COMISSÃO
EUROPEIA

Bruxelas, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação

Um contributo da Comissão Europeia para a reunião de líderes de Salzburgo — 19-20 de setembro de 2018

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Razões e objetivos da proposta

Perante a crescente dependência da vida quotidiana e das economias das tecnologias digitais, os cidadãos estão cada vez mais expostos a ciberincidentes graves. A segurança futura depende da melhoria da capacidade de proteger a União contra as ciberameaças, uma vez que tanto as infraestruturas civis quanto as capacidades militares dependem de sistemas digitais seguros.

A fim de responder aos desafios crescentes, a União aumentou continuamente as suas atividades neste domínio, baseando-se na Estratégia para a Cibersegurança de 2013[1] e nos seus objetivos e princípios para fomentar um ecossistema de cibersegurança fiável, seguro e aberto. Em 2016, a União adotou as primeiras medidas no domínio da cibersegurança por via da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[2] relativa à segurança das redes e da informação.

Face à rápida evolução do cenário da cibersegurança, em setembro de 2017, a Comissão e a alta representante da União para os Negócios Estrangeiros e a Política de Segurança apresentaram uma Comunicação Conjunta[3] intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE», com o intuito de reforçar a resiliência e a capacidade de dissuasão e de resposta a ciberataques da União. A comunicação conjunta, tendo igualmente por base iniciativas anteriores, descreveu um conjunto de propostas de ações, nomeadamente, reforçar a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), criar um quadro de certificação da cibersegurança voluntário a nível da União para aumentar a cibersegurança dos produtos e serviços no mundo digital, bem como um plano de ação para uma resposta célere e coordenada a incidentes e crises de cibersegurança em grande escala.

Na comunicação conjunta, reconheceu-se que também é do interesse estratégico da União assegurar que conserva e desenvolve capacidades tecnológicas essenciais de cibersegurança para proteger o seu mercado único digital e, em especial, para proteger redes e sistemas de informação críticos e prestar serviços fundamentais de cibersegurança. A União deve estar em posição de proteger autonomamente os seus ativos digitais e de competir no mercado mundial de cibersegurança.

Atualmente, a União é um importador líquido de produtos e soluções de cibersegurança e depende em grande medida de fornecedores não europeus[4]. O mercado da cibersegurança tem um valor global de 600 mil milhões de EUR e prevê-se que registe um aumento médio de cerca de 17 % em termos de vendas, número de empresas e postos de trabalho nos próximos

---

1 COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO: Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido [JOIN(2013) 1 final].

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

3 COMUNICAÇÃO CONJUNTA AO PARLAMENTO EUROPEU E AO CONSELHO – Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE [JOIN(2017) 450 final].

4 Projeto de relatório final sobre o Estudo do Mercado da Cibersegurança, 2018.

cinco anos. Todavia, nos 20 países que lideram o mercado da cibersegurança, há apenas seis Estados-Membros[5].

Ao mesmo tempo, existem na União elevados conhecimentos especializados e experiência em cibersegurança — mais de 660 organizações da UE registaram-se no recente levantamento de centros especializados em cibersegurança levado a cabo pela Comissão.[6] Estes conhecimentos especializados, se transformados em produtos e soluções comercializáveis, poderão permitir que a União abranja toda a cadeia de valor da cibersegurança. No entanto, os esforços das comunidades de investigação e industriais estão fragmentados, carecendo de alinhamento e de uma missão comum, o que compromete a competitividade da UE neste domínio, bem como a sua capacidade de proteger os seus ativos digitais. Os setores e subdomínios relevantes da cibersegurança (por exemplo, energia, espaço, defesa, transportes) são hoje em dia insuficientemente apoiados[7]. De igual modo, as sinergias entre os setores civis e militares da cibersegurança não são plenamente exploradas na Europa.

A criação, em 2016, da parceria público-privada contratual («PPPc») para a cibersegurança na União representou um primeiro passo sólido, reunindo as comunidades de investigação, da indústria e do setor público para facilitar a investigação e a inovação em cibersegurança, sendo que, dentro dos limites do quadro financeiro 2014-2020, deverá proporcionar resultados positivos e mais concentrados na investigação e inovação. A PPPc permitiu aos parceiros industriais expressarem o seu compromisso de investimento individual em domínios definidos na agenda estratégica de investigação e inovação da parceria.

Contudo, a União pode perseguir um investimento de uma escala muito maior e necessita de um mecanismo mais eficaz que crie capacidades duradouras, congregue esforços e competências e estimule o desenvolvimento de soluções inovadoras que respondam aos desafios industriais da cibersegurança no domínio das tecnologias polivalentes (por exemplo, inteligência artificial, computação quântica, cifragem progressiva — *blockchain* — e identificação digital segura), bem como em setores críticos (por exemplo, transportes, energia, saúde, finanças, governação, telecomunicações, indústria transformadora, defesa, espaço).

A comunicação conjunta considerou a possibilidade de reforçar a capacidade de cibersegurança da União através de uma rede de centros de competências em cibersegurança com um centro europeu de competências em cibersegurança no âmago. Tal procuraria complementar os esforços existentes de criação de capacidade neste domínio a nível nacional e da União. A comunicação conjunta expressou a intenção da Comissão de lançar uma avaliação de impacto em 2018 para examinar as opções disponíveis com vista a configurar a estrutura. Num primeiro momento e para sustentar uma futura reflexão, a Comissão lançou uma fase-piloto no âmbito do programa Horizonte 2020, para constituir uma rede de centros nacionais com vista a criar uma nova dinâmica em matéria de competências em cibersegurança e de desenvolvimento tecnológico.

Os chefes de Estado e de Governo presentes na Cimeira Digital de Taline, em setembro de 2017, apelaram para que a Comissão se tornasse «um líder mundial em cibersegurança até 2025, para assegurar a confiança e a proteção dos nossos cidadãos, consumidores e empresas em linha e permitir uma Internet livre e regida pela lei».

---

5 Projeto de relatório final sobre o Estudo do Mercado da Cibersegurança, 2018.

6 Relatórios Técnicos do JRC: Centros Especializados Europeus de Cibersegurança, 2018.

7 Relatório Técnico do JRC: Resultados do Exercício de Levantamento (consultar os anexos 4 e 5 para mais pormenores).

As Conclusões do Conselho[8] adotadas em novembro de 2017 instaram a Comissão a apresentar rapidamente uma avaliação de impacto sobre as possíveis opções e propor até meados de 2018 o instrumento jurídico relevante para a execução da iniciativa.

O Programa Europa Digital proposto pela Comissão em junho de 2018[9] procura aumentar e maximizar os benefícios da transformação digital para os cidadãos e empresas europeus em todos os domínios de intervenção relevantes da UE, reforçando as políticas e apoiando as ambições do mercado único digital. O programa propõe uma abordagem coerente e abrangente para assegurar a melhor utilização de tecnologias avançadas e a combinação certa de capacidade técnica e competências humanas para a transformação digital — não apenas no domínio da cibersegurança, mas também no tocante à infraestrutura inteligente de dados, à inteligência artificial, às competências e aplicações avançadas na indústria e em áreas de interesse público. Estes elementos são interdependentes, reforçam-se mutuamente e, quando promovidos simultaneamente, podem alcançar a escala necessária para permitir que a economia dos dados prospere[10]. O *Programa Horizonte Europa*[11] — o próximo programa-quadro de I&I da UE — também coloca a cibersegurança entre as suas prioridades.

Neste contexto, o presente regulamento propõe o estabelecimento de um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança com uma Rede de Centros Nacionais de Coordenação. Este modelo de cooperação concebido à medida deve funcionar como a seguir descrito, de molde a estimular o ecossistema industrial e tecnológico europeu no domínio da cibersegurança: O Centro de Competências facilitará e ajudará a coordenar os trabalhos da Rede e enriquecerá a Comunidade de Competências em Cibersegurança, impulsionando a agenda tecnológica neste domínio e facilitando o acesso aos conhecimentos especializados que forem sendo agregados. O Centro de Competências cumprirá essa função, designadamente, mediante a execução das partes relevantes dos programas Europa Digital e Horizonte Europa, atribuindo de subvenções e executando contratos públicos. Tendo em conta os investimentos consideráveis realizados no domínio da cibersegurança noutras regiões do mundo, bem como a necessidade de coordenar e reunir recursos relevantes na Europa, propõe-se que o Centro de Competências seja uma parceria europeia[12], facilitando, assim, o investimento conjunto da União, dos Estados-Membros e/ou da indústria. Por conseguinte, a proposta exige que os Estados-Membros contribuam com um montante proporcional para as ações do Centro de Competências e da Rede. O principal órgão de tomada de decisões é o Conselho de Administração, no qual todos os Estados-Membros têm assento, embora só os que participem financeiramente tenham direito de voto. O mecanismo de votação no Conselho de Administração segue um princípio de maioria dupla, exigindo 75 % da contribuição financeira e 75 % dos votos para a aprovação de propostas.

---

8 Conclusões do Conselho sobre a Comunicação Conjunta ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE, adotadas pelo Conselho dos Assuntos Gerais em 20 de novembro de 2017.

9 Proposta de Regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027 [COM(2018) 434].

10 Consultar o SWD(2018) 305.

11 Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece o Horizonte Europa – Programa-Quadro de Investigação e Inovação e que define as suas regras de participação e difusão [COM (2018) 435].

12 Na aceção da proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação e que define as suas regras de participação e difusão [COM(2018) 435]; e conforme referido na proposta de regulamento do Parlamento Europeu e do Conselho que cria o programa Europa Digital para o período de 2021-2027 [COM(2018) 434].

Tendo em conta a responsabilidade que lhe incumbe no que toca ao orçamento da União, a Comissão detém 50 % dos votos. No âmbito dos trabalhos do Conselho de Administração, a Comissão recorrerá, sempre que adequado, aos conhecimentos especializados do Serviço Europeu para a Ação Externa. O Conselho de Administração é auxiliado por um Conselho Consultivo Industrial e Científico para garantir o diálogo regular com o setor privado, as organizações de consumidores e outras partes interessadas relevantes.

Trabalhando estreitamente com a Rede de Centros Nacionais de Coordenação e a Comunidade de Competências em Cibersegurança (que integra um grupo amplo e diversificado de intervenientes envolvidos no desenvolvimento de tecnologias de cibersegurança, tais como entidades de investigação, indústrias do lado da oferta e da procura e o setor público) estabelecidas pelo presente regulamento, o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança seria o principal órgão de aplicação dos recursos financeiros da UE dedicados à cibersegurança ao abrigo do *Programa Europa Digital* e do *Programa Horizonte Europa* propostos.

Essa abordagem abrangente permitiria apoiar a cibersegurança em toda a cadeia de valor, desde a investigação ao apoio à implantação e adoção de tecnologias-chave. A participação financeira dos Estados-Membros deve ser proporcional à contribuição financeira da UE para esta iniciativa e constitui um elemento indispensável para o seu sucesso.

Atendendo aos seus conhecimentos especializados específicos e à representação ampla e relevante de partes interessadas, a Organização Europeia de Cibersegurança, que é a contraparte da Comissão na parceria público-privada contratual para a cibersegurança ao abrigo do Horizonte 2020, deverá ser convidada a contribuir para o trabalho do Centro e da Rede.

Além disso, o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança deve também procurar melhorar as sinergias entre as dimensões civil e militar da cibersegurança. Deve apoiar os Estados-Membros e outros intervenientes relevantes mediante a prestação de aconselhamento, a partilha de conhecimentos especializados e a facilitação da colaboração no que diz respeito a projetos e ações. Quando solicitado pelos Estados-Membros poderá também atuar como gestor de projetos, nomeadamente em relação ao Fundo Europeu de Defesa. A presente iniciativa visa contribuir para a resolução dos seguintes problemas:

- **Cooperação insuficiente entre as indústrias de procura e de oferta de cibersegurança.** As empresas europeias são confrontadas com o desafio de se manterem seguras e, em simultâneo, oferecerem produtos e serviços seguros aos seus clientes. No entanto, não são amiúde capazes de proteger apropriadamente os seus produtos, serviços e ativos existentes ou de conceber produtos e serviços inovadores seguros. Os principais ativos de cibersegurança são muitas vezes demasiado dispendiosos para serem concebidos e instalados por intervenientes individuais, cuja principal atividade comercial não está relacionada com a cibersegurança. Ao mesmo tempo, as ligações entre a procura e a oferta do mercado da cibersegurança não estão suficientemente bem desenvolvidas, levando a um fornecimento deficiente de produtos e soluções europeus adaptados às necessidades dos diferentes setores, bem como em níveis insuficientes de confiança entre os intervenientes do mercado.
- **Ausência de um mecanismo de cooperação eficiente entre Estados-Membros para criação de capacidade industrial.** Presentemente, também não existe um mecanismo de cooperação eficiente para os Estados-Membros trabalharem em conjunto no sentido da

criação das capacidades necessárias que apoiem a inovação em matéria de cibersegurança nos setores industriais e a implantação de soluções de cibersegurança europeias de vanguarda. Os mecanismos de cooperação no domínio da cibersegurança disponibilizados aos Estados-Membros nos termos da Diretiva (UE) 2016/1148 não preveem este tipo de atividades no seu mandato.

- **Cooperação insuficiente no seio das comunidades de investigação e industriais e entre estas.** Apesar da capacidade teórica da Europa de cobrir toda a cadeia de valor da cibersegurança, existem setores e subdomínios de cibersegurança relevantes (por exemplo, energia, espaço, defesa, transportes) que são, por hoje, objeto de um fraco apoio da comunidade de investigação, ou que são apenas apoiados por um número limitado de centros (por exemplo, criptografia pós-quântica e quântica, confiança e cibersegurança na IA). Embora esta colaboração exista, obviamente, é muitas vezes uma modalidade a curto prazo, do tipo consultoria, o que não permite participar em planos de investigação a longo prazo para solucionar desafios industriais em matéria de cibersegurança.
- **Cooperação insuficiente entre as comunidades civil e militar de investigação e inovação em matéria de cibersegurança.** O problema dos níveis insuficientes de cooperação também diz respeito às comunidades civil e militar. As sinergias existentes não são plenamente utilizadas devido à falta de mecanismos eficientes que permitam que estas comunidades cooperem eficientemente e criem confiança, o que, mais ainda do que noutros domínios, representa uma condição prévia para uma cooperação bem-sucedida. A esta situação acresce as capacidades financeiras limitadas no mercado de cibersegurança da UE, nomeadamente fundos insuficientes para apoiar a inovação.
- **Coerência com as disposições em vigor no mesmo domínio de intervenção**

A rede de competências em cibersegurança e o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança atuarão como um apoio adicional às disposições políticas e intervenientes existentes em matéria de cibersegurança. O mandato do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança será complementar aos esforços da ENISA, mas tem um foco diferente exige um conjunto diferente de competências. Enquanto o mandato da ENISA prevê uma função consultiva em matéria de investigação e inovação no domínio da cibersegurança na UE, o mandato proposto do Centro incide, em primeiro lugar, noutras tarefas cruciais para o reforço da resiliência em matéria de cibersegurança na UE. Além disso, o mandato da ENISA não prevê os tipos de atividades que serão as principais atribuições do Centro e da Rede — estimular o desenvolvimento e a implantação de tecnologia de cibersegurança e complementar os esforços de criação de capacidades neste domínio a nível nacional e da UE.

