela Comissão Europeia com a publicação no Jornal Oficial [ver Regulamento (UE) n.º 1025/2012].

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.

Nos termos da proposta, as tarefas de monitorização, supervisão e aplicação incumbem aos Estados-Membros. Os Estados-Membros terão de providenciar uma autoridade supervisora da certificação. Caberá a esta autoridade supervisionar a conformidade dos organismos de avaliação da conformidade, bem como dos certificados emitidos pelos organismos de avaliação da conformidade estabelecidos no respetivo território, com os requisitos do presente regulamento e dos sistemas europeus de certificação da cibersegurança. As autoridades nacionais supervisoras da certificação serão competentes para tratar das reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados emitidos por organismos de avaliação da conformidade estabelecidos nos respetivos territórios. Tanto quanto necessário, investigarão o conteúdo das reclamações e informarão os respetivos autores do andamento e do resultado da investigação num prazo razoável. Além disso, cooperarão com outras autoridades supervisoras da certificação e outras autoridades públicas, nomeadamente pela partilha de informações sobre a eventual não conformidade de produtos e serviços de TIC com os requisitos do presente regulamento ou de sistemas europeus de certificação da cibersegurança específicos.

Por último, a proposta institui o grupo europeu para a certificação da cibersegurança («Grupo»), composto por autoridades nacionais supervisoras da certificação de todos os Estados-Membros. A principal função do Grupo é prestar aconselhamento à Comissão sobre questões relacionadas com a política de certificação da cibersegurança e trabalhar com a ENISA no desenvolvimento de projetos de sistemas europeus de certificação da cibersegurança. A ENISA assistirá a Comissão assegurando o serviço de secretariado do Grupo e mantendo um inventário público atualizado de sistemas aprovados ao abrigo do quadro europeu de certificação da cibersegurança. A ENISA assegurará igualmente a sua coordenação com organismos de normalização, para assegurar a adequação das normas utilizadas nos sistemas aprovados e para identificar áreas que requeiram normas de cibersegurança.

O quadro europeu de certificação da cibersegurança («Quadro») proporcionará vários benefícios aos cidadãos e às empresas, nomeadamente:

- A criação de sistemas de certificação da cibersegurança a nível da UE para produtos ou serviços específicos proporcionará às empresas um balcão único para a certificação da cibersegurança na UE. Essas empresas poderão certificar o seu produto uma única vez e obter um certificado válido em todos os Estados-Membros. Não serão obrigadas a voltar a certificar os seus produtos ao abrigo de organismos de certificação nacionais diferentes. Tal reduzirá consideravelmente os custos para empresas, facilitará as operações transfronteiriças e, em última instância, reduzirá e evitará uma fragmentação do mercado interno para os produtos em causa.
- O Quadro estabelece a primazia dos sistemas europeus de certificação da cibersegurança sobre os sistemas nacionais: nos termos desta regra, a adoção de um sistema europeu de certificação da cibersegurança substituirá todos os sistemas nacionais paralelos existentes para os mesmos produtos ou serviços de TIC num determinado nível de garantia. Tal proporcionará mais clareza, reduzindo a proliferação atual de sistemas nacionais de certificação da cibersegurança que se sobrepõem e que são eventualmente conflituantes.
- A proposta apoia e complementa a execução da Diretiva SRI ao facultar às empresas abrangidas pela diretiva um instrumento muito útil para demonstrar a conformidade

com os requisitos de SRI em toda a União. Ao desenvolverem novos sistemas de certificação da cibersegurança, a Comissão e a ENISA estarão particularmente atentas à necessidade de assegurar que os requisitos de SRI estão refletidos nesses sistemas.

- A proposta apoiará e facilitará o desenvolvimento de uma política europeia em matéria de cibersegurança, mediante a harmonização das condições e dos requisitos substantivos para a certificação da cibersegurança de produtos e serviços de TIC na UE. Os sistemas europeus de certificação da cibersegurança farão referência a normas ou critérios de avaliação e metodologias de ensaio comuns. Tal contribuirá significativamente, embora de forma indireta, para a adoção de soluções de segurança comuns na UE, eliminando também, desta forma, obstáculos ao mercado interno.
- O Quadro foi concebido de modo a assegurar a flexibilidade necessária para os sistemas de certificação da cibersegurança. Dependendo das necessidades específicas de cibersegurança, um produto ou serviço pode ser certificado em relação a níveis de segurança superiores ou inferiores. Os sistemas europeus de certificação da cibersegurança serão concebidos tendo presente esta flexibilidade e, por conseguinte, preverão diferentes níveis de garantia (a saber, básico, substancial ou elevado), para que possam ser utilizados para diferentes finalidades ou em diferentes contextos.
- Todos os elementos referidos anteriormente tornarão a certificação da cibersegurança mais atrativa para as empresas enquanto meio eficaz para comunicar o nível de garantia da cibersegurança de produtos ou serviços de TIC. À medida que a certificação da cibersegurança se torna menos dispendiosa, mais eficaz e comercialmente atrativa, as empresas disporão de maiores incentivos para certificarem os seus produtos contra os riscos de cibersegurança, contribuindo, desta forma, para a disseminação de boas práticas de cibersegurança na conceção de produtos e serviços de TIC (cibersegurança desde a conceção).

- **Coerência com as disposições vigentes no mesmo domínio de intervenção**

Nos termos da Diretiva SRI, os operadores de setores que são cruciais para a nossa economia e sociedade, tais como a energia, os transportes, a água, a banca, as infraestruturas do mercado financeiro, os cuidados de saúde e as infraestruturas digitais, bem como os prestadores de serviços digitais (isto é, motores de pesquisa, serviços de computação em nuvem e mercados em linha), são obrigados a adotarem medidas para gerirem adequadamente os riscos de segurança. As novas regras da presente proposta complementam e asseguram a coerência com as disposições da Diretiva SRI, a fim de continuar a desenvolver a ciber-resiliência da UE pelo reforço das capacidades, da cooperação, da gestão dos riscos e da sensibilização para as questões do ciberespaço.

Além disso, as regras em matéria de certificação da cibersegurança proporcionam um instrumento essencial para as empresas sujeitas à Diretiva SRI, dado que poderão certificar os seus produtos e serviços de TIC contra riscos de cibersegurança com base em sistemas de certificação da cibersegurança válidos e reconhecidos em toda a UE. Também

complementarão os requisitos de segurança referidos no Regulamento eIDAS[17] e na Diretiva Equipamentos de Rádio[18].

- **Coerência com outras políticas da União**

O Regulamento (UE) n.º 2016/679 (Regulamento Geral sobre a Proteção de Dados, «**RGPD**»)[19] 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. 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.

A proposta de regulamento assegurará a compatibilidade com o Regulamento (CE) n.º 765/2008, que estabelece os requisitos de acreditação e fiscalização do mercado[20] ao fazer referência às regras desse quadro relativas a organismos nacionais de acreditação e a organismos de avaliação da conformidade. No tocante às autoridades supervisoras, a proposta de regulamento exigirá que os Estados-Membros designem autoridades nacionais supervisoras da certificação com responsabilidades em matéria de supervisão, monitorização e aplicação das regras. Esses organismos continuarão a estar separados dos organismos de avaliação da conformidade, conforme prescrito pelo Regulamento (CE) n.º 765/2008.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

- **Base jurídica**

A base jurídica para a ação da UE é o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que versa a aproximação das legislações dos Estados-Membros a fim de alcançar a realização dos objetivos enunciados no artigo 26.º do TFUE, nomeadamente o bom funcionamento do mercado interno.

A base jurídica do mercado interno para criar a ENISA foi validada pelo Tribunal de Justiça (no processo C-217/04 Reino Unido da Grã-Bretanha e da Irlanda do Norte contra Parlamento Europeu e Conselho da União Europeia), tendo sido novamente validada pelo regulamento de 2013 que fixa o mandato em vigor da Agência. Além disso, as atividades que refletiriam os objetivos de aumentar a cooperação e a coordenação entre Estados-Membros e aquelas que aditariam capacidades a nível da UE para complementar a ação dos Estados-Membros enquadrar-se-iam na categoria de «cooperação operacional». Tal é especificamente identificado pela Diretiva SRI (cuja base jurídica é o artigo 114.º do TFUE) como um objetivo

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

18 Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE.

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

20 Regulamento (CE) n.º 765/2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93.

a perseguir no contexto da rede de CSIRT, à qual a «ENISA assegura os serviços de secretariado e apoia ativamente a cooperação» (artigo 12.º, n.º 2). Em especial, o artigo 12.º, n.º 3, alínea f), acrescenta que a identificação de outras formas de cooperação operacional é uma tarefa da rede CSIRT, nomeadamente no que se refere: i) às categorias de riscos e de incidentes, ii) aos alertas rápidos, iii) à assistência mútua, iv) aos princípios e às formas de coordenação na resposta dos Estados-Membros a riscos e incidentes de dimensão transfronteiriça.

- A atual fragmentação dos sistemas de certificação de produtos e serviços de TIC é também uma consequência da inexistência de um processo-quadro comum eficaz e juridicamente vinculativo aplicável aos Estados-Membros. Tal dificulta a criação de um mercado interno para os produtos e serviços de TIC e afeta a competitividade da indústria europeia neste setor. A presente proposta visa resolver a fragmentação existente e os obstáculos conexos ao mercado interno mediante a disponibilização de um quadro comum para a criação de sistemas de certificação da cibersegurança válidos em toda a UE.

Subsidiariedade (no caso de competência não exclusiva)

O princípio da subsidiariedade requer a avaliação da necessidade e do valor acrescentado da ação da UE. O respeito da subsidiariedade neste domínio fora já reconhecido aquando da adoção do Regulamento ENISA em vigor[21].

A cibersegurança é uma questão de interesse comum da União. As interdependências entre redes e sistemas de informação são de tal ordem que os intervenientes individuais (públicos e privados, incluindo os cidadãos) muitas vezes não podem enfrentar ameaças, gerir os riscos e os eventuais impactos de ciberincidentes isoladamente. Por um lado, as interdependências entre Estados-Membros, nomeadamente no tocante ao funcionamento de infraestruturas críticas (energia, transportes, água, apenas para referir algumas), tornam a intervenção pública a nível europeu não só benéfica, mas também necessária. Por outro lado, a intervenção da UE pode criar um efeito indireto positivo devido à partilha de boas práticas entre Estados-Membros, que poderá conduzir ao reforço da cibersegurança na União.

Resumindo, no contexto atual e ponderando os futuros cenários, afigura-se que, para **aumentar a ciber-resiliência coletiva** da União, a **ação individual dos Estados-Membros da UE e uma abordagem fragmentada à cibersegurança** não serão suficientes.

A ação da UE é também considerada necessária para resolver a fragmentação dos atuais sistemas de certificação da cibersegurança. Permitirá que os fabricantes beneficiem plenamente de um mercado interno, com economias consideráveis no atinente a custos de ensaios e de reformulação. Embora o acordo de reconhecimento mútuo (ARM) em vigor do Grupo de Altos Funcionários para a Segurança dos Sistemas de Informação (SOG-IS) tenha, por exemplo, alcançado resultados significativos a este respeito, também revelou limitações importantes, que constituem um obstáculo à sua aptidão para proporcionar soluções sustentáveis a longo prazo na realização do potencial pleno do mercado interno.

O valor acrescentado da ação a nível da UE, sobretudo no reforço da cooperação entre Estados-Membros, mas também entre comunidades de segurança das redes e da informação,

[21] 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.

foi reconhecido pelas Conclusões do Conselho de 2016[22] e ressalta também claramente da avaliação da ENISA.

- **Proporcionalidade**

As medidas propostas não excedem o necessário para atingir os seus objetivos políticos. Ademais, o âmbito da intervenção da UE não impede outras ações nacionais no domínio das questões de segurança nacional. A ação da UE está, por conseguinte, justificada com base na subsidiariedade e proporcionalidade.

- **Escolha do instrumento**

A presente proposta revê o Regulamento (UE) n.º 526/2013, que define o mandato e as atribuições atuais da ENISA. Além disso, tendo em conta o papel importante da ENISA na criação e gestão de um quadro de certificação da cibersegurança a nível da UE, o novo mandato da ENISA e o referido Quadro são mais adequadamente criados ao abrigo de um instrumento jurídico único, utilizando-se para tal um regulamento.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DA CONSULTA DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

Avaliações *ex post*/balanços de qualidade da legislação em vigor

A Comissão, de acordo com o roteiro de avaliação[23], avaliou a **relevância, o impacto, a eficácia, a eficiência, a coerência e o valor acrescentado** da Agência relativamente ao seu desempenho, governação, estrutura organizacional interna e métodos de trabalho durante o período 2013-2016. As principais conclusões podem ser sintetizadas como se segue (para mais pormenores consultar o documento de trabalho dos serviços da Comissão sobre o tema, que acompanha a avaliação de impacto).

- **Pertinência:** num contexto de desenvolvimentos tecnológicos e de evolução das ameaças e tendo em conta a necessidade considerável de maior cibersegurança na UE, os objetivos da ENISA demonstraram ser pertinentes. De facto, os Estados-Membros e os organismos da UE apoiam-se nos seus conhecimentos especializados substanciais em questões de cibersegurança. Além disso, afigura-se necessário criar nos Estados-Membros capacidades para melhor compreender e responder às ameaças, e as partes interessadas têm de cooperar em diferentes domínios temáticos e com diferentes instituições. A cibersegurança continua a ser uma prioridade política fundamental da UE, à qual se espera que a ENISA responda; contudo, a conceção da ENISA enquanto agência da UE com um mandato fixo: i) não permite um planeamento a longo prazo e o apoio sustentável aos Estados-Membros e instituições da UE, ii) poderá conduzir a um vazio legal, uma vez que as disposições da Diretiva SRI que conferem atribuições à ENISA são de caráter permanente[24], iii) carece de coerência com uma visão que associa a ENISA a um ecossistema de cibersegurança reforçado da UE.

---

22 Conclusões do Conselho sobre o reforço do sistema de ciberresiliência da Europa e a promoção de uma indústria de cibersegurança competitiva e inovadora (15 de novembro de 2016).

23 http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf.

24 Referência aos artigos 7.º, 9.º, 11.º, 12.º e 19.º da Diretiva relativa à segurança das redes e da informação (Diretiva SRI).

- **Eficácia**: em termos gerais, a ENISA cumpriu os objetivos e executou as suas tarefas. Deu uma contribuição para uma maior segurança das redes e da informação na Europa por intermédio das suas principais atividades (reforço de capacidades, disponibilização de conhecimentos especializados, criação de comunidades e apoio às políticas). No entanto, revelou potencial para melhorias relativamente a cada uma delas. A avaliação concluiu que a ENISA criou eficazmente relações sólidas e fiáveis com algumas das partes interessadas, nomeadamente com os Estados-Membros e a comunidade de CSIRT. As intervenções no domínio do reforço de capacidades foram consideradas eficazes, sobretudo para os Estados-Membros com menos recursos. A estimulação de uma ampla cooperação foi um dos destaques, com as partes interessadas a concordarem amplamente com o papel positivo que a ENISA desempenha em juntar as pessoas. Contudo, a ENISA teve dificuldades em criar um grande impacto no vasto domínio da segurança das redes e da informação. Tal deveu-se igualmente ao facto de dispor de recursos humanos e financeiros francamente limitados para cumprir um mandato tão abrangente. A avaliação concluiu ainda que a ENISA cumpriu parcialmente o objetivo de disponibilizar conhecimentos especializados, devido aos problemas em recrutar peritos (ver também a secção relativa à eficiência infra).
- **Eficiência**: apesar do reduzido orçamento – dos mais baixos quando comparado com outras agências da UE – a Agência conseguiu contribuir para os objetivos visados, demonstrando, em termos gerais, eficiência na utilização dos seus recursos. A avaliação concluiu que, de um modo geral, os processos foram eficientes e que a delineação clara das responsabilidades no seio da organização conduziu a uma boa execução do trabalho. Um dos principais desafios à eficiência da Agência prende-se com as dificuldades da ENISA para recrutar e conservar peritos altamente qualificados. As conclusões mostram que tal pode ser explicado por uma combinação de fatores, tais como as dificuldades gerais do setor público para competir com o setor privado na contratação de peritos altamente especializados, o tipo de contratos (termo certo) que a Agência podia geralmente oferecer e o nível relativamente baixo de atratividade relacionado com a localização da ENISA, associado, nomeadamente, à dificuldade de os cônjuges encontrarem emprego. A localização dividida entre Atenas e Heráclion exigiu esforços adicionais de coordenação e gerou custos suplementares, mas a transferência, em 2013, do departamento de operações principais aumentou a eficiência operacional da Agência.
- **Coerência**: as atividades da ENISA foram, em termos gerais, coerentes com as políticas e atividades das suas partes interessadas, a nível nacional e da UE, mas é necessária uma abordagem mais coordenada à cibersegurança a nível da UE. O potencial para cooperação entre a ENISA e outros organismos da UE não foi plenamente utilizado. A evolução do cenário jurídico e político da UE torna agora o mandato em vigor menos coerente.
- **Valor acrescentado da UE**: o valor acrescentado da ENISA assenta primeiramente na capacidade da Agência de melhorar a cooperação principalmente entre Estados-Membros, mas também com comunidades de segurança das redes e da informação conexas. Não existe outro interveniente a nível da UE que apoie a cooperação entre a mesma variedade de partes interessadas em matéria de segurança das redes e da informação. O valor acrescentado fornecido pela Agência variou de acordo com as necessidades e os recursos divergentes das suas partes interessadas (por exemplo, Estados-Membros grandes face a pequenos; Estados-Membros face a indústria) e a necessidade de a Agência atribuir prioridade às suas atividades de acordo com o

programa de trabalho. A avaliação concluiu que a eventual suspensão da ENISA seria uma oportunidade perdida para todos os Estados-Membros. Não será possível garantir o mesmo nível de criação da comunidade e de cooperação entre Estados-Membros no domínio da cibersegurança. Na ausência de uma agência da UE mais centralizada, o cenário seria mais fragmentado, com a cooperação bilateral ou regional a intervir para preencher um vazio deixado pela ENISA.

No que diz especificamente respeito aos resultados passados e ao futuro da ENISA, as principais tendências que surgem da consulta de 2017 são as seguintes[25]:

- O desempenho global da ENISA durante o período de 2013 a 2016 foi avaliado positivamente pela maior parte dos inquiridos (74 %). Uma maioria de inquiridos considerou ainda que a ENISA está a alcançar os seus diferentes objetivos (pelo menos 63 % para cada um dos objetivos). Os serviços e produtos da ENISA são utilizados regularmente (mensalmente ou com maior frequência) por quase metade dos inquiridos (46 %) e são apreciados por resultarem de um organismo a nível da UE (83 %) e pela sua qualidade (62 %).
- Os inquiridos identificaram algumas lacunas e desafios para o futuro da cibersegurança na UE. Os cinco principais (numa lista de 16) foram: cooperação entre Estados-Membros; capacidade para prevenir, detetar e resolver ciberataques de grande escala; cooperação entre Estados-Membros em matérias relacionadas com a cibersegurança; cooperação e partilha de informações entre diferentes partes interessadas, nomeadamente cooperação público-privada; proteção de infraestruturas críticas contra ciberataques.
- Uma grande maioria (88 %) dos inquiridos considerou que os instrumentos e mecanismos em vigor disponíveis a nível da UE são insuficientes ou apenas parcialmente adequados para responder a esses desafios. Uma grande maioria dos inquiridos (98 %) indicou que um organismo da UE deveria responder a essas necessidades e, entre eles, a ENISA foi considerada a organização certa para o fazer por 99 % dos inquiridos.

Consultas das partes interessadas

- A Comissão organizou uma consulta pública para a revisão da ENISA entre 12 de abril e 5 de julho de 2016, tendo recebido 421 respostas[26]. Segundo os resultados, 67,5 % dos inquiridos manifestaram a opinião de que a ENISA poderia desempenhar um papel na instituição de um quadro harmonizado para a certificação da segurança de produtos e serviços de TIC.

---

[25] Responderam à consulta 90 partes interessadas de 19 Estados-Membros (88 respostas e 2 posições escritas), nomeadamente autoridades nacionais de 15 Estados-Membros e 8 organizações de cúpula que representam um número significativo de empresas europeias, como, por exemplo, a Federação Bancária Europeia, a Europa Digital (representando a indústria da tecnologia digital na Europa) e a Associação dos Operadores Europeus de Redes de Telecomunicações (ETNO). A consulta pública da ENISA foi complementada por várias outras fontes, nomeadamente: i) entrevistas aprofundadas, com aproximadamente 50 intervenientes importantes na comunidade de cibersegurança, ii) inquérito à rede de CSIRT, iii) inquérito ao conselho de administração, à comissão executiva o e ao grupo permanente de partes interessadas da ENISA.

[26] 162 contribuições de cidadãos, 33 de organizações de sociedade civil e de consumidores, 186 da indústria e 40 de autoridades públicas, incluindo as autoridades responsáveis pela aplicação da Diretiva Privacidade e Comunicações Eletrónicas.

Os resultados da consulta de 2016 sobre a PPPc para a cibersegurança[27] demonstram, na secção referente à certificação, que:

- 50,4 % (121 de 240) dos inquiridos não sabem se os sistemas nacionais de certificação são mutuamente reconhecidos nos Estados-Membros da UE. 25,8 % (62 de 240) responderam «Não», ao passo que 23,8 % (57 de 240) responderam «Sim».
- 37,9 % dos inquiridos (91 de 240) pensam que os sistemas de certificação existentes não apoiam as necessidades da indústria europeia. Por outro lado, 17,5 % (42 de 240), sobretudo empresas globais que operam no mercado europeu, manifestaram uma opinião oposta.
- 49,6 % (119 de 240) dos inquiridos afirmam não ser fácil demonstrar equivalência entre normas, sistemas de certificação e rótulos. 37,9 % (91 de 240) responderam «Não sabe», ao passo que 12,5 % (30 de 240) responderam «Sim».

Recolha e utilização de conhecimentos especializados

A Comissão baseou-se no seguinte aconselhamento especializado externo:

- Estudo sobre a avaliação da ENISA (Ramboll/Carsa 2017; SMART n.º 2016/0077);
- Estudo sobre a certificação de segurança e a rotulagem de TIC – Recolha de dados e avaliação de impacto (PriceWaterhouseCoopers 2017; SMART n.º 2016/0029).

Avaliação de impacto

- O relatório de avaliação de impacto sobre esta iniciativa identificou os seguintes problemas a abordar:
- Fragmentação de políticas e abordagens às questões da cibersegurança nos Estados-Membros;
- Dispersão de recursos e fragmentação de abordagens às questões da cibersegurança nas instituições, agências e organismos da UE;
- Conhecimento e informação insuficientes dos cidadãos e empresas, associados ao surgimento crescente de vários sistemas de certificação nacionais e setoriais.

O relatório avaliou as seguintes opções possíveis em relação ao mandato da ENISA:

- manutenção do *statu quo*, o que significaria um mandato alargado que continua limitado no tempo (opção cenário de base);
- expiração do mandato em vigor da ENISA sem renovação e extinção da ENISA (inexistência de intervenção política);
- uma «ENISA reformada»;
- uma agência da UE para a cibersegurança com capacidades operacionais plenas.

O relatório avaliou as seguintes opções possíveis em relação à certificação da cibersegurança:

- inexistência de intervenção política (opção cenário de base);

[27] Responderam à secção referente à certificação 240 partes interessadas de administrações públicas nacionais, grandes empresas, PME, microempresas e organismos de investigação.

- medidas não legislativas (atos não vinculativos);
- um ato legislativo da UE para criar um sistema obrigatório para todos os Estados-Membros com base no sistema SOG-IS;
- um quadro de certificação da cibersegurança das TIC a nível da UE.

A análise conduziu à conclusão de que uma «ENISA reformada» em combinação com um quadro de certificação da cibersegurança das TIC a nível da UE é a opção preferida.

A opção preferida foi considerada a mais eficaz para que a UE consiga alcançar os objetivos identificados: aumentar as capacidades, o grau de preparação, a cooperação, a sensibilização, e a transparência em matéria de cibersegurança e evitar a fragmentação do mercado. Foi igualmente considerada a mais coerente com as prioridades políticas da Estratégia da UE para Cibersegurança e as políticas conexas (por exemplo, a Diretiva SRI), e a Estratégia para o Mercado Único Digital. Além disso, o processo de consulta revelou que a opção preferida beneficia do apoio da maioria das partes interessadas. A análise efetuada no âmbito da avaliação de impacto demonstrou ainda que a opção preferida alcançaria os objetivos mediante uma utilização razoável de recursos.

O Comité de Controlo da Regulamentação da Comissão emitiu um primeiro parecer negativo em 24 de julho, e, após nova apresentação, um parecer positivo em 25 de agosto de 2017. O relatório de avaliação de impacto alterado inclui elementos comprovativos suplementares, as conclusões finais da avaliação da ENISA e explicações adicionais sobre as opções políticas e o seu impacto. O anexo 1 do relatório de avaliação de impacto final resume como foram tidos em consideração os comentários do Comité no segundo parecer. Em especial, o relatório foi atualizado para apresentar mais pormenorizadamente o contexto da cibersegurança na UE, incluindo as medidas que estão incluídos na comunicação conjunta «Resiliência, dissuasão e defesa: Reforçar a cibersegurança na UE», [JOIN(2017) 450] e que têm especial relevância para a ENISA: o plano de ação da UE para a cibersegurança e o Centro Europeu de Investigação e de Competências em matéria de Cibersegurança, em relação aos quais a Agência ligará os seus conselhos sobre necessidades de investigação da UE.