O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, juntamente com a rede de competências em cibersegurança, também trabalhará no sentido de apoiar a investigação a fim de facilitar e acelerar os processos de normalização e certificação, em especial os relacionados com os regimes de certificação da cibersegurança na aceção da proposta do Regulamento Cibersegurança[13][14].

[13] 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») [COM(2017) 477 final/3)].

[14] Tal é sem prejuízo dos mecanismos de certificação nos termos do Regulamento Geral sobre a Proteção de Dados, nos quais as autoridades de proteção de dados têm um papel a desempenhar, em consonância

A presente iniciativa está efetivamente a ampliar a parceria público-privada contratual (PPPc) para a cibersegurança, que foi a primeira tentativa à escala da UE de reunir a indústria da cibersegurança, a procura (compradores de produtos e soluções de cibersegurança, incluindo a administração pública e setores críticos como, por exemplo, os transportes, a saúde, a energia, e o financeiro) e a comunidade de investigação para criar uma plataforma de diálogo sustentável e criar condições para coinvestimento voluntário. A PPPc foi criada em 2016 e desencadeou 1,8 mil milhões de EUR de investimento até 2020. Contudo, a escala de investimento em curso noutras partes do mundo (por exemplo, os EUA investiram 19 mil milhões de dólares em cibersegurança só em 2017) revela que a UE tem de fazer mais para alcançar uma massa crítica de investimento e para superar a fragmentação de capacidades espalhadas pela UE.

- **Coerência com outras políticas da União**

O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança atuará como um órgão de execução único para vários programas da União que apoiam a cibersegurança (Programa Europa Digital e Horizonte Europa) e reforçará a coerência e as sinergias entre os mesmos.

Esta iniciativa também permitirá complementar os esforços dos Estados-Membros prestando contributos apropriados para os decisores políticos no domínio da educação, a fim de melhorar as competências em cibersegurança (por exemplo, desenvolvendo conteúdos curriculares de cibersegurança em sistemas educativos civis e militares) para ajudar a desenvolver uma mão de obra qualificada no domínio da cibersegurança na UE — um ativo determinante para as empresas de cibersegurança, bem como para outras indústrias com interesse na cibersegurança. No atinente ao ensino e formação no domínio da ciberdefesa, a presente iniciativa será coerente com os trabalhos em curso da plataforma para o ensino, formação e exercícios no domínio da ciberdefesa estabelecida no âmbito da Academia Europeia de Segurança e Defesa.

Esta iniciativa complementará e apoiará os esforços dos polos de inovação digital estabelecidos ao abrigo do Programa Europa Digital. Os polos de inovação digital são organizações sem fins lucrativos que ajudam as empresas — sobretudo as empresas em fase de arranque, as PME e as empresas de média capitalização — a tornarem-se mais competitivas melhorando os seus processos comerciais/de produção, bem como produtos e serviços, através da inovação inteligente viabilizada pela tecnologia digital. Os polos de inovação digital prestam serviços inovadores orientados para as empresas, tais como recolha de informações sobre o mercado, aconselhamento sobre financiamento, acesso a instalações relevantes de ensaios e experimentação, desenvolvimento de formação e competências, para ajudar os novos produtos ou serviços a alcançarem com êxito o mercado, ou para introduzir melhores processos de produção. Alguns polos de inovação digital com conhecimentos especializados específicos em cibersegurança poderiam ser diretamente envolvidos na Comunidade de Competências em Cibersegurança estabelecida pela presente iniciativa. Na maioria dos casos, os polos de inovação digital que não têm um perfil específico de cibersegurança facilitariam o acesso dos seus membros aos conhecimentos especializados e capacidades em cibersegurança disponíveis na Comunidade de Competências em

---

com o 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)

Cibersegurança, cooperando estreitamente com a Rede de Centros Nacionais de Coordenação e o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança. Os polos de inovação digital apoiariam igualmente a implantação de produtos e soluções inovadores de cibersegurança que vão ao encontro das necessidades das empresas e dos utilizadores finais que servem. Por último, os polos de inovação digital setoriais poderiam partilhar os seus conhecimentos das necessidades reais dos respetivos setores com a Rede e o Centro para contribuir para a reflexão sobre a agenda de investigação e inovação que visa dar resposta aos requisitos industriais.

Procurar-se-á obter sinergias com as Comunidades de Conhecimento e Inovação do Instituto Europeu de Inovação e Tecnologia e, em especial, com a EIT Digital.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

O Centro de Competências é estabelecido com uma dupla base jurídica devido à sua natureza e objetivos específicos. O artigo 187.º do TFUE, que estabelece as estruturas necessárias à boa execução dos programas de investigação, de desenvolvimento tecnológico e de demonstração da União, permite ao Centro de Competências criar sinergias e reunir recursos para investir nas capacidades necessárias a nível dos Estados-Membros e desenvolver ativos europeus partilhados (por exemplo, mediante processos de aquisição conjunta de infraestruturas de teste e experimentação no domínio da cibersegurança). O primeiro parágrafo do artigo 188.º prevê a adoção dessas medidas. No entanto, utilizar o primeiro parágrafo do artigo 188.º como única base jurídica não permitiria que as atividades fossem além da esfera da investigação e desenvolvimento conforme necessário para satisfazer todos os objetivos do Centro de Competências definidos no presente regulamento: apoiar a implantação no mercado de produtos e soluções de cibersegurança, ajudar a indústria europeia de cibersegurança a tornar-se mais competitiva e a aumentar a sua quota de mercado, e acrescentar valor aos esforços nacionais com vista a colmatar a lacuna de competências em cibersegurança. Por conseguinte, a fim de alcançar esses objetivos afigura-se necessário aditar o artigo 173.º, n.º 3, como base jurídica, o qual permite à União prever medidas para apoiar a competitividade da indústria.

• Justificação em termos dos princípios da subsidiariedade e da proporcionalidade

A cibersegurança é uma questão de interesse comum da União, conforme confirmado pelas conclusões do Conselho supracitadas. A dimensão e caráter transfronteiriço de incidentes como o *WannaCry* ou o *NonPetya* constituem um exemplo claro. A natureza e dimensão dos desafios tecnológicos da cibersegurança, bem como a coordenação insuficiente de esforços no seio da indústria, do setor público e das comunidades de investigação, bem como entre estes, obriga a UE a continuar a apoiar esforços de coordenação para reunir uma massa crítica de recursos e assegurar melhores conhecimentos e uma melhor gestão dos ativos. Tal é necessário com vista: aos requisitos em termos de recursos relacionados com certas capacidades para investigação, o desenvolvimento e a implantação em matéria de cibersegurança; à necessidade de disponibilizar acesso a conhecimentos especializados interdisciplinares em cibersegurança (amiúde apenas disponíveis parcialmente a nível nacional) em diferentes disciplinas; à natureza global das cadeias de valor industriais, bem como à atividade dos concorrentes mundiais que trabalham nos mercados.

Tal exige recursos e conhecimentos especializados a um nível que dificilmente poderá ser satisfeito com a ação individual de qualquer Estado-Membro. Por exemplo, uma rede de comunicação quântica pan-europeia poderia exigir um investimento da UE de aproximadamente 900 milhões de EUR, dependendo dos investimentos efetuados pelos Estados-Membros (para que fosse interligada/complementada) e do grau de possível reutilização das infraestruturas existentes. A iniciativa será fundamental para reunir financiamento e permitir que este tipo de investimento se concretize na União.

Os objetivos desta iniciativa não podem ser plenamente alcançados pelos Estados-Membros isoladamente. Conforme demonstrado, podem ser mais facilmente alcançados a nível da União agregando esforços e evitando a sua duplicação desnecessária, ajudando a alcançar massa crítica de investimento e assegurando que o investimento público é utilizado de modo eficaz. Ao mesmo tempo, de acordo com o princípio da proporcionalidade, o presente regulamento não excede o necessário para atingir esse objetivo. A ação da UE justifica-se, por conseguinte, com base na subsidiariedade e proporcionalidade.

O presente instrumento não prevê quaisquer novas obrigações regulamentares para as empresas. Ao mesmo tempo, as empresas e sobretudo as PME vão provavelmente reduzir os custos relacionados com os seus esforços de conceção de produtos inovadores e ciberseguros, uma vez que a iniciativa permite reunir recursos para investir nas capacidades necessárias a nível dos Estados-Membros ou desenvolver ativos partilhados europeus (por exemplo, mediante processos de aquisição conjunta de infraestruturas de testes e experimentação no domínio da cibersegurança). Estes ativos poderiam ser utilizados pelas indústrias e PME em diferentes setores, a fim de assegurar que os seus produtos são ciberseguros, tornando, assim, a cibersegurança numa vantagem competitiva.

- **Escolha do instrumento**

O instrumento proposto estabelece um órgão dedicado à execução das ações de cibersegurança ao abrigo do Programa Europa Digital e do Programa Horizonte Europa. Descreve o respetivo mandato, funções e estrutura de governação. A criação de um órgão da União desse tipo requer a adoção de um regulamento.

3. CONSULTAS DAS PARTES INTERESSADAS E AVALIAÇÕES DE IMPACTO

A proposta de criar uma rede de competências em cibersegurança com um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança representa uma nova iniciativa. Atua como uma continuação e intensificação da parceria público-privada contratual para a cibersegurança criada em 2016.

- **Consulta das partes interessadas**

A cibersegurança é um tópico vasto e intersetorial. A Comissão recorreu a diferentes métodos de consulta para se certificar de que o interesse público geral da União — em oposição a interesses especiais de uma gama limitada de grupos de partes interessadas — está bem patente nesta iniciativa. Este método assegura a transparência e a responsabilização no trabalho da Comissão. Apesar de não ter sido realizada qualquer consulta pública aberta para esta iniciativa, dado o seu público-alvo (comunidade industrial e de investigação e Estados-Membros), a temática já tinha sido abrangida por diversas outras consultas públicas:

- uma consulta pública aberta geral, realizada em 2018, nos domínios do investimento, da investigação e inovação, das PME e do mercado único;

- uma consulta pública em linha com a duração de 12 semanas, lançada em 2017, para procurar recolher opiniões do grande público (cerca de 90 respondentes) sobre a avaliação e revisão da ENISA;
- uma consulta pública em linha com a duração de 12 semanas, realizada em 2016, por ocasião do lançamento da parceria público-privada contratual para a cibersegurança (cerca de 240 respondentes).

A Comissão também organizou consultas específicas sobre esta iniciativa, incluindo seminários, reuniões e pedidos direcionados para obter contributos (da ENISA e da Agência Europeia de Defesa). O período de consulta estendeu-se durante mais de seis meses, de novembro de 2017 até março de 2018. A Comissão também procedeu a um levantamento dos centros de conhecimentos especializados, o que permitiu recolher contributos de 665 centros de conhecimentos especializados em cibersegurança sobre o seu saber-fazer, atividades, domínios de trabalho e cooperação internacional. O inquérito foi lançado em janeiro e as respostas enviadas até 8 de março de 2018 foram tidas em conta para a análise do relatório.

As partes interessadas das comunidades industriais e de investigação consideraram que o Centro de Competências e a Rede poderiam acrescentar valor aos esforços atuais a nível nacional, ajudando a criar um ecossistema de cibersegurança a nível da Europa que permita uma melhor cooperação entre as comunidades industriais e da investigação. Também consideraram necessário que a UE e os Estados-Membros adotem uma perspetiva estratégica, proativa e de mais longo prazo da política industrial em matéria de cibersegurança que vá além da mera investigação e inovação. As partes interessadas manifestaram a necessidade de obter acesso a capacidades fundamentais, tais como instalações de testes e experimentação, e de uma maior ambição nas medidas destinadas a colmatar a lacuna de competências em cibersegurança, por exemplo, através de projetos europeus de grande escala que atraiam os melhores talentos. Tudo o exposto anteriormente é igualmente considerado necessário para a Europa ser reconhecida mundialmente como líder em cibersegurança.

Os Estados-Membros, no âmbito das atividades de consulta realizadas desde setembro último[15], bem como em conclusões do Conselho específicas[16], saudaram a intenção de criar uma rede de competências em cibersegurança para estimular o desenvolvimento e a implantação de tecnologias de cibersegurança, sublinhando a necessidade de abranger todos os Estados-Membros e os seus atuais centros de excelência e competências e de dar especial atenção à complementaridade. Concretamente, no atinente ao futuro Centro de Competências, os Estados-Membros salientaram a importância do seu papel de coordenação no apoio à rede. Em especial no que se refere às atividades e necessidades nacionais de ciberdefesa, o exercício de levantamento das necessidades de ciberdefesa dos Estados-Membros, realizado pelo Serviço Europeu para a Ação Externa em março de 2018, demonstrou que a maioria dos Estados-Membros entende o valor acrescentado da UE no apoio ao ensino e formação em cibersegurança, bem como no apoio à indústria através da investigação e desenvolvimento[17]. Na sua opinião, a iniciativa deveria ser efetivamente aplicada juntamente com os Estados-Membros ou entidades apoiadas por estes. As colaborações entre as comunidades da indústria, da investigação e/ou do setor público reuniriam e reforçariam as entidades e

[15] Por exemplo, a mesa redonda de alto nível que reuniu Estados-Membros, o vice-presidente da Comissão, Andrus Ansip e a comissária Mariya Gabriel, em 5 de dezembro de 2017.