O relatório explica como a reforma da Agência, incluindo as novas atribuições, a melhores condições de emprego e a cooperação estrutural com organismos da UE no terreno, melhorará a sua atratividade enquanto empregador e ajudará a resolver problemas relacionados com o recrutamento de peritos. O anexo 6 do relatório apresenta igualmente uma revisão da estimativa dos custos associados às opções políticas para a ENISA. No que diz respeito ao tema da certificação, o relatório foi revisto a fim de fornecer uma explicação mais pormenorizada, incluindo a apresentação gráfica, da opção preferida, bem como de fornecer estimativas dos custos para os Estados-Membros e a Comissão associados ao novo quadro de certificação. A fundamentação para a escolha da ENISA como ator fundamental nesse quadro foi explicada mais pormenorizadamente, com base nos seus conhecimentos especializados neste domínio e por se tratar da única agência no domínio da cibersegurança a nível da UE. Por último, as secções sobre certificação foram revistas no sentido de clarificar aspetos relacionados com a diferença para o atual sistema SOG-IS e os benefícios associados às diferentes opções políticas e de explicar por que razão o tipo de produtos e serviços de TIC abrangidos por um sistema europeu de certificação será definido no próprio sistema aprovado.

Adequação e simplificação da legislação

Não aplicável

Impacto sobre os direitos fundamentais

A cibersegurança tem um papel essencial na proteção da privacidade e dos dados pessoais das pessoas em conformidade com os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE. Perante a ocorrência de ciberincidentes, a privacidade e a proteção dos nossos dados pessoais ficam claramente expostas. Por conseguinte, a cibersegurança é uma condição necessária para o respeito da privacidade e confidencialidade dos nossos dados pessoais. Nesta perspetiva, ao pretender reforçar a cibersegurança na Europa, a proposta fornece um complemento importante à legislação existente de proteção do direito fundamental à privacidade e dos dados pessoais. A cibersegurança é também essencial para proteger a confidencialidade das nossas comunicações eletrónicas e, portanto, para o exercício da liberdade de expressão e informação e outros direitos conexos, tais como a liberdade de pensamento, consciência e religião.

4. INCIDÊNCIA ORÇAMENTAL

Consultar ficha financeira

5. OUTROS ELEMENTOS

- **Planos de execução e mecanismos de acompanhamento, de avaliação e de informação**

A Comissão acompanhará a aplicação do regulamento e apresentará um relatório sobre a sua avaliação ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu de cinco em cinco anos. Estes relatórios serão públicos e descreverão pormenorizadamente a aplicação efetiva e a execução do presente regulamento.

- **Explicação pormenorizada das disposições específicas da proposta**

O título I do regulamento contém as disposições gerais: o objeto e âmbito de aplicação (artigo 1.º) e as definições (artigo 2.º), incluindo referências a definições relevantes de outros instrumentos da UE, tais como a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva SRI), o Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93, e o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, relativo à normalização europeia.

O título II do regulamento contém as principais disposições relacionadas com a ENISA, a Agência da UE para a Cibersegurança.

O capítulo I deste título define o mandato (artigo 3.º), os objetivos (artigo 4.º) e as atribuições da Agência (artigos 5.º a 11.º).

O capítulo II descreve a organização da ENISA e inclui as principais disposições sobre a sua estrutura (artigo 12.º). Aborda a composição, as regras de voto e as funções do conselho de administração (secção 1, artigos 13.º a 17.º), da comissão executiva (secção 2, artigo 18.º) e do diretor executivo (secção 3, artigo 19.º). Também inclui disposições sobre a composição e papel do grupo permanente de partes interessadas (secção 4, artigo 20.º). Por último, a secção 5 deste capítulo especifica as regras operacionais aplicáveis à Agência, nomeadamente em relação à programação das suas operações, aos conflitos de interesses, à transparência, à confidencialidade e ao acesso a documentos (artigos 21.º a 25.º).

O capítulo III diz respeito à elaboração e à estrutura do orçamento da Agência (artigos 26.º e 27.º), bem como às regras que orientam a sua execução (artigos 28.º e 29.º). Também inclui disposições que facilitam o combate à fraude, à corrupção e a outras atividades ilícitas (artigo 30.º).

O capítulo IV diz respeito ao pessoal da Agência. Inclui disposições gerais sobre o Estatuto dos Funcionários e o Regime Aplicável aos Outros Agentes, bem como regras que orientam os privilégios e imunidades (artigos 31.º e 32.º). Especifica ainda as regras de contratação e nomeação do diretor executivo da Agência (artigo 33.º). Por último, inclui disposições que orientam o recurso a peritos nacionais destacados ou a outros membros do pessoal que não façam parte do quadro de efetivos da Agência (artigo 34.º).

Finalmente, o capítulo V contém as disposições gerais relacionadas com a Agência. Descreve o estatuto jurídico (artigo 35.º) e inclui disposições que regulamentam as questões da responsabilidade, do regime linguístico, da proteção de dados pessoais (artigos 36.º a 38.º), bem como as regras de segurança em matéria de proteção de informações classificadas e de informações sensíveis não classificadas (artigo 40.º). Descreve as regras que orientam a cooperação da Agência com países terceiros e organizações internacionais (artigo 39.º). Por último, contém igualmente disposições relativas à sede e condições de funcionamento da Agência, bem como ao controlo administrativo por parte do Provedor de Justiça Europeu (artigos 41.º e 42.º).

O título III do regulamento institui o quadro europeu de certificação da cibersegurança (o «**Quadro**») de produtos e serviços de TIC como *lex generalis* (artigo 1.º). Define a finalidade geral dos sistemas europeus de certificação da cibersegurança, a saber, garantir que os produtos e serviços de TIC cumprem os requisitos de cibersegurança especificados no atinente à sua capacidade de resistir, com um determinado nível de garantia, a ações que visem comprometer a disponibilidade, autenticidade, integridade ou confidencialidade de dados armazenados, transmitidos ou tratados, ou as funções ou serviços conexos (artigo 43.º). Além disso, elenca os objetivos de segurança aos quais os sistemas europeus de certificação da cibersegurança devem visar dar resposta (artigo 45.º), tais como, entre outros, a capacidade de proteger os dados contra acesso ou divulgação, destruição ou alteração acidental ou não autorizada, e o conteúdo (ou seja, os elementos) dos sistemas europeus de certificação da cibersegurança, tal como a especificação pormenorizada do seu âmbito de aplicação, os objetivos de segurança, os critérios de avaliação, etc. (artigo 47.º).

O título III também estabelece os principais efeitos jurídicos dos sistemas europeus de certificação da cibersegurança, nomeadamente: i) a obrigação de aplicar o sistema a nível nacional e o caráter voluntário da certificação, ii) o efeito de invalidação dos sistemas europeus de certificação da cibersegurança sobre os sistemas nacionais relativos aos mesmos produtos ou serviços (artigos 48.º e 49.º).

Este título estabelece ainda o procedimento para a adoção de sistemas europeus de certificação da cibersegurança e as respetivas funções da Comissão, da ENISA e do grupo europeu para a certificação da cibersegurança («Grupo») (artigo 44.º). Por último, este título estabelece as disposições que regem os organismos de avaliação da conformidade, nomeadamente os seus requisitos, poderes e atribuições, as autoridades nacionais supervisoras da certificação, bem como a aplicação de sanções.

O Grupo é também instituído neste título como um órgão essencial composto por representantes das autoridades nacionais supervisoras da certificação cuja principal função é trabalhar com a ENISA na preparação de sistemas europeus de certificação da cibersegurança e prestar aconselhamento à Comissão sobre questões genéricas ou específicas relativas à política de certificação da cibersegurança.

O título IV do regulamento inclui as disposições finais que descrevem o exercício da delegação, os requisitos de avaliação, a revogação e sucessão, bem como a entrada em vigor.

2017/0225 (COD)

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[28],

Tendo em conta o parecer do Comité das Regiões[29],

Deliberando de acordo com o processo legislativo ordinário,

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

[28] JO C de , p. .
[29] JO C de , p. .

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 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 em grande escala e cibercrises transfronteiriças. 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[30], 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[31], que prolonga o mandato da Agência até março de 2012. O Regulamento (CE)

[30] 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).

[31] 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).

n.º 580/2011[32] 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[33], 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.

(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 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 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 do 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

[32] 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).

[33] 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).

cibersegurança, promovendo a cooperação operacional entre os Estados-Membros e entre os Estados-Membros e as instituições, as agências e os organismos da UE.

(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 contribuir pró-ativamente para os esforços nacionais e da União, exercendo simultaneamente as suas atribuições em plena cooperação com as instituições, organismos, órgãos e agências 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, incluindo a proteção das infraestruturas críticas e a ciber-resiliência. 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, organismos, órgãos e agências da União nos seus esforços para criar e reforçar as capacidades e o grau de preparação para prevenir, detetar e responder a problemas 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. A Agência deve igualmente prestar assistência no desenvolvimento e na atualização de estratégias da União e dos Estados-Membros em matéria de segurança das redes e sistemas de informação, nomeadamente de cibersegurança, promover a sua divulgação e acompanhar o progresso da 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, nomeadamente para apoiar a proteção de infraestruturas críticas, a Agência deve facilitar a criação de centros de partilha e análise de informações (ISAC), divulgando boas práticas e fornecendo orientação sobre instrumentos e procedimentos disponíveis, bem como prestando orientação sobre a abordagem a questões regulamentares relacionadas com a partilha de informações.

(18) A Agência deve agregar e analisar relatórios nacionais das CSIRT e da CERT-UE, criando regras, 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 com a criação da rede de CSIRT.

(19) A Agência deve contribuir para uma resposta a nível da UE, em caso de incidentes de cibersegurança transfronteiriços em grande escala e crises de cibersegurança. Esta função deve 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 anuais de cibersegurança.

(20) Para desempenhar as suas tarefas operacionais, a Agência deve recorrer aos conhecimentos especializados da CERT-UE mediante uma cooperação estruturada, em estreita proximidade física. A cooperação estruturada facilitará as sinergias necessárias e consolidará os conhecimentos especializados da ENISA. Sempre que pertinente, devem ser estabelecidos acordos específicos entre as duas organizações para definir a execução prática dessa cooperação.

(21) Em consonância com as suas tarefas operacionais, a Agência deve ser capaz de apoiar os Estados-Membros, seja prestando aconselhamento ou assistência técnica, ou assegurando a análise de ameaças e incidentes. 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 desempenho das suas tarefas operacionais.

(22) Como parte da cooperação regular a nível técnico para apoiar o conhecimento da situação na União, a Agência deve elaborar regularmente 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 relatórios partilhados com ela pelas CSIRT dos Estados-Membros (a título voluntário) ou pelos pontos únicos de contacto da Diretiva SRI, 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) Os inquéritos técnicos *ex post* a incidentes com impacto significativo em mais do que um Estado-Membro, apoiados ou realizados pela Agência mediante pedido ou com o acordo dos Estados-Membros em causa, devem concentrar-se na prevenção de futuros incidentes e serem levados a cabo sem prejuízo de qualquer processo judicial ou administrativo para imputar culpas ou responsabilidades.

(24) Os Estados-Membros em causa devem fornecer as informações e assistência necessárias à Agência para efeitos do inquérito, sem prejuízo do artigo 346.º do Tratado sobre o Funcionamento da União Europeia ou de outros motivos de política pública.

(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, 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 problemas relacionados com a 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 segurança da infraestrutura de Internet e das infraestruturas críticas, 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 importantes 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, organismos, órgãos e agências da União, ações de sensibilização e campanhas públicas de informação 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) 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, enquanto membro da rede de CSIRT que, além disso, assegura o seu serviço de secretariado, 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 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 anuais de cibersegurança a nível da União e, mediante solicitação, 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 e serviços.

(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, organismos, órgãos e agências da União e, se for caso disso, os Estados-Membros, a seu pedido, sobre as necessidades de investigação em matéria de segurança das redes e da informação, nomeadamente de cibersegurança.

(37) Os problemas de cibersegurança são questões mundiais. É necessário reforçar a cooperação internacional a fim de melhorar as normas de segurança, nomeadamente definindo normas 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, organismos, órgãos e agências 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 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 programa de trabalho, 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[34]. 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[35]. 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.

(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) A avaliação da conformidade é o processo pelo qual se demonstra que um produto, processo, serviço, sistema, pessoa ou organismo satisfaz os requisitos específicos que lhe são aplicáveis. Para efeitos do presente regulamento, a certificação deve ser considerada um tipo de avaliação da conformidade respeitante às características de cibersegurança de um produto, processo, serviço, sistema ou combinação dos mesmos («produtos e serviços de TIC») realizada por um terceiro independente, que não o fabricante do produto ou o prestador do serviço. A certificação, por si só, não pode garantir que os produtos e serviços de TIC certificados são ciberseguros. Trata-se antes de um procedimento e de uma 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.

(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, 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

---

34 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).