[16] Conselho dos Assuntos Gerais: Conclusões do Conselho sobre a Comunicação Conjunta ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE (20 de novembro de 2017).

[17] SEAE, março de 2018.

esforços existentes para não criar outros novos. Os Estados-Membros também deveriam ser envolvidos na definição de ações específicas destinadas ao setor público na qualidade de utilizador direto de tecnologia e conhecimentos especializados de cibersegurança.

- **Avaliação de impacto**

Uma avaliação de impacto que acompanha esta iniciativa foi apresentada ao Comité de Controlo da Regulamentação em 11 de abril de 2017 e recebeu um parecer favorável com reservas. A avaliação de impacto foi subsequentemente revista à luz das observações do Comité. O parecer do Comité e o anexo que explica como foram tidas em conta as observações do Comité são publicados com a presente proposta.

Foram tidas em consideração na avaliação de impacto várias opções políticas, tanto legislativas como não legislativas. As opções que se seguem foram selecionadas para uma avaliação aprofundada:

- Cenário de base — Opção colaborativa — assume a continuação da abordagem atual de criar capacidades industriais e tecnológicas de cibersegurança na UE através do apoio à investigação e inovação e de mecanismos de colaboração conexos ao abrigo do QF9.
- Opção 1: Rede de Competências em Cibersegurança com um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança com um mandato duplo para pôr em prática medidas de apoio às tecnologias industriais, bem como no domínio da investigação e inovação.
- Opção 2: Rede de Competências em Cibersegurança com um Centro Europeu de Investigação e Competências em Cibersegurança centrado em atividades de investigação e inovação.

As opções descartadas numa fase inicial incluíram 1) não tomar qualquer ação; 2) criar apenas a rede de competências em cibersegurança; 3) criar apenas uma estrutura centralizada; 4) utilizar uma agência existente [Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), Agência de Execução para a Investigação (REA) ou Agência de Execução para a Inovação e as Redes (INEA)].

A análise concluiu que a opção 1 é mais adequada para alcançar os objetivos da iniciativa ao mesmo tempo que oferece o maior impacto económico, social e ambiental e salvaguarda os interesses da União. Os principais argumentos a favor desta opção incluíram a capacidade de criar uma verdadeira política industrial de cibersegurança mediante o apoio a atividades relacionadas não apenas com a investigação e o desenvolvimento, mas também com a implantação no mercado; a flexibilidade para permitir diferentes modelos de cooperação com a rede de centros de competências a fim de otimizar a utilização dos conhecimentos e recursos existentes; a capacidade de estruturar a cooperação e os compromissos conjuntos das partes interessadas públicas e privadas provenientes de todos os setores relevantes, nomeadamente a defesa. Por último, a opção 1 permite igualmente aumentar sinergias e pode atuar como um mecanismo de execução para duas fontes diferentes de financiamento da cibersegurança da UE ao abrigo do próximo quadro financeiro plurianual (Programa Europa Digital, Horizonte Europa).

- **Direitos fundamentais**

A iniciativa permitirá às autoridades públicas e indústrias nos Estados-Membros prevenir e responder mais eficazmente a ciberameaças, mediante a oferta de produtos e soluções mais

seguros com os quais aquelas se poderão munir. Este aspeto é particularmente relevante para a proteção do acesso a serviços essenciais (por exemplo, transportes, saúde, serviços bancários e financeiros).

Uma maior capacidade da União Europeia de proteger autonomamente os seus produtos e serviços é também suscetível de ajudar os cidadãos a usufruírem dos seus direitos e valores democráticos (por exemplo, proteger melhor os seus direitos relacionados com a informação consagrados na Carta dos Direitos Fundamentais, sobretudo o direito à proteção dos dados pessoais e da vida privada) e, consequentemente, aumentar a sua confiança na sociedade e economia digitais.

4. INCIDÊNCIA ORÇAMENTAL

O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, em cooperação com a rede de competências em cibersegurança, será o principal órgão de execução dos recursos financeiros da UE dedicados à cibersegurança ao abrigo do Europa Digital e do Horizonte Europa.

As implicações orçamentais relacionadas com a execução do programa Europa Digital estão listadas em pormenor na ficha financeira legislativa anexada à presente proposta. A contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), será proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político. A proposta terá por base o resultado do processo de planeamento estratégico conforme definido no artigo 6.º, n.º 6. do Regulamento XXX [programa-quadro Horizonte Europa].

5. OUTROS ELEMENTOS

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

Uma cláusula de avaliação explícita, mediante a qual a Comissão levará a cabo uma avaliação independente, está prevista na presente proposta (artigo 38.º). 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. Será aplicada a metodologia «Legislar Melhor» da Comissão em matéria de avaliação.

O diretor executivo apresenta ao Conselho de Administração uma avaliação *ex post* das atividades do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e da Rede a cada dois anos, conforme definido no artigo 17.º da presente proposta. O diretor executivo 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 é responsável por monitorizar o acompanhamento adequado dessas conclusões, conforme estabelecido no artigo 16.º da presente proposta.

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

2018/0328 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação

Um contributo da Comissão Europeia para a reunião de líderes de Salzburgo — 19-20 de setembro de 2018

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 173.º, n.º 3, e o artigo 188.º, primeiro parágrafo,

Tendo em conta a proposta da Comissão Europeia,

Tendo em conta o parecer do Comité Económico e Social Europeu[18],

Tendo em conta o parecer do Comité das Regiões[19],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) A nossa vida quotidiana e as nossas economias estão cada vez mais dependentes das tecnologias digitais e os cidadãos estão cada vez mais expostos a ciberincidentes graves. A segurança futura depende, entre outros aspetos, da melhoria da capacidade tecnológica e industrial de proteger a União contra ciberameaças, uma vez que tanto as infraestruturas civis quanto as capacidades militares dependem de sistemas digitais seguros.

(2) A União aumentou continuamente as suas atividades para responder aos desafios crescentes de cibersegurança no seguimento da Estratégia para a Cibersegurança de 2013[20] destinada a promover um ecossistema de cibersegurança fiável, seguro e aberto. Em 2016, a União adotou as primeiras medidas no domínio da cibersegurança através da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[21] relativa à segurança das redes e da informação.

---

18 JO C […] de […], p. […].

19 JO C […] de […], p. […].

20 Comunicação conjunta ao Parlamento Europeu e ao Conselho: Estratégia da União Europeia para a cibersegurança: um ciberespaço aberto, seguro e protegido [JOIN(2013) 1 final].

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

(3) Em setembro de 2017, a Comissão e a alta representante da União para os Negócios Estrangeiros e a Política de Segurança apresentaram uma Comunicação Conjunta[22] intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE», com o intuito de reforçar a resiliência e a capacidade de dissuasão e de resposta a ciberataques da União.

(4) Os chefes de Estado e de Governo presentes na Cimeira Digital de Taline, em setembro de 2017, apelaram para que a Comissão se tornasse «um líder mundial em cibersegurança até 2025, para assegurar a confiança e a proteção dos nossos cidadãos, consumidores e empresas em linha e permitir uma Internet livre e regida pela lei».

(5) A perturbação substancial da rede e dos sistemas de informação pode afetar Estados-Membros individuais e o conjunto da União. Por consequência, a segurança das redes e dos sistemas de informação é essencial para o bom funcionamento do mercado interno. Presentemente, a União depende de prestadores de serviços de cibersegurança não europeus. Contudo, é também do interesse estratégico da União assegurar que conserva e desenvolve capacidades tecnológicas essenciais de cibersegurança para proteger o seu mercado único digital e, em especial, para proteger redes e sistemas de informação críticos e prestar serviços fundamentais de cibersegurança.

(6) Existem na União elevados conhecimentos especializados e experiência em investigação, tecnologia e desenvolvimento industrial no domínio da cibersegurança, mas os esforços das comunidades industriais e de investigação estão fragmentados, carecendo de alinhamento e de uma missão comum, o que compromete a competitividade neste domínio. Esses esforços e conhecimentos especializados devem ser agrupados, colocados em rede e utilizados de modo eficiente para reforçar e complementar as capacidades de investigação, tecnológicas e industriais existentes a nível da União e nacional.

(7) As Conclusões do Conselho, adotadas em novembro de 2017, instaram a Comissão a apresentar rapidamente uma avaliação de impacto sobre as possíveis opções para criar uma rede de centros de competências em matéria de cibersegurança com o Centro Europeu de Investigação e de Competências e propor o instrumento jurídico relevante até meados de 2018.

(8) O Centro de Competências deverá ser o principal instrumento da União para reunir investimento em investigação, tecnologia e desenvolvimento industrial no domínio da cibersegurança e para executar os projetos e iniciativas relevantes juntamente com a Rede de Competências em Cibersegurança. Deverá prestar apoio financeiro relacionado com a cibersegurança proveniente dos programas Horizonte Europa e Europa Digital e deve estar aberto ao Fundo Europeu de Desenvolvimento Regional e a outros programas, quando pertinente. Esta abordagem deverá contribuir para criar sinergias e coordenar o apoio financeiro relacionado com a investigação, a inovação, a tecnologia e o desenvolvimento industrial no domínio da cibersegurança e evitar a duplicação.

(9) Tendo em conta que os objetivos desta iniciativa podem ser mais adequadamente alcançados se todos os Estados-Membros ou o maior número possível de Estados-Membros participarem, e como incentivo a essa participação, apenas os

[22] Comunicação Conjunta ao Parlamento Europeu e ao Conselho – Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE [JOIN(2017) 450 final].

Estados-Membros que contribuam financeiramente para os custos administrativos e operacionais do Centro de Competências deverão beneficiar de direitos de voto.

(10) A participação financeira dos Estados-Membros deve ser proporcional à contribuição financeira da União para esta iniciativa.

(11) O Centro de Competências deverá facilitar e ajudar a coordenar o trabalho da Rede de Competências no domínio da Cibersegurança («a Rede»), constituída pelos centros nacionais de coordenação em cada Estado-Membro. Os centros nacionais de coordenação devem receber apoio financeiro direto da União, incluindo subvenções concedidas sem convites à apresentação de propostas, a fim de realizarem atividades relacionadas com o presente regulamento.

(12) Os centros nacionais de coordenação são selecionados pelos Estados-Membros. Além da capacidade administrativa necessária, os centros devem possuir ou ter acesso direto a conhecimentos tecnológicos especializados em matéria de cibersegurança, nomeadamente em domínios como a criptografia, os serviços de segurança de TIC, a deteção de intrusões, a segurança de sistemas, a segurança de redes, a segurança de programas e aplicações informáticos, ou os aspetos humanos e sociais da segurança e da privacidade. Devem igualmente ter capacidade para se envolverem e coordenarem eficazmente com a indústria, o setor público, incluindo as autoridades designadas nos termos da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[23], e a comunidade de investigação.

(13) Caso seja prestado apoio financeiro aos centros nacionais de coordenação com vista a apoiar terceiros a nível nacional, o mesmo deve ser transmitido às partes interessadas relevantes mediante convenções de subvenção em cascata.

(14) Tecnologias emergentes como a inteligência artificial, a Internet das coisas, a computação de alto desempenho (CAD) e a computação quântica, a cifragem progressiva e conceitos como a identificação digital segura criam novos desafios para a cibersegurança, oferecendo simultaneamente soluções. Avaliar e validar a robustez dos sistemas de TIC existentes e futuros exigirá testar soluções de segurança contra ataques perpetrados em máquinas de CAD e quânticas. O Centro de Competência, a Rede e a Comunidade de Competências em Cibersegurança ajudarão a fazer avançar e difundir as mais recentes soluções de cibersegurança. Ao mesmo tempo, o Centro de Competências e a Rede deverão estar ao serviço de programadores e operadores em setores críticos como os transportes, a energia, a saúde, as finanças, a governação, as telecomunicações, a indústria transformadora, a defesa e o espaço para ajudá-los a resolver os seus problemas de cibersegurança.

(15) O Centro de Competências deverá assumir diversas funções principais. Em primeiro lugar, deverá facilitar e ajudar a coordenar o trabalho da Rede Europeia de Competências em Cibersegurança e alimentar a Comunidade de Competências em Cibersegurança. O Centro deverá impulsionar a agenda tecnológica da cibersegurança e facilitar o acesso aos conhecimentos especializados recolhidos na Rede e na Comunidade de Competências em Cibersegurança. Em segundo lugar, deverá executar partes relevantes dos programas Europa Digital e Horizonte Europa mediante a atribuição de subvenções, normalmente na sequência de um convite concorrencial à

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

apresentação de propostas. Em terceiro lugar, o Centro de Competências deverá facilitar o investimento conjunto por parte da União, dos Estados-Membros e/ou da indústria.

(16) O Centro de Competências deverá estimular e apoiar a cooperação e a coordenação das atividades da Comunidade de Competências em Cibersegurança, o que envolverá um grupo amplo, aberto e diversificado de intervenientes envolvidos no domínio da tecnologia de cibersegurança. Essa comunidade deverá incluir, nomeadamente, entidades de investigação, indústrias do lado da oferta e do lado da procura e o setor público. A Comunidade de Competências em Cibersegurança deverá fornecer contributos para as atividades e para o plano de trabalho do Centro de Competências e deverá também beneficiar das atividades de formação de comunidades do Centro de Competências e da Rede mas, por outro lado, não deve ser privilegiada no tocante aos convites à apresentação de propostas ou aos concursos públicos.

(17) A fim de responder às necessidades das indústrias do lado da oferta e do lado da procura, a missão do Centro de Competências de prestar conhecimentos e assistência técnica em matéria de cibersegurança às indústrias deve referir-se aos produtos e serviços de TIC e a todos os demais produtos e soluções industriais e tecnológicos nos quais a cibersegurança tem de ser incorporada.

(18) Nos casos em que o Centro de Competências e a Rede devam procurar obter sinergias entre as esferas civil e militar da cibersegurança, os projetos financiados pelo programa Horizonte Europa serão executados em consonância com o Regulamento XXX [Regulamento Horizonte Europa], que prevê que as atividades de investigação e inovação realizadas ao abrigo do Horizonte Europa devem incidir sobre aplicações civis.

(19) Com vista a assegurar uma colaboração estruturada e sustentável, a relação entre o Centro de Competências e os centros nacionais de coordenação deverá estar assente num acordo contratual.