35 JO L 8 de 12.1.2001, p. 1.

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, 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 são outras 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 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 ARM do SOG-IS apresenta algumas insuficiências relacionadas com os seus custos elevados e âmbito de aplicação limitado. Até à data, apenas foram desenvolvidos alguns perfis de proteção para produtos digitais, tais como a assinatura digital, o tacógrafo digital e os cartões inteligentes. Mais importante, 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 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 da UE, 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 produtos e serviços de TIC. Esses sistemas devem ser implementados e supervisionados por autoridades nacionais supervisoras da certificação 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 permitem 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 produtos e serviços de TIC certificados ao abrigo desses sistemas cumprem os requisitos especificados. Esses requisitos dizem respeito à capacidade de resistir, com um determinado nível de garantia, a ações que se visem comprometer a disponibilidade, autenticidade, integridade e confidencialidade de dados armazenados, transmitidos ou tratados, as funções conexas ou serviços oferecidos por esses produtos, processos, serviços e sistemas ou acessíveis por via deles, na aceção do presente regulamento. É impossível definir pormenorizadamente no presente regulamento os requisitos de cibersegurança relativos a todos os produtos e serviços de TIC. Os produtos e serviços de TIC e 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 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.

(56) Devem ser atribuídas competências à Comissão para pedir à ENISA que prepare propostas de sistemas destinados a 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 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.

(57) O recurso à certificação europeia da cibersegurança deve manter-se voluntário, salvo disposição em contrário na legislação da União ou nacional. Todavia, 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.

(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 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) É necessário exigir que todos os Estados-Membros designem uma autoridade supervisora da certificação da cibersegurança para supervisionar a conformidade dos organismos de avaliação da conformidade e dos certificados emitidos pelos organismos de avaliação da conformidade estabelecidos no seu território com os requisitos do presente regulamento e dos sistemas de certificação da cibersegurança pertinentes. As autoridades nacionais supervisoras da certificação devem tratar das reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados emitidos por organismos de avaliação da conformidade estabelecidos nos respetivos territórios, 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 supervisoras da certificação 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 autoridades nacionais supervisoras da certificação. As principais atribuições do Grupo serão: 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 Comissão relacionados com a manutenção e revisão dos sistemas europeus de certificação da cibersegurança existentes.

(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.

(62) O apoio da Agência à certificação da cibersegurança deve também incluir ligações com o Comité de Segurança do Conselho e o organismo nacional competente, relativamente à aprovação criptográfica de produtos a utilizar em redes classificadas.

(63) Com vista a especificar mais pormenorizadamente os critérios para a acreditação de organismos de avaliação da conformidade, o poder de adotar atos, nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia, deve ser delegado na Comissão. A Comissão deve efetuar consultas adequadas durante os seus trabalhos preparatórios, nomeadamente a nível de peritos. As consultas devem ser realizadas na observância dos princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016. Em particular, a fim de assegurar a igualdade de participação na preparação de atos delegados, o Parlamento Europeu e o Conselho devem receber todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(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 supervisoras da certificação 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

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 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.

Artigo 2.º
Definições

Para efeitos do presente regulamento, entende-se por:

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

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

4) «Operador de serviços essenciais»: uma entidade pública ou privada na aceção do artigo 4.º, n.º 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, n.º 6, da Diretiva (UE) 2016/1148;

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

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

8) «Ciberameaça»: uma potencial circunstância ou evento que possa afetar negativamente 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 de produtos e serviços de tecnologias da informação e comunicação (TIC) abrangidos pelo âmbito de aplicação desse sistema específico;

10) «Certificado europeu de cibersegurança»: um documento emitido por um organismo de avaliação da conformidade que ateste que um determinado produto ou serviço de

TIC cumpre os requisitos específicos estabelecidos por um sistema europeu de certificação da cibersegurança;

11) «Produto e serviço de TIC»: um elemento ou grupo de elementos de redes e sistemas de informação;

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

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

14) «Avaliação da conformidade»: a avaliação da conformidade na aceção do artigo 2.º, n.º 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, n.º 13, do Regulamento (CE) n.º 765/2008;

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

TÍTULO II
ENISA — a «Agência da União Europeia para a Cibersegurança»

CAPÍTULO I
MANDATO, OBJECTIVOS E ATRIBUIÇÕES

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 na União.

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.

3. Os objetivos e as atribuições da Agência não prejudicam 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 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 relacionadas com a cibersegurança.

3. A Agência apoia o reforço das capacidades e do grau de preparação em toda a União, prestando assistência à União Europeia, aos Estados-Membros e às partes interessadas públicas e privadas a fim de aumentar a proteção das suas redes e sistemas de informação, desenvolver capacidades e competências no domínio da cibersegurança, e alcançar a ciber-resiliência.

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 pertinentes, incluindo o setor privado, em questões relacionadas com a cibersegurança.

5. A Agência aumenta as capacidades em matéria de cibersegurança a nível da União a fim de complementar a ação dos Estados-Membros na prevenção e resposta a ciberameaças, nomeadamente em caso de incidentes transfronteiriços.

6. A Agência promove o recurso à certificação, nomeadamente contribuindo 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.

Artigo 5.º

Atribuições relacionadas com a 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 violação da 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 institui o Código Europeu das Comunicações Eletrónicas].

Artigo 6.º

Atribuições relacionadas com 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 problemas e incidentes de cibersegurança e a sua capacidade de resposta aos mesmos, fornecendo-lhes os conhecimentos especializados necessários;

b) Às instituições, órgãos, organismos e agências da UE, nos seus esforços para melhorar a prevenção, a deteção e a análise de problemas e incidentes de cibersegurança e a sua capacidade de resposta aos mesmos, 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 os progressos da 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 anualmente os exercícios de cibersegurança em grande escala 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, por meio do intercâmbio de boas práticas 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 facilita o estabelecimento de centros de partilha e análise de informações (ISAC) setoriais e apoia-os permanentemente, 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

Atribuições relacionadas com a cooperação operacional a nível da União

1. A Agência apoia a cooperação operacional entre os organismos públicos competentes, e entre as partes interessadas.

2. A Agência coopera a nível operacional e estabelece sinergias com as instituições, organismos, órgãos e agências 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 apoia ativamente a partilha de informações e a cooperação entre os seus membros.

4. A Agência contribui para a cooperação operacional no âmbito da rede de CSIRT, prestando apoio aos Estados-Membros, nomeadamente:

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

   b) Fornecendo-lhes, a seu pedido, assistência técnica em caso de incidentes com um impacto significativo ou substancial;

   c) Analisando vulnerabilidades, artefactos e incidentes.

No exercício destas atribuições, a Agência e a CERT-UE encetam uma cooperação estruturada, de modo a beneficiar de sinergias, em especial no que diz respeito a aspetos operacionais.

5. Na sequência de pedidos apresentados por dois ou mais Estados-Membros afetados, e com o único objetivo de prestar aconselhamento para a prevenção de incidentes

futuros, a Agência presta apoio a inquéritos técnicos *ex post*, ou procede aos mesmos, relativos a incidentes com um impacto significativo ou substancial que as empresas afetadas tenham notificado, em conformidade com a Diretiva (UE) 2016/1148. A Agência procede igualmente a tais inquéritos mediante pedido devidamente justificado da Comissão, com o acordo dos Estados-Membros em causa, em caso de incidentes similares que afetem mais de dois Estados-Membros.

O âmbito dos inquéritos e o procedimento a seguir na sua realização são acordados entre os Estados-Membros em causa e a Agência e não prejudicam qualquer investigação criminal em curso sobre o mesmo incidente. Os inquéritos são concluídos por relatórios técnicos finais elaborados pela Agência, nomeadamente com base nas informações e comentários que os Estados-Membros e as empresas em causa facultarem, e acordados com os Estados-Membros em causa. Será partilhado com a rede de CSIRT um resumo do relatório, centrado nas recomendações para a prevenção de incidentes futuros.

6. A Agência organiza anualmente 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. Os exercícios anuais a nível da União incluem elementos técnicos, operacionais e estratégicos e ajudam a preparar a resposta colaborativa, a nível da União, a incidentes de cibersegurança transfronteiriços em larga escala. A Agência contribui também, se for caso disso, para exercícios de cibersegurança setoriais e ajuda a organizá-los, juntamente com os ISAC competentes, e permite igualmente que estes participem nos exercícios de cibersegurança a nível da União.

7. A Agência 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 (numa base voluntária) ou pelos pontos únicos de contacto no âmbito da Diretiva SRI (em conformidade com o artigo 14.º, n.º 5, da Diretiva SRI); pelo Centro Europeu da Cibercriminalidade (EC3) da Europol; 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, com vista a 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) Apoiando a resposta técnica a um incidente ou crise, nomeadamente facilitando a partilha de soluções técnicas entre Estados-Membros;

   d) Apoiando a comunicação pública relativa a incidentes ou crises;

   e) Ensaiando os planos de cooperação destinados a responder a esses incidentes ou crises.

Artigo 8.º

Atribuições relacionadas com o mercado, a certificação da cibersegurança e a normalização

A Agência:

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

   1) Elaborando propostas de sistemas europeus de certificação da cibersegurança de produtos e serviços de TIC, 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 supervisoras da certificação e a indústria;

b) Facilita o estabelecimento e a adoção de normas europeias e internacionais para a gestão dos riscos e para a segurança de produtos e serviços de TIC, e 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

Atribuições relacionadas com o conhecimento, a informação e a sensibilização

A Agência:

a) Analisa 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 problemas relacionados com a 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 da infraestrutura de Internet e das infraestruturas de apoio aos setores enumerados no anexo II da Diretiva (UE) 2016/1148;

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

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

Artigo 10.º

Atribuições relacionadas com a 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 lhe 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

Atribuições relacionadas com a 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, nomeadamente:

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, mediante pedido da Comissão, o intercâmbio de boas práticas entre as organizações internacionais competentes;

c) Disponibilizando, mediante pedido, conhecimentos especializados à Comissão.

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.°;

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.°;

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

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;

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 internas ou externas;

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.° 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.°, n.º 1, do Estatuto dos Funcionários, e no artigo 6.° 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 eventualidade de este não poder cumprir as suas funções.

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 internas e externas.

   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 por 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. Se necessário, em caso de urgência, a comissão executiva pode tomar determinadas decisões provisórias em nome do conselho de administração, nomeadamente em matéria de gestão administrativa, incluindo a suspensão da delegação de poderes da autoridade investida do poder de nomeação, e em matéria orçamental.

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 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;

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. O diretor executivo decide da necessidade de destacar pessoal para um ou mais Estados-Membros, de modo a assegurar a execução eficaz e eficiente das atribuições da Agência. Antes de decidir da instalação de delegações locais, o diretor executivo deve obter o consentimento prévio da Comissão, do conselho de administração e dos Estados-Membros em causa. 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. Sempre que apropriado ou exigido, deve ser alcançado um acordo com o Estado-Membro em causa.

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, 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.

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[36] 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.

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

---

36 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).

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[37] e 2015/444[38] da Comissão. Essas regras incluem disposições relativas ao intercâmbio, tratamento e armazenamento de informações classificadas.

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

[37] 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).

[38] Decisão da Comissão (UE, Euratom) 2015/444 do Conselho, 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).

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 adotará 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[39], 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.

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[40], 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.

---

39 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).

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

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, ou ambos.
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[41]. 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.

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

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[42].

2. O conselho de administração adota as disposições de execução a que se refere o artigo 24.º, n. 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.

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 ambos. 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.

[42] 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 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 as melhores condições possíveis 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

Sistemas europeus de certificação da cibersegurança

Um sistema europeu de certificação da cibersegurança atesta que os produtos e serviços de TIC que foram certificados em conformidade com esse sistema cumprem os requisitos especificados no que respeita à sua capacidade de resistir, com um determinado nível de garantia, a ações que visem comprometer a disponibilidade, autenticidade, integridade ou confidencialidade de dados armazenados, transmitidos ou tratados, ou as funções ou serviços oferecidos por esses produtos, processos, serviços e sistemas ou acessíveis por via deles.

Artigo 44.º

Elaboração e adoção de um sistema europeu de certificação da cibersegurança

1. Na sequência de um pedido da Comissão, 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. Os Estados-Membros ou o grupo europeu para a certificação da cibersegurança (a seguir designado por «Grupo») criado nos termos do artigo 53.º podem propor à Comissão que se 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 Agência consulta todas as partes interessadas pertinentes e coopera estreitamente com o Grupo. O Grupo presta à ENISA a assistência e o aconselhamento especializado de que esta necessite, no que concerne a elaboração da proposta de sistema, nomeadamente fornecendo pareceres sempre que necessário.
3. A ENISA transmite à Comissão a proposta de sistema europeu de certificação da cibersegurança 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, em conformidade com o artigo 55.º, n.º 2, que estabeleçam sistemas europeus de certificação da cibersegurança de produtos e serviços de TIC que cumpram os requisitos estabelecidos nos artigos 45.º, 46.º e 47.º do presente regulamento.
5. A ENISA mantém um sítio onde disponibiliza informações sobre os sistemas europeus de certificação da cibersegurança, bem como ações de divulgação dos mesmos.

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 ter em conta, conforme aplicável, 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 autorizada;

b) Proteger dados armazenados, transmitidos ou sujeitos a qualquer outro tipo de tratamento contra a destruição acidental ou não autorizada e a perda ou alteração acidental;

c) Assegurar que as pessoas, programas ou máquinas autorizadas podem aceder exclusivamente aos dados, serviços ou funções abrangidos pelos seus direitos de acesso;

d) Registar que dados, funções ou serviços foram comunicados, quando e por quem;

e) Assegurar a possibilidade de verificar que dados, serviços ou funções foram acedidos ou utilizados, 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) Assegurar que os produtos e serviços de TIC são equipados com suportes lógicos atualizados que não contêm vulnerabilidades conhecidas e que incluem mecanismos que permitam atualizações seguras desses suportes.

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 produtos e serviços de TIC certificados por esse sistema.

2. Os níveis de garantia básico, substancial e elevado satisfazem, respetivamente, os seguintes critérios:

a) O nível de garantia básico corresponde a um certificado, emitido no âmbito de um sistema europeu de certificação da cibersegurança, que confere um nível de confiança limitado relativamente às propriedades de cibersegurança declaradas ou reivindicadas por determinado produto ou serviço de TIC, e que se caracteriza por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é reduzir o risco de incidentes de cibersegurança;

b) O nível de garantia substancial corresponde a um certificado, emitido no âmbito de um sistema europeu de certificação da cibersegurança, que confere um nível de confiança substancial relativamente às propriedades de cibersegurança declaradas ou reivindicadas por determinado produto ou serviço de TIC, e que se caracteriza por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é reduzir substancialmente o risco de incidentes de cibersegurança;

c) O nível de garantia elevado corresponde a um certificado, emitido no âmbito de um sistema europeu de certificação da cibersegurança, que confere um nível de confiança mais elevado relativamente às propriedades de cibersegurança declaradas ou reivindicadas por determinado produto ou serviço de TIC que um certificado de nível de garantia substancial, e que se caracteriza por

referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é prevenir incidentes de cibersegurança;

Artigo 47.º

Elementos dos sistemas europeus de certificação da cibersegurança

1. Um sistema europeu de certificação da cibersegurança inclui os seguintes elementos:

   a) Objeto e âmbito da certificação, nomeadamente os tipos ou categorias de produtos e serviços de TIC abrangidos;

   b) Especificação pormenorizada dos requisitos de cibersegurança em relação aos quais os produtos e serviços de TIC específicos são avaliados, por exemplo, por referência a normas ou especificações técnicas da União ou internacionais;

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

   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) Informações necessárias para a certificação que os requerentes devem fornecer 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, incluindo mecanismos para demonstrar a conformidade permanente com os requisitos de cibersegurança especificados, caso o sistema inclua a vertente de acompanhamento;

   h) Condições para a concessão, manutenção, continuação, alargamento e redução do âmbito da certificação;

   i) Regras relativas às consequências da não conformidade de produtos e serviços de TIC certificados com os requisitos de certificação;

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

   k) Regras relativas à conservação de registos por parte dos organismos de avaliação da conformidade;

   l) Identificação dos sistemas nacionais de certificação da cibersegurança que abranjam os mesmos tipos ou categorias de produtos e serviços de TIC;

   m) Conteúdo do certificado emitido.

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 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 48.º

Certificação da cibersegurança

1. Os 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.

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, 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 público será um dos seguintes:

   a) Uma autoridade nacional supervisora da certificação a que se refere o artigo 50.º, n.º 1;

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

   c) Um organismo instituído ao abrigo de legislação, de instrumentos regulamentares ou de outros procedimentos administrativos oficiais de um Estado-Membro afetado e que cumpra os requisitos relativos aos organismos de certificação de produtos, processos e serviços, além da norma ISO/IEC 17065:2012.

5. As pessoas singulares ou coletivas que submetem os seus produtos ou serviços de TIC ao processo de certificação fornecem ao organismo de avaliação da conformidade a que se refere o artigo 51.º todas as informações necessárias para efetuar o procedimento de certificação.

6. Os certificados são emitidos por um período máximo de três anos e podem ser renovados nas mesmas condições, 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 de cibersegurança e os procedimentos conexos relativos a 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 em vigor relativos a 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 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 permanecem válidos até à respetiva data de expiração.

Artigo 50.º

Autoridades nacionais supervisoras da certificação

1. Cada Estado-Membro designa uma autoridade nacional supervisora da certificação.

2. Os Estados-Membros informam a Comissão da identidade da autoridade designada.

3. As autoridades nacionais supervisoras da certificação são independentes das entidades que supervisionam, no que se refere à organização, às decisões de financiamento, à estrutura jurídica e à tomada de decisões.

4. Os Estados-Membros asseguram que as autoridades nacionais supervisoras da certificação 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 supervisoras da certificação:

   a) Controlar e garantir a aplicação das disposições do presente título a nível nacional e supervisionar a conformidade dos certificados que tenham sido emitidos por organismos de avaliação da conformidade estabelecidos nos respetivos territórios com os requisitos estabelecidos no presente título e no correspondente sistema europeu de certificação da cibersegurança;

   b) Controlar e supervisionar as atividades dos organismos de avaliação da conformidade para efeitos do presente regulamento, nomeadamente no que respeita à notificação dos organismos de avaliação da conformidade e às tarefas conexas estabelecidas no artigo 52.º do presente regulamento;

   c) Tratar as reclamações apresentadas por pessoas singulares ou coletivas relativamente a certificados emitidos por organismos de avaliação da conformidade estabelecidos nos respetivos territórios, 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 supervisoras da certificação 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 europeus de certificação da cibersegurança específicos;

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

7. As autoridades nacionais supervisoras da certificação dispõem, no mínimo, das competências para:

a) Solicitar aos organismos de avaliação da conformidade e aos titulares de certificados europeus de cibersegurança que lhes forneçam as informações de que necessitem para o desempenho das suas funções;

b) Conduzir investigações, sob a forma de auditorias, aos organismos de avaliação da conformidade e aos titulares de certificados europeus de cibersegurança, 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 ou os titulares de certificados 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 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 supervisoras da certificação 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 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.

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 revogam 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 supervisoras da certificação 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 para emitirem certificados com os níveis de garantia especificados conforme referido no artigo 46.º, bem como, sem demora, 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 supervisora da certificação 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 por essa mesma autoridade nacional. 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 supervisora da certificação.

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. Esses atos de execução são adotados em conformidade com o 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 autoridades nacionais supervisoras da certificação. As autoridades nacionais supervisoras da certificação são representadas pelos seus presidentes ou por outros representantes de alto nível.

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;

   c) Propor à Comissão que solicite à Agência que elabore uma proposta de sistema europeu de certificação da cibersegurança, em conformidade com o artigo 44.º do presente regulamento;

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 supervisoras da certificação a que se refere o presente título mediante 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.

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

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 é um comité na aceção do Regulamento (UE) n.º 182/2011.
2. Sempre que se remeta para o presente número, aplica-se o artigo 5.º 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) nº 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.

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*

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

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»)

1.2. Domínio(s) de intervenção abrangido(s)

Domínio de intervenção: 09 — Redes de comunicações, conteúdos e tecnologia

Atividade: 09.02 mercado único digital

1.3. Natureza da proposta/iniciativa

☒ A proposta/iniciativa refere-se a **uma nova ação (Título III – Certificação)**

☐A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**[43]

☒A proposta/iniciativa refere-se **à prorrogação de uma ação existente (Título II – mandato da ENISA)**

☐ A proposta/iniciativa refere-se a **uma ação reorientada para uma nova ação**

1.4. Objetivo(s)

1.4.1. Objetivo(s) estratégico(s) plurianual(is) da Comissão visado(s) pela proposta/iniciativa

1. Aumentar a resiliência dos Estados-Membros, das empresas e da UE no seu conjunto

2. Assegurar o funcionamento correto do mercado interno da UE para os produtos e serviços de TIC

3. Aumentar a competitividade mundial das empresas da UE que operam no domínio das TIC.

4. Aproximar as legislações, regulamentações e disposições administrativas dos Estados-Membros que requerem cibersegurança

1.4.2. Objetivo(s) específico(s):

Com os objetivos gerais em mente, no contexto mais lato da estratégia revista para a cibersegurança, o instrumento, ao delinear o âmbito de aplicação e mandato da ENISA e ao criar o quadro europeu de certificação de produtos e serviços de TIC, pretende alcançar os objetivos específicos que se seguem:

1. Aumentar as **capacidades e o grau de preparação** dos Estados-Membros e das empresas.
2. Melhorar a **cooperação e coordenação** entre Estados-Membros e instituições, nas agências e nos organismos da UE.
3. Aumentar as **capacidades a nível da UE para complementar a ação dos Estados-Membros**, designadamente no caso de cibercrises transfronteiriças.

[43] Referidos no artigo 54.º, n.º 2, alíneas a) ou b), do Regulamento Financeiro.

4. Aumentar a **sensibilização** dos cidadãos e das empresas para as questões da cibersegurança.
5. Reforçar a confiança no mercado único digital e na inovação digital mediante uma maior **transparência da garantia de cibersegurança**[44] de produtos e serviços de TIC.

A ENISA contribuirá para alcançar os objetivos supracitados mediante:

Reforço do apoio à elaboração de políticas – prestar orientação e aconselhamento à Comissão e aos Estados-Membros para que atualizem e desenvolvam um quadro normativo holístico no domínio da cibersegurança, bem como políticas e iniciativas legislativas setoriais que envolvam questões de cibersegurança; contribuir para o trabalho do grupo de cooperação [artigo 11.º da Diretiva (UE) 2016/1148], prestando conhecimentos especializados e assistência; apoiar o desenvolvimento e a execução de políticas no domínio da identificação eletrónica e dos serviços de confiança; promover o intercâmbio de boas práticas entre as autoridades competentes;

Reforço do apoio ao reforço de capacidades – prestar apoio aos Estados-Membros, às instituições, organismos, órgãos e agências da União para que desenvolvam e melhorem a prevenção, deteção, análise de problemas e incidentes de cibersegurança, bem como a capacidade de lhes dar resposta; assistir os Estados-Membros, mediante solicitação da sua parte, no desenvolvimento das CSIRT nacionais e das estratégias nacionais para a cibersegurança; assistir as instituições da União no desenvolvimento e revisão de estratégias da União para a cibersegurança; disponibilizar formações em cibersegurança; assistir os Estados-Membros, por via do grupo de cooperação, no intercâmbio de boas práticas; facilitar a criação de centros de partilha e análise de informações (ISAC) setoriais.

Apoio à cooperação operacional e à gestão de crises – apoiar a cooperação entre organismos públicos competentes e entre partes interessadas mediante o estabelecimento de cooperação sistemática com as instituições, organismos, órgãos e agências da União que lidam com a cibersegurança, a cibercriminalidade e a proteção da privacidade e dos dados pessoais; assegurar os serviços de secretariado da rede de CSIRT [artigo 12.º, n.º 2, da Diretiva (UE) 2016/1148], bem como contribuir para a cooperação operacional dentro da rede, prestando, em cooperação com a CERT-UE, apoio aos Estados-Membros, mediante solicitação da sua parte; organizar exercícios de cibersegurança regulares; contribuir para desenvolver uma resposta colaborativa aos incidentes de cibersegurança transfronteiriços em grande escala e às crises de cibersegurança; realizar, em cooperação com a rede de CSIRT, inquéritos técnicos *ex post* relativos a incidentes com um impacto significativo e emitir recomendações de acompanhamento;

Funções relacionadas com o mercado (normalização, certificação) – realizar uma série de funções que apoiem especificamente o mercado interno: «observatório do mercado» da cibersegurança, analisando as tendências importantes do mercado da cibersegurança para adequar melhor a procura e a oferta. apoiar e promover o desenvolvimento e a execução da política da União em matéria de certificação da cibersegurança de produtos e serviços de TIC mediante a preparação de propostas de sistemas europeus de certificação da cibersegurança, assegurando os serviços de secretariado do grupo para a certificação da cibersegurança, disponibilizando orientações e boas práticas relativamente aos requisitos de segurança de produtos e serviços de TIC em cooperação com as autoridades nacionais

[44] Entende-se por «transparência da garantia de cibersegurança»: prestar aos utilizadores informações suficientes sobre as propriedades de cibersegurança que lhes permitam determinar objetivamente o nível de segurança de um determinado produto, serviço ou processo de TIC.

supervisoras da certificação e a indústria; **Reforço do apoio ao conhecimento, à informação e à sensibilização** – prestar assistência e aconselhamento à Comissão e aos Estados-Membros para que atinjam um elevado nível de conhecimento, em toda a União, sobre as questões relacionadas com a SRI e a sua aplicação às empresas interessadas. Tal implica igualmente reunir, organizar e disponibilizar ao público, por intermédio de um portal específico, informação sobre segurança das redes e sistemas de informação [ou cibersegurança]. Outro elemento importante são as ações de sensibilização e as campanhas de informação dirigidas ao público em geral sobre riscos de cibersegurança.