(20) Deverão ser previstas disposições adequadas para garantir a responsabilidade e a transparência do Centro de Competências.

(21) Atendendo aos respetivos conhecimentos especializados em matéria de cibersegurança, o Centro Comum de Investigação da Comissão e a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) devem desempenhar uma parte ativa na Comunidade de Competências em Cibersegurança e no Conselho Consultivo Industrial e Científico.

(22) Caso recebam uma contribuição financeira do orçamento geral da União, os centros nacionais de coordenação e as entidades que integram a Comunidade de Competências em Cibersegurança devem publicitar o facto de as respetivas atividades serem realizadas no contexto da presente iniciativa.

(23) A contribuição da União para o Centro de Competências deverá financiar metade dos custos resultantes das atividades de estabelecimento, administrativas e de coordenação do Centro de Competências. A fim de evitar a duplicação do financiamento, essas atividades não devem beneficiar simultaneamente de uma contribuição de outros programas da União.

(24) O Conselho de Administração do Centro de Competências, composto por representantes dos Estados-Membros e da Comissão, deve definir a orientação geral das atividades do Centro de Competências e garantir que este 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 do Centro de Competências, aprovar o plano de trabalho e o plano estratégico plurianual do Centro de Competências, os quais devem refletir as prioridades para o cumprimento dos objetivos e atribuições do Centro, aprovar o seu próprio regulamento interno, nomear o diretor executivo e decidir da prorrogação ou do termo do mandato deste último.

(25) Para o funcionamento correto e eficaz do Centro de Competências, a Comissão e os Estados-Membros devem assegurar que as pessoas nomeadas para o Conselho de Administração possuam níveis adequados de experiência e de competências profissionais especializadas em áreas funcionais. 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.

(26) O bom funcionamento do Centro de Competências 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 no domínio da cibersegurança, e que desempenhe as suas funções com total independência.

(27) O Centro de Competências deve dispor de um Conselho Consultivo Industrial e Científico que aja enquanto órgão consultivo para garantir o diálogo regular com o setor privado, as organizações de consumidores e outras partes interessadas relevantes. O Conselho Consultivo Industrial e Científico deve concentrar-se em questões relevantes para as partes interessadas e chamar a atenção do Conselho de Administração do Centro de Competências para as mesmas. A composição do Conselho Consultivo Industrial e Científico e as atribuições que lhe são conferidas, tais como ser consultado relativamente ao plano de trabalho, devem assegurar uma representação suficiente das partes interessadas nos trabalhos do Centro de Competências.

(28) O Centro de Competências deverá beneficiar, por via do seu Conselho Consultivo Industrial e Científico, dos conhecimentos especializados específicos e da ampla e relevante representação das partes interessadas gerada por intermédio da parceria público-privada contratual para a cibersegurança ao longo da vigência do Horizonte 2020.

(29) O Centro de Competências deve dispor de regras em matéria de prevenção e gestão de conflitos de interesse. O Centro de Competências 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[24]. O tratamento de dados pessoais pelo Centro de Competências estará sujeito ao Regulamento (UE) n.º XXX/2018 do Parlamento Europeu e do Conselho. O Centro de Competências 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.

(30) É essencial que os interesses financeiros da União e dos Estados-Membros sejam protegidos por medidas proporcionadas, aplicadas ao longo do ciclo de despesa,

[24] 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).

incluindo a prevenção, a deteção e a investigação de irregularidades, a recuperação de fundos perdidos, pagos indevidamente ou utilizados incorretamente, e, se for caso disso, a imposição de sanções administrativas e financeiras nos termos do Regulamento XXX (UE, Euratom) do Parlamento Europeu e do Conselho[25] [Regulamento Financeiro].

(31) O Centro de Competências deverá funcionar de forma aberta e transparente, facultando em tempo útil todas as informações pertinentes e promovendo as suas atividades, nomeadamente as atividades de informação e divulgação ao público em geral. Os regulamentos internos dos órgãos do Centro de Competências deverão ser tornados públicos.

(32) O auditor interno da Comissão deverá exercer relativamente ao Centro de Competências os mesmos poderes que exerce em relação à Comissão.

(33) A Comissão, o Centro de Competências, o Tribunal de Contas e o Organismo Europeu de Luta Antifraude deverão ter acesso a todas as informações e instalações necessárias para realizarem auditorias e inquéritos sobre as subvenções, os contratos e os acordos assinados pelo Centro de Competências.

(34) Uma vez que os objetivos do presente regulamento, nomeadamente conservar e desenvolver as capacidades tecnológicas e industriais no domínio da cibersegurança da União, aumentar a competitividade da indústria de cibersegurança da União e transformar a cibersegurança numa vantagem competitiva para outras indústrias da União, não podem ser suficientemente alcançados pelos Estados-Membros devido à dispersão dos recursos limitados existentes, bem como à dimensão do investimento necessário, mas podem, em vez disso, ser mais adequadamente alcançados a nível da União, para assim evitar a duplicação desnecessária desses esforços, ajudar a alcançar uma massa crítica de investimento e assegurar que o financiamento público é utilizado de modo eficaz, esta última pode adotar medidas de acordo com o princípio da subsidiariedade, conforme estabelecido 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 esses objetivos,

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES E PRINCÍPIOS GERAIS DO CENTRO DE COMPETÊNCIAS E DA REDE

Artigo 1.º

Objeto

1. O presente regulamento estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (doravante designado por «Centro de Competências») e a Rede de Centros Nacionais de Coordenação, e define regras para a nomeação de centros nacionais de coordenação assim como para a criação da Comunidade de Competências em Cibersegurança.

[25] [aditar título e referência do JO].

2. O Centro de Competências contribui para a execução da parte relativa à cibersegurança do Programa Europa Digital estabelecido pelo Regulamento n.º XXX, em especial as ações relacionadas com o artigo 6.º do Regulamento (UE) n.º XXX [Programa Europa Digital], bem como do Programa Horizonte Europa estabelecido pelo Regulamento n.º XXX, em especial o anexo I, pilar II, secção 2.2.6, da Decisão n.º XXX que estabelece o programa específico de execução do Horizonte Europa — Programa-Quadro de Investigação e Inovação [número de ref.ª do programa específico].

3. O Centro de Competências tem sede em [Bruxelas, Bélgica].

4. O Centro de Competências é dotado de personalidade jurídica. Em cada Estado-Membro, goza da mais ampla capacidade jurídica reconhecida às pessoas coletivas pelo respetivo direito interno. Pode, designadamente, adquirir ou alienar bens móveis e imóveis e estar em juízo.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Cibersegurança», a proteção de redes e sistemas de informação, dos seus utilizadores e de outras pessoas contra ciberameaças;

2) «Produtos e soluções de cibersegurança», os produtos, serviços ou processos de tecnologias da informação e comunicação (TIC) com a finalidade específica de proteger redes e sistemas de informação, os seus utilizadores e as pessoas afetadas contra ciberameaças;

3) «Autoridade pública», qualquer governo ou outra administração pública, incluindo órgãos consultivos públicos, a nível nacional, regional ou local ou qualquer pessoa singular ou coletiva que desempenhe funções de administração pública nos termos das disposições do seu direito nacional, incluindo o exercício de deveres específicos;

4) «Estado-Membro participante», um Estado-Membro que contribui financeiramente a título voluntário para os custos administrativos e operacionais do Centro de Competências.

Artigo 3.º

Missão do Centro e da Rede

1. O Centro de Competências e a Rede ajudam a União a:

   a) Conservar e desenvolver as capacidades tecnológicas e industriais no domínio da cibersegurança necessárias para proteger o mercado único digital;

   b) Aumentar a competitividade da indústria de cibersegurança da União e transformar a cibersegurança numa vantagem competitiva para outras indústrias da União.

2. O Centro de Competências exerce as suas funções, quando apropriado, em colaboração com a Rede de Centros Nacionais de Coordenação e uma Comunidade de Competências em Cibersegurança.

Artigo 4.º

Objetivos e atribuições do Centro

O Centro de Competências tem os seguintes objetivos e funções conexas:

1. Facilitar e ajudar a coordenar os trabalhos da Rede de Centros Nacionais de Coordenação (doravante designada por «Rede») a que se refere o artigo 6.º e da Comunidade de Competências em Cibersegurança a que se refere o artigo 8.º.

2. Contribuir para a execução da parte relativa à cibersegurança do Programa Europa Digital estabelecido pelo Regulamento n.º XXX[26], em especial as ações relacionadas com o artigo 6.º do Regulamento (UE) n.º XXX [Programa Europa Digital], bem como do Programa Horizonte Europa estabelecido pelo Regulamento n.º XXX[27], em especial o anexo I, pilar II, secção 2.2.6, da Decisão n.º XXX que estabelece o programa específico de execução do Horizonte Europa — Programa-Quadro de Investigação e Inovação [número de ref.ª do programa específico].

3. Reforçar as capacidades, os conhecimentos e as infraestruturas de cibersegurança ao serviço das indústrias, do setor público e das comunidades de investigação, realizando as seguintes tarefas:

    a) Em relação às infraestruturas industriais e de investigação de vanguarda em matéria de cibersegurança e aos serviços conexos, adquirir, atualizar, operar e disponibilizar essas infraestruturas e serviços conexos a um vasto leque de utilizadores na União, desde a indústria, incluindo as PME, até ao setor público e à comunidade de investigação e científica;

    b) No tocante às infraestruturas industriais e de investigação de vanguarda em matéria de cibersegurança e aos serviços conexos, prestar apoio a outras entidades, incluindo a nível financeiro, para a aquisição, atualização, operação e disponibilização dessas infraestruturas e serviços conexos a um vasto leque de utilizadores na União, desde a indústria, incluindo as PME, até ao setor público e à comunidade de investigação e científica;

    c) Prestar conhecimentos e assistência técnica no domínio da cibersegurança à indústria e às autoridades públicas, nomeadamente mediante o apoio a ações destinadas a facilitar o acesso aos conhecimentos especializados disponíveis na Rede e na Comunidade de Competências em Cibersegurança;

4. Contribuir para a ampla implantação de produtos e soluções de cibersegurança de vanguarda na economia, realizando as seguintes tarefas:

    a) Estimular a investigação no domínio da cibersegurança, o desenvolvimento e a adoção de produtos e soluções de cibersegurança da União pelas autoridades públicas e as indústrias utilizadoras;

    b) Assistir as autoridades públicas, as indústrias do lado da procura e outros utilizadores na adoção e integração das soluções de cibersegurança mais recentes;

[26] [aditar título completo e referência do JO].

[27] [aditar título completo e referência do JO].

c) Apoiar, em especial, as autoridades públicas na organização dos seus procedimentos de contratação pública, ou realizar a adjudicação de contratos para produtos e soluções de cibersegurança de vanguarda em nome das autoridades públicas;

d) Prestar apoio financeiro e assistência técnica a empresas em fase de arranque e PME no domínio da cibersegurança para que se liguem a potenciais mercados e atraiam investimento;

5. Melhorar a compreensão da cibersegurança e contribuir para reduzir as lacunas de competências na União relacionadas com a cibersegurança, realizando as seguintes tarefas:

a) Apoiar o contínuo desenvolvimento de competências de cibersegurança, se for caso disso, juntamente com as agências e organismos relevantes da UE, nomeadamente a ENISA;

6. Contribuir para o reforço da investigação e desenvolvimento no domínio da cibersegurança na União:

a) Prestando apoio financeiro aos esforços de investigação no domínio da cibersegurança com base numa agenda estratégica plurianual industrial, tecnológica e de investigação comum, continuamente avaliada e melhorada;

b) Apoiando projetos de investigação e demonstração de grande escala em capacidades tecnológicas de cibersegurança da próxima geração, em colaboração com a indústria e a Rede;

c) Apoiando a investigação e inovação para a normalização na tecnologia de cibersegurança;

7. Melhorar a cooperação entre as esferas civil e militar no tocante às tecnologias e aplicações de cibersegurança de dupla utilização, realizando as seguintes tarefas:

a) Apoiar os Estados-Membros e as partes interessadas no domínio da investigação e da indústria relativamente à investigação, ao desenvolvimento e à implantação;

b) Contribuir para a cooperação entre os Estados-Membros, apoiando a educação, a formação e exercícios;

c) Reunir partes interessadas para promover sinergias entre os mercados e a investigação no domínio da cibersegurança civil e militar;

8. Reforçar sinergias entre as dimensões civil e militar da cibersegurança em relação ao Fundo Europeu de Defesa, realizando as seguintes tarefas:

a) Prestar aconselhamento, partilhar conhecimentos especializados e facilitar a colaboração entre as partes interessadas relevantes;

b) Gerir projetos de ciberdefesa multinacionais, quando solicitado pelos Estados-Membros, e, desta forma, atuar como um gestor de projetos na aceção do Regulamento XXX [Regulamento que estabelece o Fundo Europeu de Defesa].

Artigo 5.º

Investimento em infraestruturas, capacidades, produtos ou soluções e respetiva utilização

1. Caso o Centro de Competências preste financiamento para infraestruturas, capacidades, produtos ou soluções nos termos do artigo 4.º, n.os 3 e 4, sob a forma de uma subvenção ou de um prémio, o plano de trabalho do Centro de Competências poderá especificar:

   a) Regras que regem o funcionamento de uma infraestrutura ou capacidade, nomeadamente, se for caso disso, confiando o funcionamento a uma entidade de acolhimento com base em critérios a definir pelo Centro de Competências;

   b) Regras que regem o acesso e a utilização de uma infraestrutura ou capacidade.

2. O Centro de Competências pode ser responsável pela execução geral de ações de contratação pública conjuntas, incluindo contratos públicos pré-comerciais, em nome de membros da Rede, de membros da Comunidade de Competências em Cibersegurança ou de outros terceiros que representem utilizadores de produtos e soluções de cibersegurança. Para o efeito, o Centro de Competências pode ser assistido por um ou mais centros nacionais de coordenação ou por membros da Comunidade de Competências em Cibersegurança.

Artigo 6.º

Nomeação de centros nacionais de coordenação

1. Até [data], cada Estado-Membro nomeia uma entidade para atuar como centro nacional de coordenação para efeitos do presente regulamento e notifica essa nomeação à Comissão.

2. Com base numa avaliação relativa à conformidade dessa entidade com os critérios estabelecidos no n.º 4, a Comissão emite uma decisão, no prazo de seis meses a contar da nomeação transmitida pelo Estado-Membro, que acredita a entidade como um centro nacional de coordenação ou que rejeita a nomeação. A lista dos centros nacionais de coordenação é publicada pela Comissão.

3. Os Estados-Membros podem, em qualquer altura, nomear uma nova entidade como centro nacional de coordenação para efeitos do presente regulamento. Os n.os 1 e 2 são aplicáveis à nomeação de uma nova entidade.

4. Os centros nacionais de coordenação nomeados devem ter a capacidade de apoiar o Centro de Competências e a Rede no exercício da sua missão, estabelecida no artigo 3.º do presente regulamento. Devem possuir ou ter acesso direto a conhecimentos especializados tecnológicos no domínio da cibersegurança e estar em posição de se envolverem e coordenarem com a indústria, o setor público e a comunidade de investigação.

5. A relação entre o Centro de Competências e os centros nacionais de coordenação assenta num acordo contratual assinado entre o Centro de Competências e cada um dos centros nacionais de coordenação. O acordo prevê as regras que regem a relação e a repartição de tarefas entre o Centro de Competências e cada centro nacional de coordenação.

6. A Rede de Centros Nacionais de Coordenação é composta por todos os centros nacionais de coordenação nomeados pelos Estados-Membros.

Artigo 7.º

Atribuições dos centros nacionais de coordenação

1. Os centros nacionais de coordenação têm as seguintes atribuições:

   a) Apoiar o Centro de Competência na consecução dos seus objetivos e, em especial, na coordenação da Comunidade de Competências em Cibersegurança;

   b) Facilitar a participação da indústria e de outros intervenientes a nível do Estado-Membro em projetos transfronteiriços;

   c) Contribuir, juntamente com o Centro de Competências, para identificar e resolver desafios industriais em matéria de cibersegurança específicos de determinados setores;

   d) Atuar como ponto de contacto a nível nacional para a Comunidade de Competências em Cibersegurança e o Centro de Competências;

   e) Procurar estabelecer sinergias com atividades relevantes a nível nacional e regional;

   f) Executar ações específicas para as quais o Centro de Competências concedeu subvenções, incluindo por meio da prestação de apoio financeiro a terceiros, em linha com o artigo 204.º do Regulamento XXX [novo Regulamento Financeiro], ao abrigo das condições especificadas nas convenções de subvenção em causa;

   g) Promover e divulgar os resultados pertinentes do trabalho da Rede, da Comunidade de Competências em Cibersegurança e do Centro de Competências a nível nacional ou regional;

   h) Avaliar pedidos de entidades estabelecidas no mesmo Estado-Membro que o centro de coordenação com vista à integração na Comunidade de Competências em Cibersegurança.

2. Para efeitos da alínea f), o apoio financeiro a terceiros pode ser prestado em qualquer uma das formas especificadas no artigo 125.º do Regulamento XXX [novo Regulamento Financeiro], incluindo na forma de montantes fixos.

3. Os centros nacionais de coordenação podem receber uma subvenção da União nos termos do artigo 195.º, alínea d), do Regulamento XXX [novo Regulamento Financeiro], relativa à realização das atribuições estabelecidas neste artigo.

4. Os centros nacionais de coordenação cooperam, quando adequado, no âmbito da Rede, para efeitos de execução das funções a que se refere o n.º 1, alíneas a), b), c), e) e g).

Artigo 8.º

A Comunidade de Competências em Cibersegurança

1. A Comunidade de Competências em Cibersegurança contribui para a missão do Centro de Competências definida no artigo 3.º e para melhorar e divulgar os conhecimentos especializados em matéria de cibersegurança na União.

2. A Comunidade de Competências em Cibersegurança é composta por representantes da indústria, do meio académico, de organizações de investigação sem fins lucrativos e de associações, bem como de entidades públicas e outras entidades que lidem com

questões operacionais e técnicas. A Comunidade procura reunir as principais partes interessadas no que diz respeito às capacidades tecnológicas e industriais em matéria de cibersegurança na União. Envolverá ainda os centros nacionais de coordenação e as instituições e organismos da União com conhecimentos especializados relevantes.

3. Apenas entidades estabelecidas dentro da União podem ser acreditadas como membros da Comunidade de Competências em Cibersegurança. Para tal, devem demonstrar que possuem conhecimentos especializados em matéria de cibersegurança no tocante a, pelo menos, um dos seguintes domínios:

   a) Investigação;

   b) Desenvolvimento industrial;

   c) Formação e ensino.

4. O Centro de Competências acredita entidades estabelecidas nos termos da legislação nacional como membros da Comunidade de Competências em Cibersegurança, após o centro nacional de coordenação do Estado-Membro em que a entidade está estabelecida examinar se essa entidade satisfaz os critérios previstos no n.º 3. A acreditação não está limitada no tempo, mas pode ser revogada pelo Centro de Competências em qualquer altura, se o mesmo ou o centro nacional de coordenação competente considerar que a entidade em causa não satisfaz os critérios estabelecidos no n.º 3 ou está abrangida pelas disposições relevantes estabelecidas no artigo 136.º do Regulamento XXX [novo Regulamento Financeiro].

5. O Centro de Competências acredita órgãos, agências e organismos pertinentes da União como membros da Comunidade de Competências em Cibersegurança após verificar se as entidades em causa cumprem os critérios previstos no n.º 3. A acreditação não está limitada no tempo, mas pode ser revogada pelo Centro de Competências em qualquer altura, se o mesmo considerar que a entidade em causa não satisfaz os critérios estabelecidos no n.º 3 ou está abrangida pelas disposições relevantes estabelecidas no artigo 136.º do Regulamento XXX [novo Regulamento Financeiro].

6. Os representantes da Comissão podem participar nos trabalhos da comunidade.

Artigo 9.º

Atribuições dos membros da Comunidade de Competências em Cibersegurança

Os membros da Comunidade de Competências em Cibersegurança devem:

1) Apoiar o Centro de Competências na consecução da missão e dos objetivos estabelecidos nos artigos 3.º e 4.º e, para o efeito, trabalhar em estreita colaboração com o Centro de Competências e os centros nacionais de coordenação relevantes;

2) Participar em atividades promovidas pelo Centro de Competências e pelos centros nacionais de coordenação;

3) Participar, quando adequado, em grupos de trabalho criados pelo Conselho de Administração do Centro de Competências para realizar atividades específicas previstas no plano de trabalho do Centro de Competências;

4) Apoiar, quando necessário, o Centro de Competências e os centros nacionais de coordenação na promoção de projetos específicos;

5) Promover e divulgar os resultados relevantes das atividades e projetos realizados no seio da comunidade.

Artigo 10.º

Cooperação do Centro de Competências com instituições, órgãos, organismos e agências da União

1. O Centro de Competências coopera com as instituições, órgãos, organismos e agências pertinentes da União, nomeadamente a Agência da União Europeia para a Segurança das Redes e da Informação, a Equipa de Resposta a Emergências Informáticas (CERT-EU), o Serviço Europeu para a Ação Externa, o Centro Comum de Investigação da Comissão, a Agência de Execução para a Investigação, a Agência de Execução para a Inovação e as Redes, o Centro Europeu da Cibercriminalidade na Europol, bem como a Agência Europeia de Defesa.

2. Essa cooperação ocorre no quadro de acordos de trabalho. Tais acordos são submetidos a aprovação prévia da Comissão.

CAPÍTULO II

ORGANIZAÇÃO DO CENTRO DE COMPETÊNCIAS

Artigo 11.º

Filiação e estrutura

1. Os membros do Centro de Competências são a União, representada pela Comissão, e os Estados-Membros.

2. A estrutura do Centro de Competências inclui:

   a) Um Conselho de Administração, com as competências definidas no artigo 13.º;

   b) Um diretor executivo, com as competências definidas no artigo 16.º;

   c) Um Conselho Consultivo Industrial e Científico, com as competências definidas no artigo 20.º.

SECÇÃO I

CONSELHO DE ADMINISTRAÇÃO

Artigo 12.º

Composição do Conselho de Administração

1. O Conselho de Administração é composto por um representante de cada Estado-Membro e por cinco representantes da Comissão, em nome da União.

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 tecnologia, bem como das 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.

5. Os membros do Conselho de Administração agem no interesse do Centro de Competências, salvaguardando os respetivos fins, missões, identidade, autonomia e coerência, com toda a independência e transparência.

6. A Comissão pode convidar observadores para as reuniões do Conselho de Administração, incluindo, conforme adequado, representantes dos organismos, órgãos e agências pertinentes da União.

7. A Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) é um observador permanente do Conselho de Administração.

Artigo 13.º

Atribuições do Conselho de Administração

1. O Conselho de Administração assume a responsabilidade global pela orientação estratégica e pelo funcionamento do Centro de Competências e supervisiona a realização das suas atividades.

2. O Conselho de Administração aprova o seu regulamento interno. O regulamento interno prevê procedimentos específicos para identificar e prevenir conflitos de interesses e assegurar a confidencialidade de quaisquer informações sensíveis.

3. O Conselho de Administração toma as decisões estratégicas necessárias, nomeadamente:

   a) Adotar um plano estratégico plurianual que inclua uma declaração das principais prioridades e iniciativas previstas do Centro de Competências, incluindo uma estimativa das necessidades e das fontes de financiamento;

   b) Adotar o plano de trabalho do Centro de Competências, as contas e o balanço anuais e o relatório anual de atividades com base numa proposta do diretor executivo;

   c) Adotar as regras financeiras específicas do Centro de Competências em conformidade com o [artigo 70.º do RF];

   d) Adotar um procedimento para a nomeação do diretor executivo;

   e) Adotar os critérios e procedimentos para avaliar e acreditar as entidades como membros da Comunidade de Competências em Cibersegurança;

   f) Nomear, demitir, renovar o mandato e orientar e acompanhar o desempenho do diretor executivo, e nomear o contabilista;

   g) Adotar o orçamento anual do Centro de Competências, incluindo o quadro de pessoal correspondente com indicação do número de lugares temporários, por grupo de funções e por grau, bem como do número de agentes contratuais e de peritos nacionais destacados, expressos em equivalentes a tempo inteiro;

   h) Adotar regras relativas aos conflitos de interesse;

   i) Criar grupos de trabalho com membros da Comunidade de Competências em Cibersegurança;

j) Nomear membros do Conselho Consultivo Industrial e Científico;

k) Criar um órgão de auditoria interna em conformidade com o Regulamento Delegado (UE) n.º 1271/2013 da Comissão[28];

l) Promover o Centro de Competências a nível mundial, para aumentar a sua atratividade e torná-lo um órgão de excelência em cibersegurança de reputação mundial;

m) Estabelecer a política de comunicação da Empresa Comum, sob recomendação do diretor executivo;

n) Assumir a responsabilidade por monitorizar o seguimento adequado das conclusões de avaliações retrospetivas.

o) Estabelecer, se necessário, regras de execução do Estatuto dos Funcionários e do Regime aplicável aos Outros Agentes, nos termos do artigo 31.º, n.º 3;

p) Estabelecer, se necessário, regras em matéria de destacamento de peritos nacionais para o Centro de Competências e de recurso a estagiários, em conformidade com o artigo 32.º, n.º 2;

q) Adotar regras de segurança para o Centro de Competências;

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

s) Adotar a metodologia para calcular a contribuição financeira dos Estados-Membros;

t) Assumir a responsabilidade por qualquer tarefa que não seja especificamente atribuída a um órgão do Centro de Competências, podendo atribuir essas tarefas a qualquer órgão do Centro de Competências.

Artigo 14.º

Presidente e reuniões do Conselho de Administração

1. O Conselho de Administração elege de entre os seus membros com direito de voto um presidente e um vice-presidente por um período de dois anos. Os mandatos do presidente e do vice-presidente podem ser prorrogados uma única vez, na sequência de uma decisão do Conselho de Administração. 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. O presidente participa na votação.

2. O Conselho de Administração reúne-se, em reunião ordinária, pelo menos três vezes por ano. Pode realizar reuniões extraordinárias a pedido da Comissão, a pedido de um terço dos seus membros, a pedido do presidente, ou a pedido do diretor executivo no desempenho das suas atribuições.

[28] 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).

3. O diretor executivo participa nas deliberações, salvo decisão em contrário do Conselho de Administração, mas não tem direito de voto. O Conselho de Administração pode, caso a caso, convidar outras pessoas para assistirem às suas reuniões na qualidade de observadores.

4. Os membros do Conselho Consultivo Industrial e Científico podem participar, a convite do presidente, nas reuniões do Conselho de Administração, sem direito a voto.

5. Os membros do Conselho de Administração e respetivos suplentes podem ser assistidos nas reuniões por consultores ou peritos, sob reserva do disposto no regulamento interno.

6. O Centro de Competências assegura os serviços de secretariado do Conselho de Administração.

Artigo 15.º

Regras de votação do Conselho de Administração

1. A União tem direito a 50 % dos direitos de voto. Os direitos de voto da União são indivisíveis.

2. Cada Estado-Membro participante tem direito a um voto.

3. O Conselho de Administração toma as suas decisões por uma maioria de, pelo menos 75 % dos votos, incluindo os votos dos membros que se encontrem ausentes, representando, pelo menos, 75 % das contribuições financeiras para o Centro de Competências. A contribuição financeira será calculada com base nas despesas estimadas propostas pelos Estados-Membros a que se refere o artigo 17.º, n.º 2, alínea c), e com base no relatório sobre o valor das contribuições dos Estados-Membros participantes a que se refere o artigo 22.º, n.º 5.

4. Apenas os representantes da Comissão e os representantes dos Estados-Membros participantes têm direito de voto.

5. O presidente participa na votação.

SECÇÃO II

DIRETOR EXECUTIVO

Artigo 16.º

Nomeação, demissão ou renovação do mandato do diretor executivo

1. O diretor executivo deve ser uma pessoa com experiência e elevada reputação nas áreas de atividade do Centro de Competências.

2. O diretor executivo é contratado como agente temporário do Centro de Competências, nos termos do artigo 2.º, alínea a), do Regime aplicável aos Outros Agentes.

3. O diretor executivo é nomeado pelo Conselho de Administração de entre uma lista de candidatos proposta pela Comissão, na sequência de um processo de seleção aberto e transparente.