Reforço do apoio à investigação e inovação – prestar aconselhamento sobre necessidades de investigação e definição de prioridades no domínio da cibersegurança;

Apoio à cooperação internacional – apoiar os esforços da União para cooperar com países terceiros e com organizações internacionais no sentido de promover a cooperação internacional em matéria de cibersegurança.

CERTIFICAÇÃO

O quadro de certificação contribuirá para a consecução dos objetivos por via do aumento geral da transparência da garantia de cibersegurança[45] de produtos e serviços de TIC, reforçando, desta forma, a confiança no mercado único digital e na inovação digital. Tal deverá também ajudar a evitar a fragmentação dos sistemas de certificação na UE e dos requisitos de segurança conexos, bem como dos critérios de avaliação, entre Estados-Membros e setores.

1.4.3. Resultados e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada

É expectável que uma ENISA reforçada (apoiando as capacidades, a prevenção, a cooperação e a sensibilização a nível da UE e, por conseguinte, criada para aumentar a ciber-resiliência geral da UE), que contribua igualmente para o quadro de certificação de produtos e serviços de TIC a nível da UE, produza os seguintes impactos (lista não exaustiva):

Impacto global:

— Impacto global positivo no mercado interno, graças à menor fragmentação do mercado e à criação de confiança nas tecnologias digitais mediante uma melhor cooperação, abordagens mais harmonizadas às políticas de cibersegurança da UE e maiores capacidades a nível da UE. Tal deverá produzir um impacto económico positivo ao ajudar a reduzir os custos de incidentes de cibersegurança/cibercriminalidade, cujo impacto económico estimado na União se situa nos 0,41 % do PIB da UE (ou seja, aproximadamente 55 mil milhões de EUR).

Resultados específicos:

Reforço das capacidades e do grau de preparação dos Estados-Membros e das empresas em relação à cibersegurança

— Reforço das capacidades e do grau de preparação dos Estados-Membros em relação à cibersegurança (graças à análise estratégica de longo prazo das ciberameaças e dos

[45] Entende-se por «transparência da garantia de cibersegurança»: prestar aos utilizadores informações suficientes sobre as propriedades de cibersegurança que lhes permitam determinar objetivamente o nível de segurança de um determinado produto, serviço ou processo de TIC.

ciberincidentes, orientação e relatórios, corretagem de conhecimentos especializados e boas práticas, disponibilidade de formação e materiais de formação, exercícios «CyberEurope» reforçados);

— Reforço das capacidades dos intervenientes privados, graças ao apoio à criação de centros de partilha e análise de informações (ISAC) em vários setores;

— Reforço do grau de preparação da UE e dos Estados-Membros em matéria de cibersegurança, graças à disponibilidade de planos bem ensaiados e acordados em caso de incidentes de cibersegurança transfronteiriços em grande escala, testados nos exercícios «CyberEurope».

Reforço da cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da UE

— Reforço da cooperação dentro dos setores público e privado e entre estes;

— Maior coerência na abordagem à execução da Diretiva SRI entre fronteiras e setores;

— Reforço da cooperação no domínio da certificação graças a um quadro institucional que permite o desenvolvimento de sistemas europeus de certificação da cibersegurança e o desenvolvimento de uma política comum neste domínio.

Reforço das capacidades a nível da UE para complementar a ação dos Estados-Membros

— Reforço da «capacidade operacional da UE» para complementar a ação dos Estados-Membros e apoiá-los, mediante pedido e em relação a serviços limitados e identificados previamente. Espera-se que estes aspetos tenham um impacto positivo no êxito da prevenção, deteção e resposta a incidentes a nível dos Estados-Membros e da União.

Aumento da sensibilização dos cidadãos e das empresas para as questões de cibersegurança

— Reforço da sensibilização geral dos cidadãos e das empresas para questões da cibersegurança;

— Reforço da capacidade de tomar decisões de compra fundamentadas relativamente a produtos e serviços de TIC, graças à certificação da cibersegurança.

Reforço da confiança no mercado único digital e na inovação digital mediante uma maior transparência da garantia de cibersegurança de produtos e serviços de TIC

— Reforço da transparência da garantia de cibersegurança[46] de produtos e serviços de TIC, graças à simplificação de procedimentos para certificação da segurança por meio de um quadro a nível da UE;

— Reforço do nível de garantia das propriedades de segurança de produtos e serviços de TIC;

— Maior adoção da certificação da segurança, incentivada por procedimentos simplificados, custos reduzidos e pela perspetiva de oportunidades de negócio a nível na UE não entravadas pela fragmentação do mercado;

— Reforço da competitividade no mercado da cibersegurança da UE devido à redução de custos e encargos administrativos para as PME e à eliminação de possíveis obstáculos à entrada no mercado causados pela diversidade de sistemas nacionais de certificação.

[46] Entende-se por «transparência da garantia de cibersegurança»: prestar aos utilizadores informações suficientes sobre as propriedades de cibersegurança que lhes permitam determinar objetivamente o nível de segurança de um determinado produto, serviço ou processo de TIC.

Outros

— Não se prevê um impacto ambiental significativo em relação nenhum dos objetivos;

— Em relação ao orçamento da UE, esperam-se ganhos de eficiência devidos a uma maior cooperação e coordenação das atividades entre instituições, agências e organismos da UE.

1.4.4. Indicadores de resultados e de impacto

Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa.

(a)

Objetivo: aumentar as capacidades e o grau de preparação dos Estados-Membros e das empresas:

- Número de formações organizadas pela ENISA
- Cobertura geográfica (número de países e zonas) da assistência direta prestada pela ENISA
- Grau de preparação alcançado pelos Estados-Membros em termos de maturidade das CSIRT e da supervisão de medidas regulamentares relacionadas com a cibersegurança
- Número de boas práticas para infraestruturas críticas a nível da UE disponibilizadas pela ENISA
- Número de boas práticas para PME a nível da UE disponibilizadas pela ENISA
- Publicação, pela ENISA, de uma análise estratégica anual das ciberameaças e dos ciberincidentes para identificar tendências emergentes
- Contribuição regular da ENISA para as atividades dos grupos de trabalho para a cibersegurança das organizações europeias de normalização (OEN)

Objetivo: reforçar a cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da UE:

- Número de Estados-Membros que seguiram as recomendações e pareceres da ENISA no seu processo de definição de políticas
- Número de instituições, agências e organismos da UE que seguiram as recomendações e pareceres da ENISA no seu processo de definição de políticas
- Execução correta do programa de trabalho da rede de CSIRT e bom funcionamento na infraestrutura informática e dos canais de comunicação da rede de CSIRT
- Número de relatórios técnicos disponibilizados ao grupo de cooperação e por este utilizados
- Abordagem corrente à execução da Diretiva SRI entre fronteiras e setores
- Número de avaliações da conformidade com a regulamentação realizadas pela ENISA
- Número de ISACS criados em diferentes setores, nomeadamente para infraestruturas críticas

- Criação e funcionamento regular de uma plataforma de informação que divulgue informações sobre cibersegurança resultantes das instituições, das agências e dos organismos da UE
- Contribuição regular para a preparação dos programas de trabalho de investigação e inovação da UE
- Acordo de cooperação entre a ENISA, o EC3 e a CERT-UE em vigor
- Número de sistemas de certificação incluídos e desenvolvidos ao abrigo do Quadro

Objetivo: aumentar as capacidades a nível da UE para complementar a ação dos Estados-Membros, designadamente no caso de cibercrises transfronteiriças:

- Publicação, pela ENISA, de uma análise estratégica anual das ciberameaças e dos ciberincidentes para identificar tendências emergentes
- Publicação, pela ENISA, de informações agregadas sobre incidentes comunicados nos termos da Diretiva SRI
- Número de exercícios pan-europeus coordenados pela Agência e número de Estados-Membros e organizações envolvidas.
- Número de pedidos para apoiar respostas de emergência efetuados pelos Estados-Membros à ENISA e respondidos positivamente pela Agência
- Número de análises de vulnerabilidades, artefactos e incidentes realizadas pela ENISA em cooperação com a CERT-UE
- Disponibilidade de relatórios da situação a nível da UE com base em informações disponibilizadas à ENISA pelos Estados-Membros e outras entidades no caso de ciberincidentes transfronteiriços em grande escala

Objetivo: aumento da sensibilização dos cidadãos e das empresas para as questões da cibersegurança:

- Realização regular de campanhas de sensibilização a nível da UE e nacional e atualização regular dos tópicos, em função das necessidades de aprendizagem emergentes
- Aumento da sensibilização para a cibernética entre os cidadãos da UE
- Realização regular de um questionário de sensibilização para a cibersegurança e aumento da percentagem de respostas corretas ao longo do tempo
- Publicação regular de boas práticas em matéria de cibersegurança e de ciber-higiene dirigidas aos funcionários e às organizações

Objetivo: reforçar a confiança no mercado único digital e na inovação digital mediante uma maior transparência da garantia de cibersegurança[47] de produtos e serviços de TIC:

- Número de sistemas que aderem ao quadro da UE
- Redução dos custos de obtenção de um certificado de segurança de TIC
- Número de organismos de avaliação da conformidade especializados em

[47] Entende-se por «transparência da garantia de cibersegurança»: prestar aos utilizadores informações suficientes sobre as propriedades de cibersegurança que lhes permitam determinar objetivamente o nível de segurança de um determinado produto, serviço ou processo de TIC.

certificação de TIC nos Estados-Membros

- Criação do grupo europeu para a certificação da cibersegurança e organização regular de reuniões
- Orientações para a certificação de acordo com o quadro da UE em vigor
- Publicação regular de análises das principais tendências no mercado da cibersegurança da UE
- Número de produtos e serviços de TIC certificados de acordo com as regras do quadro europeu de certificação da segurança de TIC
- Aumento do número de utilizadores finais que estão conscientes das características de segurança de produtos e serviços de TIC

(b)

1.4.5. Necessidade(s) a satisfazer a curto ou a longo prazo

À luz dos requisitos regulamentares e da rápida evolução do cenário de ameaças à cibersegurança, o mandato da ENISA necessita de ser revisto para estabelecer um conjunto renovado de atribuições e funções, com vista a apoiar eficaz e eficientemente os esforços dos Estados-Membros, das instituições da UE e de outras partes interessadas destinados a garantir um ciberespaço seguro na União Europeia. É delineado o âmbito sugerido do mandato, reforçando as áreas nas quais a Agência demonstrou um claro valor acrescentado e aditando as novas áreas nas quais é necessário apoio, atendendo às novas prioridades e instrumentos políticos, designadamente a Diretiva SRI, a revisão da Estratégia da UE para a Cibersegurança, o futuro plano de ação da UE para a cibersegurança, a cooperação na gestão de cibercrises e a certificação da segurança das TIC. O novo mandato proposto pretende atribuir à Agência um papel mais forte e mais central, nomeadamente no apoio mais ativo aos Estados-Membros no combate a ameaças específicas (capacidade operacional), e torná-la num centro de conhecimentos especializados que apoia os Estados-Membros e a Comissão em matéria de certificação de cibersegurança.

Simultaneamente, a proposta estabelece um quadro europeu de certificação da cibersegurança de produtos e serviços de TIC e especifica as funções e tarefas essenciais da ENISA no domínio da certificação da cibersegurança. O Quadro estabelece disposições e procedimentos comuns que permitem a criação de sistemas de certificação da cibersegurança a nível da UE para produtos/serviços de TIC específicos ou riscos de cibersegurança. A criação de sistemas europeus de certificação da cibersegurança de acordo com o Quadro permitirá que os certificados emitidos nos termos dos mesmos sejam válidos e reconhecidos em todos os Estados-Membros e responder à atual fragmentação do mercado.

1.4.6. Valor acrescentado da intervenção da União

A cibersegurança é genuinamente um problema mundial, que é transfronteiriço por natureza e que está a tornar-se cada vez mais transetorial devido às interdependências entre redes e sistemas de informação. O número, a complexidade e a dimensão dos incidentes de cibersegurança e o seu impacto na economia e na sociedade estão a aumentar com o tempo, sendo expectável que esse aumento continue paralelamente aos desenvolvimentos tecnológicos, como, por exemplo, a proliferação da Internet das coisas. Como tal, não se prevê que a necessidade de um maior esforço comum dos Estados-Membros, das instituições da UE e das partes interessadas privadas para fazer face às ameaças de cibersegurança diminua no futuro.

Desde a sua instituição em 2004, a ENISA visou promover a cooperação entre Estados-Membros e as partes interessadas da SRI, nomeadamente apoiando a cooperação público-privada. Este apoio à cooperação incluiu o trabalho técnico para proporcionar um quadro do cenário de ameaça a nível da UE, a criação de grupos de peritos e a organização de exercícios pan-europeus de ciberincidentes e gestão de crises para os setores públicos e privados (designadamente o «Cyber Europe»). A Diretiva SRI confiou funções suplementares à ENISA, nomeadamente a função de secretariado da rede de CSIRT para cooperação operacional entre os Estados-Membros.