4. Para efeitos da celebração do contrato com o diretor executivo, o Centro de Competências é representado pelo presidente do Conselho de Administração.

5. O mandato do diretor executivo tem a duração de quatro anos. No termo desse período, a Comissão procede a uma avaliação que tenha em conta a avaliação do trabalho realizado pelo diretor executivo e as futuras atribuições e desafios do Centro de Competências.

6. O Conselho de Administração, deliberando sob proposta da Comissão que tenha em conta a avaliação referida no n.º 5, pode prorrogar uma vez o mandato do diretor executivo, por um período não superior a quatro anos.

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

8. O diretor executivo só pode ser exonerado por decisão do Conselho de Administração, deliberando sob proposta da Comissão.

Artigo 17.º

Atribuições do diretor executivo

1. O diretor executivo é responsável pelas operações e pela gestão quotidiana do Centro de Competências e é o seu representante legal. O diretor executivo presta contas ao Conselho de Administração e desempenha as suas funções com total independência, no âmbito das competências que lhe são conferidas.

2. O diretor executivo desempenha, em especial, as seguintes funções de forma independente:

   a) Executa as decisões adotadas pelo Conselho de Administração;

   b) Apoia o Conselho de Administração nos seus trabalhos, presta os serviços de secretariado para as suas reuniões e fornece todas as informações necessárias ao exercício dos seus deveres;

   c) Prepara e apresenta ao Conselho de Administração, para adoção, após consulta do Conselho de Administração e da Comissão, o projeto de plano estratégico plurianual e o projeto de plano de trabalho anual do Centro de Competências, nomeadamente o âmbito dos convites à apresentação de propostas, dos convites à manifestação de interesse e dos concursos públicos necessários para executar o plano de trabalho e as correspondentes estimativas de despesas propostas pelos Estados-Membros e pela Comissão;

   d) Prepara e apresenta ao Conselho de Administração, para adoção, o projeto de orçamento anual, incluindo o correspondente quadro de pessoal, indicando o número de lugares temporários em cada grau e grupo de funções e o número de agentes contratuais e de peritos nacionais destacados, expressos em equivalentes a tempo inteiro;

   e) Executa o plano de trabalho e comunica informações sobre essa execução ao Conselho de Administração;

   f) Prepara o projeto de relatório anual de atividades sobre o Centro de Competências, incluindo as informações sobre as respetivas despesas;

   g) Assegura a aplicação de procedimentos de monitorização e avaliação eficazes relacionados com o desempenho do Centro de Competências;

h) Prepara um plano de ação para o seguimento das conclusões das avaliações retrospetivas e a apresentação à Comissão, de dois em dois anos, de um relatório sobre os progressos realizados;

i) Prepara, negoceia e celebra acordos com os centros nacionais de coordenação;

j) Assume a responsabilidade pelas matérias administrativas, financeiras e de pessoal, nomeadamente a execução do orçamento do Centro de Competências, tendo em devida conta o aconselhamento recebido do órgão de auditoria interna, dentro dos limites da delegação de poderes conferida pelo Conselho de Administração;

k) Aprova e gere o lançamento de convites à apresentação de propostas, nos termos do plano de trabalho, e administra as convenções e decisões de subvenção;

l) Aprova a lista de ações selecionadas para financiamento, com base na classificação estabelecida por um painel de peritos independentes;

m) Aprova e gere o lançamento de concursos públicos, nos termos do plano de trabalho, e administra os contratos;

n) Aprova as propostas apresentadas a concurso selecionadas para financiamento;

o) Apresentar os projetos de contas e de balanço anuais ao órgão de auditoria interna e, subsequentemente, ao Conselho de Administração;

p) Vela por que se proceda à avaliação e à gestão dos riscos;

q) Assina contratos, decisões e convenções de subvenção individuais;

r) Assina contratos públicos;

s) Elabora 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 para a apresentação de relatórios sobre os progressos realizados à Comissão, duas vezes por ano, e, regularmente, ao Conselho de Administração;

t) Elabora o projeto de regras financeiras aplicáveis ao Centro de Competências;

u) Institui um sistema de controlo interno eficaz e eficiente, assegurar o seu funcionamento e comunicar ao Conselho de Administração qualquer alteração significativa nele introduzida;

v) Assegura uma comunicação eficaz com as instituições da União;

w) Adota quaisquer outras medidas necessárias para avaliar os progressos alcançados pelo Centro de Competências no sentido do cumprimento da missão e dos objetivos definidos nos artigos 3.º e 4.º do presente regulamento;

x) Executa quaisquer outras tarefas que lhe sejam confiadas ou delegadas pelo Conselho de Administração.

SECÇÃO III

CONSELHO CONSULTIVO INDUSTRIAL E CIENTÍFICO

Artigo 18.º

Composição do Conselho Consultivo Industrial e Científico

1. O Conselho Consultivo Industrial e Científico é constituído por 16 membros, no máximo. Os membros são designados pelo Conselho de Administração de entre os representantes das entidades da Comunidade de Competências em Cibersegurança.

2. Os membros do Conselho Consultivo Industrial e Científico devem ter conhecimentos especializados no tocante à investigação, ao desenvolvimento industrial, aos serviços profissionais ou à implantação dos mesmos no domínio da cibersegurança. Os níveis de conhecimentos especializados exigidos serão especificados mais pormenorizadamente pelo Conselho de Administração.

3. Os procedimentos relativos à designação dos membros pelo Conselho de Administração e ao funcionamento do Conselho Consultivo são especificados no regulamento interno do Centro de Competências e tornados públicos.

4. O mandato dos membros do Conselho Consultivo Industrial e Científico tem a duração de três anos. Esse mandato é renovável.

5. Os representantes da Comissão e da Agência da União Europeia para a Segurança das Redes e da Informação podem participar nos trabalhos do Conselho Consultivo Industrial e Científico e apoiar os mesmos.

Artigo 19.º

Funcionamento do Conselho Consultivo Industrial e Científico

1. O Conselho Consultivo Industrial e Científico reúne-se, pelo menos, duas vezes por ano.

2. O Conselho Consultivo Industrial e Científico pode aconselhar o Conselho de Administração sobre a criação de grupos de trabalho sobre questões específicas relevantes para o trabalho do Centro de Competências, quando necessário, sob a coordenação geral de um ou mais membros do Conselho Consultivo Industrial e Científico.

3. O Conselho Consultivo Industrial e Científico elege o seu presidente.

4. O Conselho Consultivo Industrial e Científico adota o seu regulamento interno, incluindo a designação dos representantes que, quando adequado, o devem representar e a duração da sua designação.

Artigo 20.º

Atribuições do Conselho Consultivo Industrial e Científico

O Conselho Consultivo Industrial e Científico presta aconselhamento ao Centro de Competências relativamente ao exercício das suas atividades e deve:

1) Prestar aconselhamento estratégico e contributos ao diretor executivo e ao Conselho de Administração para fins da elaboração do plano de trabalho e do plano estratégico plurianual nos prazos fixados pelo Conselho de Administração;

2) Organizar consultas públicas abertas ao público e a partes interessadas privadas que tenham um interesse no domínio da cibersegurança, a fim de recolher contributos para o aconselhamento estratégico referido no n.º 1;

3) Promover e recolher opiniões sobre o plano de trabalho e o plano estratégico plurianual do Centro de Competências.

CAPÍTULO III
DISPOSIÇÕES FINANCEIRAS

Artigo 21.º

Participação financeira da União

1. A contribuição financeira da União para o Centro de Competências, destinada a cobrir as despesas administrativas e as despesas operacionais, inclui o seguinte:

   a) 1 981 668 000 EUR ao abrigo do Programa Europa Digital, incluindo um máximo de 23 746 000 EUR para cobrir despesas administrativas;

   b) Um montante do Programa Horizonte Europa, incluindo para custos administrativas, a ser determinado tendo em conta o processo de planeamento estratégico a realizar nos termos do artigo 6.º, n.º 6, do Regulamento XXX [Regulamento Horizonte Europa].

2. A contribuição máxima da União é paga com as dotações do orçamento geral da União afetadas ao [Programa Europa Digital] e ao programa específico que executa o programa Horizonte Europa, instituído pela Decisão XXX.

3. O Centro de Competências executa as ações de cibersegurança do [Programa Europa Digital] e do [Programa Horizonte Europa] nos termos do artigo 62.º, alínea c), subalínea iv), do Regulamento (UE, Euratom) XXX[29] [o Regulamento Financeiro].

4. A contribuição financeira da União não cobre as tarefas mencionadas no artigo 4.º, n.º 8, alínea b).

Artigo 22.º

Contribuições dos Estados-Membros participantes

1. Os Estados-Membros participantes fazem uma contribuição total para os custos operacionais e administrativos do Centro de Competências, pelo menos, nos mesmos montantes referidos no artigo 21.º, n.º 1, do presente regulamento.

2. Para efeitos de avaliar as contribuições referidas no n.º 1 e no artigo 23.º, n.º 3, alínea b), subalínea ii), os custos são determinados de acordo com as práticas habituais em matéria de contabilidade de custos dos Estados-Membros em causa, as normas contabilísticas aplicáveis do Estado-Membro e as Normas Internacionais de Contabilidade e Normas Internacionais de Relato Financeiro aplicáveis. Os custos são certificados por um auditor externo independente nomeado pelo Estado-Membro em causa. Caso haja incertezas que decorram da certificação, o Centro de Competências pode verificar o método de valoração.

3. Caso um Estado-Membro participante não cumpra os compromissos respeitantes à sua contribuição financeira, o diretor executivo notifica-o por escrito e fixa um prazo razoável para a resolução desse incumprimento. Se a situação não for regularizada no prazo estabelecido, o diretor executivo convoca uma reunião do Conselho de Administração para decidir se o direito de voto do Estado-Membro participante em falta lhe deve ser retirado ou se devem ser adotadas outras medidas até que este

[29] [aditar título completo e referência do JO].

respeite as suas obrigações. Os direitos de voto do Estado-Membro em falta são suspensos até que as suas obrigações sejam cumpridas.

4. A Comissão pode fazer cessar, reduzir proporcionalmente ou suspender a contribuição financeira da União para o Centro de Competências se os Estados-Membros participantes não contribuírem, contribuírem apenas parcialmente ou contribuírem tardiamente em relação ao disposto no n.º 1.

5. Os Estados-Membros participantes comunicam ao Conselho de Administração, até 31 de janeiro de cada ano, o valor das contribuições a que se refere o n.º 1 realizadas em cada um dos exercícios anteriores.

Artigo 23.º

Custos e recursos do Centro de Competências

1. O Centro de Competências é financiado conjuntamente pela União e pelos Estados-Membros por meio de contribuições financeiras pagas em prestações e contribuições que consistem em custos incorridos pelos centros nacionais de coordenação e pelos beneficiários ao executarem ações que não sejam reembolsadas pelo Centro de Competências.

2. As despesas administrativas do Centro de Competências não devem exceder [número] EUR e são cobertas por meio de contribuições financeiras repartidas anualmente em partes iguais entre a União e os Estados-Membros participantes. Se uma parte da contribuição para as despesas administrativas não for utilizada, a mesma pode ser disponibilizada para cobrir as despesas operacionais do Centro de Competências.

3. As despesas operacionais do Centro de Competências são cobertas através de:

   a) Contribuição financeira da União;

   b) Contribuições dos Estados-Membros participantes na forma de:

      i) contribuições financeiras,

      ii) quando adequado, contribuições em espécie dos Estados-Membros participantes destinadas a cobrir os custos incorridos pelos centros nacionais de coordenação e beneficiários durante a execução de ações indiretas, subtraindo a contribuição do Centro de Competências e qualquer outra contribuição da União para esses custos.

4. Os recursos do Centro de Competências inscritos no seu orçamento são constituídos pelas seguintes contribuições:

   a) Contribuições financeiras dos Estados-Membros participantes para as despesas administrativas;

   b) Contribuições financeiras dos Estados-Membros participantes para as despesas operacionais;

   c) Quaisquer receitas geradas pelo Centro de Competências;

   d) Quaisquer outras contribuições, receitas e recursos financeiros.

5. Os juros gerados pelas contribuições pagas ao Centro de Competências pelos Estados-Membros participantes são considerados receitas do Centro.

6. Todos os recursos do Centro de Competências, bem como as suas atividades, são dedicados à consecução dos objetivos definidos no artigo 4.º.

7. O Centro de Competências é o proprietário de todos os ativos por si gerados ou para si transferidos a fim de realizar os seus objetivos.

8. O eventual excedente das receitas em relação às despesas não reverte para os membros participantes do Centro de Competências, salvo em caso da sua dissolução.

Artigo 24.º

Compromissos financeiros

Os compromissos financeiros do Centro de Competências não podem exceder o montante dos recursos financeiros disponíveis ou inscritos no orçamento pelos seus membros.

Artigo 25.º

Exercício financeiro

O exercício financeiro tem início em 1 de janeiro e termina em 31 de dezembro.

Artigo 26.º

Elaboração do orçamento

1. O diretor executivo elabora anualmente um projeto de mapa previsional de receitas e despesas do Centro de Competências para o exercício financeiro seguinte e transmite-o ao Conselho de Administração, acompanhado de um projeto do quadro de pessoal. As receitas e as despesas devem ser equilibradas. As despesas do Centro de Competências incluem as remunerações do pessoal e as despesas administrativas, de infraestruturas e de funcionamento. As despesas administrativas devem ser mantidas a um nível mínimo.

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 do Centro de Competências para o exercício financeiro 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.

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 contribuição a cargo do orçamento geral, que submete à apreciação do 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 contribuição destinada ao Centro de Competências.

6. O Parlamento Europeu e o Conselho aprovam o quadro de pessoal do Centro de Competências.

7. O Conselho de Administração adota o orçamento do Centro ao mesmo tempo que o plano de trabalho. O orçamento do Centro torna-se definitivo após a aprovação do orçamento geral da União. Se necessário, o Conselho de Administração ajusta o

orçamento e o plano de trabalho do Centro de Competências em função do orçamento geral da União.

Artigo 27.º

Apresentação das contas do Centro de Competências e quitação

A apresentação das contas provisórias e definitivas do Centro de Competências e a respetiva quitação seguem as regras e o calendário do Regulamento Financeiro e das suas regras financeiras adotadas nos termos do artigo 29.º.

Artigo 28.º

Prestação de informações operacionais e financeiras

1. O diretor executivo apresenta anualmente ao Conselho de Administração um relatório sobre o desempenho das suas funções, em conformidade com as regras financeiras do Centro de Competências.
2. No prazo de dois meses a contar do encerramento de cada exercício financeiro, o diretor executivo apresenta ao Conselho de Administração, para aprovação, um relatório anual de atividades centrado nos progressos realizados pelo Centro de Competências no ano civil anterior, em especial no que se refere ao plano de trabalho anual desse ano. O relatório deve incluir, entre outras, informações sobre as seguintes matérias:
   a) Ações operacionais desenvolvidas e despesas correspondentes;
   b) Ações propostas, incluindo a sua repartição por tipo de participantes, incluindo PME, e por Estado-Membro;
   c) Ações selecionadas para financiamento, incluindo a sua repartição por tipo de participantes, incluindo PME, e por Estado-Membro, e indicando a contribuição do Centro de Competências para cada participante e cada ação;
   d) Progressos realizados no sentido da concretização dos objetivos estabelecidos no artigo 4.º e propostas de ações complementares necessárias para esse efeito.
3. Depois de aprovado pelo Conselho de Administração, o relatório anual de atividades é tornado público.

Artigo 29.º

Regras financeiras

O Centro de Competências adota as suas regras financeiras específicas nos termos do artigo 70.º do Regulamento XXX [novo Regulamento Financeiro].

Artigo 30.º

Proteção dos interesses financeiros

1. O Centro de Competências deve tomar medidas adequadas que garantam, quando são executadas ações financiadas ao abrigo do presente regulamento, a proteção dos interesses financeiros da União mediante a aplicação de medidas preventivas contra a fraude, a corrupção e outras atividades ilegais, a realização de controlos eficazes e, se

forem detetadas irregularidades, a recuperação dos montantes pagos indevidamente e, se for caso disso, a aplicação de sanções efetivas, proporcionadas e dissuasivas.

2. O Centro de Competências concede aos funcionários da Comissão e a outras pessoas por esta autorizadas, bem como ao Tribunal de Contas, acesso aos seus locais e instalações, bem como a todas as informações, incluindo informações em formato eletrónico, necessárias para a realização das suas auditorias.

3. O Organismo Europeu de Luta Antifraude (OLAF) pode realizar inquéritos, incluindo verificações e inspeções no local, em conformidade com as disposições e os procedimentos previstos no Regulamento (Euratom, CE) n.º 2185/96 do Conselho[30] e no Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho[31], a fim de verificar a existência de fraudes, de atos de corrupção ou de outras atividades ilegais lesivas dos interesses financeiros da União no âmbito de uma convenção de subvenção ou de um contrato financiado, direta ou indiretamente, ao abrigo do presente regulamento.

4. Sem prejuízo do disposto nos n.[os] 1, 2 e 3, os contratos e as convenções de subvenção resultantes da execução do presente regulamento devem incluir disposições que habilitem expressamente a Comissão, o Centro de Competências, o Tribunal de Contas e o OLAF a procederem às referidas auditorias e inquéritos, de acordo com as respetivas competências. Sempre que a execução de uma ação é objeto de subcontratação ou subdelegação, no todo ou em parte, ou implica a adjudicação de um contrato público ou o apoio financeiro a terceiros, o contrato ou convenção de subvenção deve estabelecer a obrigação de o contratante ou beneficiário impor aos terceiros envolvidos a aceitação explícita dos referidos poderes da Comissão, do Centro de Competências, do Tribunal de Contas e do OLAF.

CAPÍTULO IV

PESSOAL DO CENTRO DE COMPETÊNCIAS

Artigo 31.º

Pessoal

1. O Estatuto dos Funcionários e o Regime aplicável aos Outros Agentes da União Europeia fixados no Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho[32] (adiante designados, respetivamente, por «Estatuto dos Funcionários» e «Regime aplicável aos Outros Agentes»), bem como as regras adotadas conjuntamente pelas instituições da União para executar o Estatuto dos Funcionários e o Regime aplicável aos Outros Agentes, são aplicáveis ao pessoal do Centro de Competências.

---

30 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).

31 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).

32 Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho, de 29 de fevereiro de 1968, que fixa o Estatuto dos Funcionários das Comunidades Europeias assim como o Regime aplicável aos outros agentes destas Comunidades, e institui medidas especiais temporariamente aplicáveis aos funcionários da Comissão (JO L 56 de 4.3.1968, p. 1).

2. O Conselho de Administração exerce, relativamente ao pessoal do Centro de Competências, os poderes conferidos pelo Estatuto dos Funcionários à autoridade investida do poder de nomeação e os poderes conferidos pelo Regime aplicável aos Outros Agentes à autoridade habilitada a celebrar contratos («poderes da autoridade investida do poder de nomeação»).

3. O Conselho de Administração adota, em conformidade com o artigo 110.º do Estatuto dos Funcionários, uma decisão baseada no artigo 2.º, n.º 1, do Estatuto dos Funcionários e no artigo 6.º do Regime aplicável aos Outros Agentes, em que delega no diretor executivo os poderes da autoridade investida do poder de nomeação relevantes e em que define as condições em que essa delegação de poderes pode ser suspensa. O diretor executivo está autorizado a subdelegar os referidos poderes.

4. Em circunstâncias excecionais, o Conselho de Administração pode decidir suspender temporariamente a delegação dos poderes da autoridade investida do poder de nomeação no diretor executivo e qualquer subdelegação feita por este último. Nesse caso, o Conselho de Administração exerce ele próprio os poderes da autoridade investida do poder de nomeação ou delega-os num dos seus membros ou num membro do pessoal do Centro de Competências que não seja o diretor executivo.

5. O Conselho de Administração adota as disposições de execução do Estatuto dos Funcionários e do Regime aplicável aos Outros Agentes adequadas, em conformidade com o artigo 110.º do Estatuto dos Funcionários.

6. Os recursos humanos são determinados no quadro de pessoal do Centro de Competências, onde se indicam o número de lugares temporários, por grupo de funções e por grau, e o número de agentes contratuais, expresso em equivalentes a tempo inteiro, em conformidade com o seu orçamento anual.

7. O pessoal do Centro de Competências é constituído por agentes temporários e agentes contratuais.

8. Todas as despesas de pessoal são suportadas pelo Centro de Competências.

Artigo 32.º

Peritos nacionais destacados e outro pessoal

1. O Centro de Competências pode recorrer a peritos nacionais destacados ou a outro pessoal não contratado pelo Centro de Competências.

2. O Conselho de Administração deve adotar, em acordo com a Comissão, uma decisão que estabeleça os termos do destacamento de peritos nacionais para o Centro de Competências.

Artigo 33.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 Tratado sobre o Funcionamento da União Europeia é aplicável ao Centro de Competências e ao seu pessoal.

CAPÍTULO V

DISPOSIÇÕES COMUNS

Artigo 34.º

Regras de segurança

1. O artigo 12.º, n.º 7, do Regulamento (UE) n.º XXX [Programa Europa Digital] é aplicável à participação em todas as ações financiadas pelo Centro de Competências.

2. As regras de segurança específicas que se seguem aplicam-se a todas as ações financiadas ao abrigo do Horizonte Europa:

   a) Para efeitos do artigo 34.º, n.º 1 [Propriedade e proteção], do Regulamento (UE) n.º XXX [Horizonte Europa], quando previsto no plano de trabalho, a conceção de licenças não exclusivas pode estar limitada a terceiros estabelecidos ou considerados como estando estabelecidos em Estados-Membros e controlados por Estados-Membros e/ou nacionais dos Estados-Membros;

   b) Para efeitos do artigo 36.º, n.º 4, alínea b) [Transferência e concessão de licenças], do Regulamento (UE) n.º XXX [Horizonte Europa], a transferência ou licenciamento para uma entidade jurídica estabelecida num país associado ou estabelecida na União, mas controlada a partir de países terceiros, deve ser igualmente motivo de objeção a transferências de propriedade de resultados, ou a concessões de licenças exclusivas relativas a resultados;

   c) Para efeitos do artigo 37.º, n.º 3, alínea a) [Direitos de acesso], do Regulamento (UE) n.º XXX [Horizonte Europa], quando previsto no plano de trabalho, a concessão de acesso a resultados e conhecimentos preexistentes pode estar limitada apenas a entidades jurídicas estabelecidas ou consideradas como estando estabelecidas em Estados-Membros e controladas por Estados-Membros e/ou nacionais dos Estados-Membros.

Artigo 35.º

Transparência

1. O Centro de Competências exerce as suas atividades com elevado nível de transparência.

2. O Centro de Competências 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. O Centro de Competências publica as declarações de interesses feitas nos termos do artigo 41.º.

3. Sob proposta do diretor executivo, o Conselho de Administração pode autorizar partes interessadas a assistir, como observadores, a algumas atividades do Centro de Competências.

4. O Centro de Competências estabelece, no seu regulamento interno, as disposições práticas de execução das regras relativas à transparência referidas nos n.os 1 e 2. Em relação às ações financiadas pelo Horizonte Europa, terá em devida conta as disposições do anexo III do Regulamento Horizonte Europa.

Artigo 36.º

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

1. Sem prejuízo do disposto no artigo 35.º, o Centro de Competências 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 Conselho Consultivo Industrial e Científico, os peritos externos que participam nos grupos de trabalho *ad hoc* e os membros do pessoal do Centro estão sujeitos à obrigação de confidencialidade prevista no artigo 339.º do Tratado sobre o Funcionamento da União Europeia, mesmo após a cessação das suas funções.

3. O Conselho de Administração do Centro de Competências adota as regras de segurança do Centro de Competências, após aprovação pela Comissão, com base nos princípios e regras estabelecidos pelas regras de segurança da Comissão para a proteção de informações classificadas da União Europeia (ICUE) e de informações sensíveis não classificadas, incluindo as disposições relativas ao tratamento e conservação de tais informações estabelecidas pelas Decisões (UE, Euratom) 2015/443[33] e 2015/444[34].

4. O Centro de Competências pode tomar todas as medidas necessárias para facilitar o intercâmbio de informações pertinentes para as suas atribuições com a Comissão e com os Estados-Membros e, caso se justifique, com outras agências e organismos da União. Qualquer acordo administrativo celebrado para este efeito sobre a partilha de ICUE ou, na ausência de tal acordo, qualquer divulgação *ad hoc* de ICUE deve receber a aprovação prévia da Comissão.

Artigo 37.º

Acesso a documentos

1. O Regulamento (CE) n.º 1049/2001 é aplicável aos documentos detidos pelo Centro de Competências.

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 do Centro de Competências.

3. As decisões tomadas pelo Centro de Competências 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 Tratado sobre o Funcionamento da União Europeia, ou ser objeto de recurso para o Tribunal de Justiça da União Europeia, nos termos do artigo 263.º do Tratado sobre o Funcionamento da União Europeia.

---

33 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).

34 Decisão (UE, Euratom) 2015/444 da Comissão, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (JO L 72 de 17.3.2015, p. 53).

Artigo 38.º

Acompanhamento, avaliação e revisão

1. O Centro de Competências assegura que as suas atividades, incluindo as geridas através dos centros nacionais de coordenação e da Rede, são sujeitas a um acompanhamento contínuo e sistemático e a avaliação periódica. O Centro de Competências assegura que os dados para acompanhar a execução e os resultados do programa são recolhidos de forma eficiente, eficaz e oportuna e que são impostos requisitos apropriados de comunicação de informações aos beneficiários dos fundos da União e aos Estados-Membros. Os resultados da avaliação devem ser tornados públicos.

2. Assim que houver informações suficientes disponíveis sobre a execução do presente regulamento, mas o mais tardar três anos e meio após o início da execução do presente regulamento, a Comissão realiza uma avaliação intercalar do Centro de Competências. A Comissão elabora um relatório sobre essa avaliação e apresenta-o ao Parlamento Europeu e ao Conselho até 31 de dezembro de 2024. O Centro de Competências e os Estados-Membros transmitem à Comissão todas as informações necessárias para a elaboração desse relatório.

3. A avaliação a que se refere o n.º 2 incluirá uma avaliação dos resultados alcançados pelo Centro de Competências, tendo em conta os seus objetivos, mandato e atribuições. Se a Comissão considerar que se justifica manter o Centro de Competências, tendo em conta os objetivos, o mandato e as atribuições que lhe foram conferidos, pode propor a prorrogação do mandato do Centro de Competências fixado no artigo 46.º.

4. Com base nas conclusões da avaliação intercalar a que se refere o n.º 2, a Comissão pode agir em conformidade com o disposto no [artigo 22.º, n.º 5], ou tomar quaisquer outras medidas adequadas.

5. O acompanhamento, a avaliação, a eliminação progressiva e a renovação da contribuição do Horizonte Europa seguirá as disposições dos artigos 8.º, 45.º e 47.º do anexo III do Regulamento Horizonte Europa e as modalidades de execução acordadas.

6. O acompanhamento, a comunicação de informações e a avaliação da contribuição do programa Europa Digital seguirá as disposições dos artigos 24.º e 25.º do referido programa.

7. No caso de dissolução do Centro de Competências, a Comissão realiza uma avaliação final do Centro de Competências no prazo de seis meses após a sua dissolução, mas o mais tardar dois anos após o acionamento do processo de dissolução a que se refere o artigo 46.º do presente regulamento. Os resultados da avaliação final são apresentados ao Parlamento Europeu e ao Conselho.

Artigo 39.º

Responsabilidade do Centro de Competências

1. A responsabilidade contratual do Centro de Competências é regida pela legislação aplicável ao acordo, decisão ou contrato em causa.

2. Em matéria de responsabilidade extracontratual, o Centro de Competências deve reparar, de acordo com os princípios gerais comuns ao direito dos Estados-Membros, os danos causados pelo seu pessoal no desempenho das suas funções.

3. Os pagamentos do Centro de Competências no âmbito da responsabilidade referida nos n.os 1 e 2, bem como os custos e despesas conexos incorridos, são considerados como despesas do Centro de Competências pelo que são cobertos pelos seus recursos.