O valor acrescentado da ação a nível da UE, sobretudo no reforço da cooperação entre Estados-Membros, mas também entre comunidades de SRI, foi reconhecido pelas Conclusões do Conselho de 2016[48] e ressalta também claramente da avaliação de 2017 da ENISA, que demonstra que o valor acrescentado da Agência assenta essencialmente na sua capacidade de reforçar a cooperação entre essas partes interessadas. Não existe outro interveniente a nível da UE que apoie a cooperação da mesma variedade de partes interessadas em matéria de SRI.

O valor acrescentado da ENISA em reunir comunidades e partes interessadas em matéria de cibersegurança é também é válido no domínio da certificação. O aumento da cibercriminalidade e das ameaças à segurança conduziu ao surgimento de iniciativas nacionais que definem requisitos de cibersegurança e de certificação de nível elevado para os componentes de TIC utilizados na infraestrutura tradicional. Apesar de importantes, estas iniciativas têm o risco de criar fragmentação do mercado único e obstáculos à interoperabilidade. Um vendedor de TIC poderá ter de se submeter a diversos processos de certificação para poder vender em vários Estados-Membros. É pouco provável que a ineficácia/ineficiência dos sistemas de certificação atuais seja solucionada sem uma intervenção da UE. Na ausência de ação, é muito provável que a fragmentação do mercado aumente a curto/médio prazo (nos próximos 5-10 anos) com o surgimento de novos sistemas de certificação. A falta de coordenação e interoperabilidade entre esses sistemas é um elemento que reduz o potencial do mercado único digital. Tal vem demonstrar o valor acrescentado de criar um quadro europeu de certificação da cibersegurança de produtos e serviços de TIC, criando as condições certas para responder eficazmente ao problema relacionado com a coexistência de diversos procedimentos de certificação em vários Estados-Membros, reduzindo os custos de certificação e, desta forma, tornando a certificação na UE globalmente mais atrativa de um ponto de vista comercial e competitivo.

1.4.7. Lições tiradas de experiências anteriores semelhantes

Nos termos da base jurídica da ENISA, a Comissão realizou uma avaliação da Agência que incluiu um estudo independente, bem como uma consulta pública. A avaliação concluiu que os objetivos da ENISA continuam a ser pertinentes hoje em dia. Num contexto de desenvolvimentos tecnológicos, de ameaças em evolução e de uma necessidade importante de maior segurança das redes e da informação (SRI) na UE, existe uma necessidade de conhecimentos especializados técnicos sobre a evolução de problemas relacionados com a segurança das redes e da informação. Afigura-se necessário criar, nos Estados-Membros, capacidades para compreender e responder às ameaças, e as partes interessadas têm de cooperar em diferentes domínios temáticos e com diferentes instituições.

[48] Conclusões do Conselho sobre o reforço do sistema de ciberresiliência da Europa e a promoção de uma indústria de cibersegurança competitiva e inovadora (15 de novembro de 2016).

A Agência foi bem-sucedida em contribuir para uma maior SRI na Europa ao proporcionar o reforço de capacidades nos 28 Estados-Membros, melhorando a cooperação entre Estados-Membros e partes interessadas de SRI, a prestação de conhecimentos especializados, a criação de comunidade e o apoio a políticas.

Embora a ENISA tenha conseguido produzir um impacto, pelo menos até certo ponto, no vasto domínio da SRI, não conseguiu desenvolver plenamente um nome de marca forte nem ganhar visibilidade suficiente para ser reconhecida como «o» centro de conhecimentos especializados na Europa. Tal explica-se pelo mandato alargado da ENISA, que não está equipada com recursos de dimensão proporcional. Além disso, a ENISA continua a ser a única agência da UE com um mandato fixo, o que limita a sua capacidade de desenvolver uma visão a longo prazo e de apoiar as partes interessadas de um modo sustentável. Isto contrasta igualmente com as disposições da Diretiva SRI, que confiam à ENISA funções sem termo.

No que diz respeito à certificação da cibersegurança de produtos e serviços de TIC, de momento não existe um quadro europeu. No entanto, o aumento da cibercriminalidade e das ameaças à segurança conduziu ao surgimento de iniciativas nacionais, que criam o risco de fragmentação do mercado único.

1.4.8. Compatibilidade e eventual sinergia com outros instrumentos adequados

A iniciativa é deveras coerente com as políticas existentes, nomeadamente no domínio do mercado interno. De facto, foi concebida de acordo com a abordagem geral à cibersegurança, conforme definida pela revisão da Estratégia para o Mercado Único Digital, a fim de complementar um conjunto abrangente de medidas, tais como a revisão da Estratégia da UE para a Cibersegurança, o plano para cooperação em matéria de cibercrises e as iniciativas para combater a cibercriminalidade. Assegurará um alinhamento com as disposições da legislação existente em matéria de cibersegurança e basear-se-á nestas, em especial a Diretiva SRI, a fim de continuar a desenvolver a ciber-resiliência da UE pelo reforço das capacidades, da cooperação, da gestão dos riscos e da sensibilização para as questões do ciberespaço.

As medidas de certificação sugeridas deverão resolver a potencial fragmentação causada pelos sistemas nacionais de certificação existentes e em preparação, contribuindo, assim, para o desenvolvimento do mercado único digital. A proposta também apoia e complementa a execução da Diretiva SRI ao facultar às empresas abrangidas pela diretiva um instrumento para demonstrar a conformidade com os requisitos de SRI em toda a União.

O quadro europeu de certificação da cibersegurança de TIC, tal como proposto, aplica-se sem prejuízo do Regulamento Geral sobre a Proteção de Dados (RGPD)[49] e, em especial, das disposições pertinentes relativas à certificação[50] conforme se aplicam à segurança do tratamento de dados pessoais. Por último, tanto quanto possível, os sistemas propostos no futuro quadro europeu deverão ter por base normas internacionais, para evitar a criação de barreiras comerciais e assegurar a coerência com iniciativas internacionais.

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

[50] Tais como os artigos 42.º (Certificação) e 43.º (Organismos de certificação), bem como os artigos 57.º, 58.º e 70.º relativos, respetivamente, às atribuições e aos poderes pertinentes das autoridades supervisoras independentes e às atribuições do Comité Europeu para a Proteção de Dados.

1.5. Duração da ação e impacto financeiro

☐ Proposta/iniciativa de **duração limitada**

– ☐ Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA

☒ Proposta/iniciativa de **duração ilimitada**

– Aplicação com um período de arranque entre 2019 e 2020,

– seguido de um período de aplicação a um ritmo de cruzeiro

1.6. Modalidade(s) de gestão planeada(s)[51]

☒ **Gestão direta** pela Comissão (Título III – Certificação)

– ☐ nas agências de execução

☐ **Gestão partilhada** com os Estados-Membros

☒ **Gestão indireta**, confiando tarefas de execução orçamental:

☐ a organizações internacionais e respetivas agências (a especificar);

☐ ao BEI e ao Fundo Europeu de Investimento;

☒ aos organismos referidos nos artigos 208.º e 209.º (Título II – ENISA)

☐ a organismos de direito público;

☐ a organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;

☐ a organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;

☐ às pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

Observações:

O regulamento abrange:

— O título II da proposta de regulamento revê o mandato da Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), atribuindo-lhe um papel importante na certificação;

— O título III institui um quadro para a criação de sistemas europeus de certificação da cibersegurança de produtos e serviços de TIC, no qual a ENISA desempenha um papel crucial.

[51] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições

O acompanhamento começará imediatamente após a adoção do instrumento jurídico e centrar-se-á na sua aplicação. A Comissão organizará reuniões com a ENISA, os representantes dos Estados-Membros (por exemplo, grupo de peritos) e as partes interessadas relevantes, em especial para facilitar a execução das regras relativas à certificação, tais como a criação do conselho.

A primeira avaliação ocorrerá cinco anos após a entrada em vigor do instrumento jurídico, contanto que haja dados suficientes disponíveis. O instrumento jurídico inclui uma cláusula explícita de avaliação e revisão [artigo XXX], mediante a qual a Comissão realizará uma avaliação independente. Posteriormente, a Comissão transmitirá ao Parlamento Europeu e ao Conselho a sua avaliação, acompanhada, quando pertinente, de uma proposta de revisão, a fim de medir o impacto do regulamento e o seu valor acrescentado. Serão realizadas novas avaliações de cinco em cinco anos. Será aplicada a metodologia «Legislar Melhor» da Comissão em matéria de avaliação. Estas avaliações serão conduzidas com a ajuda de debates específicos de peritos, estudos e amplas consultas das partes interessadas.

O diretor executivo da ENISA deverá apresentar ao conselho de administração uma avaliação *ex post* das atividades da ENISA de dois em dois anos. A Agência deverá igualmente preparar um plano de ação de acompanhamento relativamente às conclusões das avaliações retrospetivas e comunicar os progressos à Comissão, de dois em dois anos. O conselho de administração será responsável por fiscalizar o acompanhamento adequado dessas conclusões.

Os alegados casos de má administração das atividades da Agência podem ser sujeitos a inquéritos do Provedor de Justiça Europeu, nos termos do disposto no artigo 228.º do Tratado.

As fontes dos dados para a monitorização planeada serão, maioritariamente, a ENISA, o grupo europeu para certificação da cibersegurança, o grupo de cooperação, a rede de CSIRT e as autoridades dos Estados-Membros. Além dos dados resultantes dos relatórios (nomeadamente os relatórios de atividade anuais) da ENISA, do grupo europeu para a certificação da cibersegurança, do grupo de cooperação e da rede de CSIRT, serão utilizadas ferramentas específicas de recolha de dados quando necessário (por exemplo, inquéritos às autoridades nacionais, Eurobarómetro e relatórios da campanha «mês da cibersegurança» e dos exercícios pan-europeus).

2.2. Sistema de gestão e de controlo

2.2.1. Risco(s) identificado(s)

Os riscos identificados são limitados: já existe uma agência da União e o seu mandato será delineado, reforçando as áreas nas quais a Agência demonstrou um claro valor acrescentado e aditando as novas áreas nas quais é necessário apoio, atendendo às novas prioridades e instrumentos políticos, designadamente a Diretiva SRI, a revisão da Estratégia da UE para a Cibersegurança, o futuro plano de ação da UE para a cibersegurança, a cooperação na gestão de cibercrises e a certificação da segurança das TIC.

Por conseguinte, a proposta especifica as funções da Agência e proporciona ganhos em matéria de eficiência. O aumento das competências e atribuições operacionais não representa um risco real, uma vez que estas consistem em complementar a ação dos Estados-Membros e em apoiá-los, mediante pedido e em relação a serviços limitados e identificados previamente.

Além disso, o modelo da Agência proposto, em conformidade com a abordagem comum, assegurará a existência de um controlo suficiente, por forma a garantir que a ENISA contribui para os seus objetivos. Os riscos operacionais e financeiros das alterações propostas são aparentemente limitados.

Simultaneamente, é necessário assegurar recursos financeiros adequados para que a ENISA execute as atribuições conferidas pelo novo mandato, nomeadamente no domínio da certificação.

2.2.2. Meio(s) de controlo previsto(s)

As contas da agência serão sujeitas à aprovação do Tribunal de Contas e ao procedimento de quitação, e estão previstas auditorias.

As atividades da agência estão sujeitas à supervisão do Provedor de Justiça Europeu, nos termos do disposto no artigo 228.º do Tratado.

Ver também pontos 2.1 e 2.2.1 supra.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas

As medidas de prevenção e de proteção da ENISA seriam aplicáveis, especificamente:

— O pagamento de qualquer serviço ou estudo solicitado é controlado pelo pessoal da agência antes de ser efetuado, tendo em conta todas as obrigações contratuais, os princípios económicos e as boas práticas financeiras ou de gestão. Serão incluídas disposições antifraude (supervisão, requisitos de informação, etc.) em todos os acordos e contratos celebrados entre a agência e os destinatários de qualquer pagamento;

— Na luta contra a fraude, corrupção e outras atividades ilícitas, aplicam-se, sem quaisquer restrições, as disposições do 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);

— A agência deve aderir, no prazo de seis meses a contar da entrada em vigor do presente regulamento, ao Acordo Interinstitucional, de 25 de maio de 1999, entre o Parlamento Europeu, o Conselho da União Europeia e a Comissão das Comunidades Europeias relativo aos inquéritos internos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF) e publicar sem demora as disposições adequadas aplicáveis a todo o pessoal da agência.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvida(s)

- Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Natureza da despesa	Participação			
		DD/ DND[52].	dos países EFTA[53]	dos países candidatos[54]	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
1a Competitividade para o crescimento e o emprego	09.0203 ENISA e certificação da segurança das tecnologias da informação e comunicação	DD	SIM	NÃO	NÃO	NÃO
5 Despesas administrativas	09.0101 Despesas relativas ao pessoal no ativo do domínio de intervenção Redes de Comunicação, Conteúdos e Tecnologias 09.0102 Despesas relativas ao pessoal	DND	NÃO	NÃO	NÃO	NÃO

[52] DD = dotações diferenciadas/DND = dotações não diferenciadas.

[53] EFTA: Associação Europeia de Comércio Livre.

[54] Países candidatos e, se for caso disso, candidatos potenciais dos Balcãs Ocidentais.

	externo no ativo do domínio de intervenção Redes de Comunicação, Conteúdos e Tecnologias 09.010211 Outras despesas de gestão					

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

Em milhões de EUR (três casas decimais)

Rubrica do quadro financeiro plurianual	1a	Competitividade para o crescimento e o emprego

ENISA			**Base de referência** **2017 (31.12.2016)**		**2019** ***(a partir de 1.7.2019)***	**2020**	**2021**	**2022**	**TOTAL**
Título 1: Despesas de pessoal *(incluindo também as despesas relacionadas com recrutamento de pessoal, formação, infraestruturas médico-sociais e serviços externos)*	Autorizações	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Pagamentos	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Título 2: Despesas de infraestruturas e funcionamento	Autorizações	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Pagamentos	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Título 3: Despesas operacionais	Autorizações	(3 a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Pagamentos	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
TOTAL das dotações	Autorizações	=1+1a+3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**

para a ENISA	Pagamentos	=2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Rubrica do quadro financeiro plurianual	**5**	Despesas administrativas

Em milhões de EUR (três casas decimais)

		2019 *(a partir de 1.7.2019)*	**2020**	**2021**	**2022**	**TOTAL**
DG: CNECT						
• Recursos humanos		0,216	0,846	0,846	0,846	**2,754**
• Outras despesas administrativas		0,102	0,235	0,238	0,242	**0,817**
TOTAL DG CNECT	Dotações	0,318	1,081	1,084	1,088	**3,571**

Os custos com pessoal foram calculados de acordo com a data de recrutamento planeada (prevê-se que o contrato de trabalho se inicie em 1.7.2019).

A perspetiva de recursos após 2020 é indicativa e não prejudica as propostas da Comissão para o quadro financeiro plurianual após 2020.

TOTAL das dotações da RUBRICA 5 do quadro financeiro plurianual	(Total das autorizações = total dos pagamentos)	0,318	1,081	1,084	1,088	**3,571**

Em milhões de EUR (três casas decimais)

		2019	2020	2021	2022	TOTAL
TOTAL das dotações das RUBRICAS 1 a 5 do quadro financeiro plurianual	Autorizações	16,868	21,727	23,332	24,11	**86,038**
	Pagamentos	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Impacto estimado nas dotações da Agência

– ☐ A proposta/iniciativa não acarreta a utilização de dotações operacionais

– ☒ A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e as realizações[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTAL**
Aumentar as capacidades e o grau de preparação dos Estados-Membros e das empresas.	1,408	1,900	1,931	1,969	7,208
Reforçar a cooperação e coordenação entre Estados-Membros e instituições, agências e organismos da UE.	0,939	1,266	1,288	1,313	4,806
Reforçar as capacidades a nível da UE para complementar a ação dos Estados-Membros, nomeadamente no caso de cibercrises transfronteiriças.	0,704	0,950	0,965	0,985	3,604
Aumentar a sensibilização dos cidadãos e das empresas para as questões de cibersegurança.	0,704	0,950	0,965	0,985	3,604
Reforçar a confiança no mercado único digital e na inovação digital mediante uma maior transparência da garantia de cibersegurança de produtos e serviços de TIC.	0,939	1,266	1,288	1,313	4,806
CUSTO TOTAL	4 694	6,332	6,437	6,565	24,028

[55] Este quadro apresenta apenas as despesas de funcionamento, como para o Título 3.

3.2.3. Impacto estimado nos recursos humanos da Agência

3.2.3.1. Síntese

– ☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

– ☒ A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

	T3/4 2019	**2020**	**2021**	**2022**
Funcionários temporários (graus AD)	4,242	5,695	6,381	6,709
Funcionários temporários (graus AST)	1,601	1,998	2,217	2,217
Agentes contratuais	2,041	2,041	2,041	2,041
Peritos nacionais destacados	0,306	0,447	0,656	0,796
TOTAL	**8,190**	**10,181**	**11,295**	**11,763**

Os custos com pessoal foram calculados de acordo com a data de recrutamento planeada (em relação ao pessoal atual da ENISA, assumiu-se uma situação de pleno emprego a partir de 1.1.2019). Para o pessoal novo, prevê-se que a contratação progressiva se inicie em 1.7.2019 e que se alcance o pleno emprego em 2022. A perspetiva de recursos após 2020 é indicativa e não prejudica as propostas da Comissão para o quadro financeiro plurianual após 2020.

Impacto estimado no pessoal (ETI adicionais) – quadro de pessoal

Grupo de funções e grau	2017 **ENISA atual**	Q3/Q4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

Totais AD	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Totais AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Totais AST/SC					
TOTAL	48	12	10	7	3

Atribuições conferidas ao pessoal AD/AST suplementar destinadas a alcançar os objetivos do instrumento, descritos na secção 1.4.2:

Atribuições	AD	AST	SNE	Total
Política e reforço de capacidades	8	1		9
Cooperação operacional	8	1	7	16
Certificação (atribuições relacionadas com o mercado)	9	3	2	14
Conhecimento, informação e sensibilização	1	1		2
TOTAL	26	6	9	41

Descrição das tarefas a executar:

Atribuições	**Recursos adicionais necessários**
Desenvolvimento e execução de políticas da UE e reforço de capacidades	As atribuições incluirão prestar assistência ao grupo de cooperação, apoiar a execução coerente da SRI entre fronteiras, comunicar regularmente informações sobre o estado da execução do quadro jurídico da UE, aconselhar e coordenar iniciativas de cibersegurança setoriais, nomeadamente na energia, nos transportes (por

	exemplo, aéreo, rodoviário, marítimo, automóveis conectados), na saúde e nas finanças e prestar apoio à criação de centros de partilha e análise de informações (ISAC) em vários setores.
Cooperação operacional e gestão de crises	**As atribuições incluirão:** Assegurar o serviço de secretariado da rede de CSIRT, garantindo, entre outros, o bom funcionamento da infraestrutura informática e dos canais de comunicação da rede de CSIRT. Assegurar a cooperação estruturada com a CERT-UE, o EC3 e outros organismos competentes da UE. Organizar **Exercícios Cyber Europe**[56] — tarefas relacionadas com a transformação do exercício, de um evento bienal para anual, e a garantia de que os exercícios analisam os incidentes do início ao fim. **Assistência técnica** — tarefas que incluem a cooperação estruturada com a CERT-UE para prestar assistência técnica no caso de incidentes significativos e apoiar a análise de acidentes. Tal incluirá prestar assistência aos Estados-Membros para lidarem com incidentes e analisarem vulnerabilidades, artefactos e incidentes. Facilitar a cooperação entre Estados-Membros individuais na resposta a situações de emergência mediante a análise e agregação de relatórios de situação nacionais, baseados em informações disponibilizadas à Agência pelos Estados-Membros e outras entidades. **Plano de ação para a resposta coordenada a ciberincidentes transfronteiriços em grande escala** — a Agência contribuirá para desenvolver uma resposta cooperativa, a nível da União e dos Estados-Membros, a incidentes de cibersegurança transfronteiriços em grande escala ou a crises de cibersegurança mediante um conjunto de tarefas que vão desde contribuir para estabelecer um conhecimento da situação a nível da União até testes dos planos de cooperação para incidentes. **Inquéritos técnicos *ex post* sobre incidentes** —

[56] O «Cyber Europe» é o maior e mais abrangente exercício de cibersegurança da UE até à data, envolvendo mais de 700 profissionais de cibersegurança dos 28 Estados-Membros. O mesmo é realizado de dois em dois anos. A avaliação da ENISA e a Estratégia da UE para Cibersegurança de 2013 chamam a atenção para o facto de que muitas partes interessadas defendem a intensificação do «Cyber Europe», tornando-o num evento anual, dada a rápida evolução da natureza das ciberameaças. No entanto, de momento, isto não é viável devido aos recursos limitados da Agência.

	realizar ou contribuir para inquéritos técnicos *ex post* sobre incidentes, em cooperação com a rede de CSIRT, com vista a emitir recomendações e reforçar as capacidades na forma de relatórios públicos, para prevenir melhor futuros incidentes.
Atribuições relacionadas com o mercado (normalização, certificação)	As tarefas incluirão apoiar ativamente o trabalho realizado no âmbito do quadro de certificação, nomeadamente prestando conhecimentos técnicos especializados para preparar as propostas de sistemas europeus de certificação da cibersegurança. As tarefas incluirão também apoio ao desenvolvimento e execução das políticas da União em matéria de normalização, certificação e observatório do mercado, o que exigirá facilitar a adoção de normas de gestão dos riscos dos produtos eletrónicos, redes e serviços e aconselhar os operadores de serviços essenciais e os prestadores de serviços digitais sobre requisitos de segurança técnica. As tarefas incluirão ainda fornecer análises das principais tendências no mercado da cibersegurança.
Conhecimento, informação e sensibilização:	Com vista a assegurar um acesso facilitado a informação mais bem estruturada sobre riscos de cibersegurança e eventuais soluções, a proposta confere à Agência uma nova atribuição de desenvolver e manter o «polo de informação» da União. As tarefas incluirão reunir, organizar e disponibilizar ao público, por intermédio de um portal específico, informações sobre segurança das redes e sistemas de informação, nomeadamente cibersegurança, fornecidas pelas instituições, agências e organismos da UE. As tarefas incluirão igualmente apoiar as atividades da ENISA no domínio da sensibilização, a fim de permitir à Agência intensificar esses esforços.

3.2.3.2. Necessidades estimadas de recursos humanos para a DG responsável

– ☐ A proposta/iniciativa não acarreta a utilização de recursos humanos.

– ☒ A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

As estimativas devem ser expressas em números inteiros (ou, no máximo, com uma casa decimal)

		Pessoal adicional			
	Base de referência em 2017	Q3/4 2019	2020	2021	2020
• **Lugares do quadro do pessoal (funcionários e agentes temporários)**					
09 01 01 01 (na sede e nos gabinetes de representação da Comissão)	1	2	3		
• **Pessoal externo (em equivalente a tempo completo: ETC)**[57]					
09 01 02 01 (AC, PND e TT da «dotação global»)	1	2			
TOTAL		**4**	**3**		

Descrição das tarefas a executar:

Funcionários e agentes temporários	Representar a Comissão no conselho de administração da agência. Elaborar o parecer da Comissão sobre o documento único de programação da ENISA e acompanhar a sua execução. Supervisionar a elaboração do orçamento da agência e acompanhar a sua execução. Assistir a agência no desenvolvimento das suas atividades em consonância com as políticas da União, nomeadamente pela participação em reuniões pertinentes. Supervisionar a execução do quadro para os sistemas europeus de certificação da cibersegurança de produtos e serviços de TIC. Manter contactos com os Estados-Membros e outras partes interessadas pertinentes relativamente aos esforços de certificação. Cooperar com a ENISA em relação às propostas de sistemas. Preparar propostas de sistemas europeus de

[57] AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

	cibersegurança.
Pessoal externo	Idem

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

– ☐ A proposta/iniciativa é compatível com o atual quadro financeiro plurianual.

– ☒ A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual.

A proposta implicará reprogramar o artigo 09 02 03 devido à revisão do mandato da ENISA, que confere à agência novas atribuições relacionadas, entre outras, com a execução da Diretiva SRI e o quadro europeu de certificação da cibersegurança. Os montantes correspondentes:

Ano	Previsto	Pedido
2019	10,739	16,550
2020	10,954	20,646
2021	Não aplicável	22,248*
2022	Não aplicável	23,023*

*Trata-se de uma estimativa. O financiamento pela UE após 2020 será examinado no contexto de um debate alargado a toda a Comissão sobre todas as propostas para o período após 2020. Significa isto que, uma vez apresentada a sua proposta para o próximo quadro financeiro plurianual, a Comissão apresentará uma ficha financeira legislativa alterada, tendo em conta as conclusões da avaliação de impacto[58].

– ☐ A proposta/iniciativa requer a mobilização do Instrumento de Flexibilidade ou a revisão do quadro financeiro plurianual[59].

3.2.5. Participação de terceiros no financiamento

– ☐ A proposta/iniciativa não prevê o cofinanciamento por terceiros.

– ☒ A proposta/iniciativa prevê o cofinanciamento estimado seguinte:

[58] Hiperligação para a página com a avaliação de impacto

[59] Ver os artigos 11.º e 17.º do Regulamento (UE, Euratom) n.º 1311/2013 do Conselho, que estabelece o quadro financeiro plurianual para o período 2014-2020.

	Ano **2019**	Ano **2020**	Ano **2021**	Ano **2022**
EFTA	p.m.[60]	p.m.	p.m.	p.m.

3.3. Impacto estimado nas receitas

– ☒ A proposta/iniciativa não tem impacto financeiro nas receitas.

– ☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

  – ☐ nos recursos próprios

  – ☐ nos diversos

[60] O montante exato para os anos seguintes será conhecido quando o fator de proporcionalidade da EFTA for fixado para o ano em causa.