4. O cumprimento das obrigações do Centro de Competências é da sua exclusiva responsabilidade.

Artigo 40.º

Competência do Tribunal de Justiça da União Europeia e direito aplicável

1. O Tribunal de Justiça da União Europeia é competente:

   1) Com fundamento em cláusula compromissória constante de acordos ou contratos celebrados pelo Centro de Competências, ou nas suas decisões;

   2) Em litígios respeitantes à reparação de danos causados pelo pessoal do Centro de Competências no desempenho das suas funções;

   3) Em litígios entre o Centro de Competências e o seu pessoal, nos limites e condições estabelecidos pelo Estatuto dos Funcionários.

2. Em todas as matérias não abrangidas pelo presente regulamento ou por outros atos jurídicos da União, é aplicável o direito do Estado-Membro onde está situada a sede do Centro de Competências.

Artigo 41.º

Responsabilidade dos membros e seguros

1. A responsabilidade financeira dos membros pelas dívidas do Centro de Competências está limitada à contribuição que tenham já efetuado para as despesas administrativas.

2. O Centro de Competências subscreve e mantém em vigor os seguros adequados.

Artigo 42.º

Conflitos de interesses

O Conselho de Administração do Centro de Competências adota regras em matéria de prevenção e gestão de conflitos de interesses no que se refere aos seus membros, órgãos e pessoal. Essas regras incluem as disposições destinadas a evitar conflitos de interesses relativamente aos representantes dos membros em exercício no Conselho de Administração, bem como no Conselho Consultivo Industrial e Científico nos termos do Regulamento XXX [novo Regulamento Financeiro].

Artigo 43.º

Proteção de dados pessoais

1. O tratamento de dados pessoais pelo Centro de Competências está sujeito às disposições do Regulamento (UE) n.º XXX/2018 do Parlamento Europeu e do Conselho.

2. O Conselho de Administração adota as disposições de execução a que se refere o artigo xx.º, n. 3, do Regulamento (UE) n.º xxx/2018. O Conselho de Administração pode adotar medidas adicionais necessárias para a aplicação do Regulamento (UE) n.º xxx/2018 pelo Centro de Competências.

Artigo 44.º

Apoio do Estado-Membro de acolhimento

Entre o Centro de Competências e o Estado-Membro [Bélgica] em que se encontra a sua sede pode ser celebrado um acordo administrativo respeitante aos privilégios e imunidades e a outro apoio a prestar por esse Estado-Membro ao Centro de Competências.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Artigo 45.º

Ações iniciais

1. A Comissão é responsável pelo estabelecimento e funcionamento inicial do Centro de Competências, até que este disponha de capacidade operacional para executar o seu próprio orçamento. Nos termos do direito da União, a Comissão realiza todas as ações necessárias com a participação dos órgãos competentes do Centro de Competências.

2. Para efeitos do n.º 1, até o diretor executivo assumir as suas funções, após nomeação pelo Conselho de Administração, em conformidade com o estipulado no artigo 16.º, a Comissão pode designar um diretor executivo interino e exercer as respetivas funções, podendo este ser assistido por um número limitado de funcionários da Comissão. A Comissão pode afetar um número limitado dos seus funcionários a título provisório.

3. O diretor executivo interino pode autorizar todos os pagamentos abrangidos pelas dotações inscritas no orçamento anual do Centro de Competências, uma vez aprovados pelo Conselho de Administração, e adotar decisões e celebrar acordos e contratos, incluindo contratos de trabalho, após a aprovação do quadro de pessoal do Centro de Competências.

4. O diretor executivo interino determina, de comum acordo com o diretor executivo do Centro de Competências e sob reserva de aprovação pelo Conselho de Administração, a data em que o Centro de Competências passa a ter capacidade para executar o seu próprio orçamento. A partir dessa data, a Comissão abster-se-á de

conceder autorizações e executar pagamentos relacionados com as atividades do Centro de Competências.

Artigo 46.º

Duração

1. O Centro de Competências é criado pelo período que decorre de 1 de janeiro de 2021 a 31 de dezembro de 2029.
2. No fim desse período, salvo decisão em contrário através de uma revisão do presente regulamento, é acionado o processo de dissolução. O processo de dissolução é automaticamente acionado se a União ou todos os Estados-Membros participantes se retirarem do Centro de Competências.
3. Para efeitos do processo de dissolução do Centro de Competências, o Conselho de Administração nomeia um ou mais liquidatários para darem cumprimento às suas decisões.
4. Quando o Centro de Competências se encontrar em fase de dissolução, os seus ativos serão utilizados para cobrir as suas responsabilidades e as despesas decorrentes da dissolução. Qualquer excedente é distribuído entre a União e os Estados-Membros participantes, proporcionalmente à respetiva contribuição financeira para o Centro de Competências. O eventual excedente distribuído à União reverte para o orçamento da União.

Artigo 47.º

Entrada em vigor

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

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

1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB

1.3. Natureza da proposta/iniciativa

1.4. Objetivo(s)

1.5. Justificação da proposta/iniciativa

1.6. Duração e impacto financeiro

1.7. Modalidade(s) de gestão prevista(s)

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

2.2. Sistema de gestão e de controlo

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

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

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

3.2.2. Impacto estimado nas dotações operacionais

3.2.3. Impacto estimado nas dotações de natureza administrativa

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participação de terceiros no financiamento

3.3. Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

Regulamento que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança

1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB[35]

Investigação e inovação

Investimentos Estratégicos Europeus

1.3. Natureza da proposta/iniciativa

☒ A proposta/iniciativa refere-se a uma nova ação

☐ A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**[36]

☐ A proposta/iniciativa refere-se à prorrogação de uma ação existente

☐ 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. Um mercado único digital conectado

2. Um novo impulso para o emprego, o crescimento e o investimento

1.4.2. Objetivo(s) específico(s) em causa

Objetivos específicos

1.3 A economia digital pode desenvolver o seu pleno potencial apoiada por iniciativas que permitam o crescimento completo das tecnologias digitais e de dados.

2.1 A Europa mantém a sua posição de líder mundial na economia digital, onde as empresas europeias podem crescer a nível global, aproveitando o forte empreendedorismo digital e as empresas em fase de arranque com bom desempenho e onde a indústria e os serviços públicos dominam a transformação digital.

2.2. A investigação europeia encontra oportunidades de investimento para potenciais avanços e medidas emblemáticas no domínio da tecnologia, nomeadamente o programa Horizonte 2020/Horizonte Europa e o recurso a parcerias público-privadas.

[35] ABM: *activity based management* (gestão por atividades); ABB: *activity based budgeting* (orçamentação por atividades).

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

1.4.3. Resultados e impacto esperados

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

O Centro de Competências, juntamente com a Rede e a Comunidade, procurará a consecução dos seguintes objetivos:

(1) Contribuir para a execução da parte relativa à cibersegurança do Programa Europa Digital estabelecido pelo Regulamento n.º XXX, em especial as ações relacionadas com o artigo 6.º do Regulamento (UE) n.º XXX [Programa Europa Digital], bem como do Programa Horizonte Europa estabelecido pelo Regulamento n.º XXX, em especial o anexo I, pilar II, secção 2.2.6, da Decisão n.º XXX que estabelece o programa específico de execução do Horizonte Europa — Programa-Quadro de Investigação e Inovação, e bem assim de outros programas da União, quando previsto em atos jurídicos da União;

(2) Reforçar as capacidades, os conhecimentos e as infraestruturas de cibersegurança ao serviço das indústrias, do setor público e das comunidades de investigação;

(3) Contribuir para a ampla implantação de produtos e soluções de cibersegurança de vanguarda na economia;

(4) Melhorar a compreensão da cibersegurança e contribuir para reduzir as lacunas de competências na União relacionadas com a cibersegurança;

(5) Contribuir para o reforço da investigação e desenvolvimento no domínio da cibersegurança na União;

(6) Melhorar a colaboração entre as esferas civil e militar no tocante às tecnologias e aplicações de dupla utilização;

(7) Reforçar as sinergias entre as dimensões civil e militar da cibersegurança;

(8) Facilitar e ajudar a coordenar os trabalhos da Rede de Centros Nacionais de Coordenação («Rede») a que se refere o artigo 10.º e da Comunidade de Competências em Cibersegurança a que se refere o artigo 12.º.

1.4.4. Indicadores de resultados e de impacto

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

· Número de infraestruturas e/ou ferramentas de cibersegurança adquiridas conjuntamente.

· Concessão de acesso a tempo de testes e experimentação aos investigadores e à indústria europeus na Rede e no seio do Centro. Sempre que já existam instalações, aumento do número de horas disponíveis para essas comunidades comparativamente com as horas atualmente disponíveis.

· Aumento do número de comunidades de utilizadores servidas e o número de investigadores que obtêm acesso a instalações de cibersegurança europeias quando comparado com o número das que têm de procurar esses recursos fora da Europa.

· Início de um aumento da competitividade dos fornecedores europeus, expressa em termos de quota do mercado mundial (meta de 25 % de quota de mercado até 2027) e em termos de quota dos resultados de I&D europeus adotados pela indústria.

· Contribuição para as próximas tecnologias de cibersegurança, expressa em termos de direitos de autor, patentes, publicações científicas e produtos comerciais.

· Número de conteúdos curriculares no domínio das competências em cibersegurança avaliados e alinhados, número de programas de certificação profissional da cibersegurança avaliados.

· Número de cientistas, estudantes e utilizadores (industriais e das administrações públicas) formados.

1.5. Justificação da proposta/iniciativa

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

Alcançar uma massa crítica de investimento em desenvolvimento tecnológico e industrial no domínio da cibersegurança e superar a fragmentação das capacidades relevantes espalhadas pela UE.

1.5.2. Valor acrescentado da participação da UE.

A cibersegurança é uma questão de interesse comum da União, conforme confirmado pelas conclusões do Conselho supracitadas. A dimensão e caráter transfronteiriço de incidentes como o *WannaCry* ou o *NonPetya* constituem um exemplo claro. A natureza e dimensão dos desafios tecnológicos da cibersegurança, bem como a coordenação insuficiente de esforços no seio da indústria, do setor público e das comunidades de investigação, bem como entre estes, obriga a UE a continuar a apoiar esforços de coordenação para reunir uma massa crítica de recursos e assegurar melhores conhecimentos e uma melhor gestão dos ativos. Tal é necessário com vista: aos requisitos em termos de recursos relacionados com certas capacidades para investigação, o desenvolvimento e a implantação em matéria de cibersegurança; à necessidade de disponibilizar acesso a conhecimentos especializados interdisciplinares em cibersegurança (amiúde apenas disponíveis parcialmente a nível nacional) em diferentes disciplinas; à natureza global das cadeias de valor industriais, bem como à atividade dos concorrentes mundiais que trabalham nos mercados.

Tal exige recursos e conhecimentos especializados a um nível que dificilmente poderá ser satisfeito com a ação individual de qualquer Estado-Membro. Por exemplo, uma rede de comunicação quântica pan-europeia poderia exigir um investimento da UE na ordem dos 900 milhões de EUR, dependendo dos investimentos efetuados pelos Estados-Membros (para que fosse interligada/complementada) e do grau de possível reutilização das infraestruturas existentes.

1.5.3. Lições retiradas de experiências anteriores semelhantes

A avaliação intercalar do Horizonte 2020, entre outros aspetos, confirmou a pertinência continuada do apoio da UE à I&D e dos desafios sociais (entre eles o «Sociedades Seguras», a partir do qual é apoiada a I&D em cibersegurança). Ao mesmo tempo, a avaliação confirma que o reforço da liderança industrial continua a ser um desafio e que subsiste uma lacuna de inovação, com a UE a ficar para trás nos avanços e na criação de mercado em termos de inovação.

A avaliação intercalar do Mecanismo Interligar a Europa (MIE) parece confirmar o valor acrescentado da intervenção da UE para lá da I&D, embora, ao abrigo do MIE, a cibersegurança tivesse uma ênfase (na segurança operacional) e lógica de intervenção algo diferentes. Ao mesmo tempo, a maioria dos beneficiários de subvenções no domínio da cibersegurança do MIE — a Comunidade de Equipas de

Resposta a Incidentes de Segurança Informática (CSIRT) — manifestou o desejo de um programa de apoio personalizado ao abrigo do próximo QFP.

A criação, em 2016, da parceria público-privada contratual («PPPc») para a cibersegurança na UE representou um primeiro passo sólido, reunindo as comunidades de investigação, da indústria e do setor público para facilitar a investigação e a inovação em cibersegurança, sendo que, dentro dos limites do quadro financeiro 2014-2020, deverá proporcionar resultados positivos e mais concentrados na investigação e inovação. A PPPc permitiu aos parceiros industriais expressarem o seu compromisso de investimento individual em domínios definidos na agenda estratégica de investigação e inovação da parceria.

1.5.4. Compatibilidade e eventual sinergia com outros instrumentos adequados

A rede de competências em cibersegurança e o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança atuarão como um apoio adicional às disposições políticas e intervenientes existentes em matéria de cibersegurança. O mandato do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança será complementar aos esforços da ENISA, mas tem um foco diferente exige um conjunto diferente de competências. Enquanto a ENISA tenha um papel a desempenhar em matéria de aconselhamento sobre investigação e inovação na UE, o mandato proposto do Centro incide, em primeiro lugar, noutras tarefas cruciais para o reforço da resiliência em matéria de cibersegurança na UE. O Centro deverá estimular o desenvolvimento e a implantação de tecnologias de cibersegurança e complementar os esforços no sentido de reforçar as capacidades neste domínio, a nível nacional e da UE.

O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, juntamente com a rede de competências em cibersegurança, também trabalhará no sentido de apoiar a investigação a fim de facilitar e acelerar os processos de normalização e certificação, em especial os relacionados com os regimes de certificação da cibersegurança na aceção do Regulamento Cibersegurança.

O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança atuará como um mecanismo de execução único para dois programas europeus que apoiam a cibersegurança (Programa Europa Digital e Horizonte Europa) e reforçará a coerência e as sinergias entre os mesmos.

Esta iniciativa permite complementar os esforços dos Estados-Membros, prestando contributos apropriados para os decisores políticos no domínio da educação, a fim de melhorar o ensino em matéria de cibersegurança (por exemplo, desenvolvendo conteúdos curriculares de cibersegurança em sistemas educativos civis e militares, mas também contributos para a educação básica em cibersegurança). Permitirá igualmente apoiar o alinhamento e a avaliação contínua dos programas profissionais de certificação da cibersegurança — todas as atividades necessárias para ajudar a colmatar a lacuna no domínio das competências em cibersegurança e facilitar o acesso das indústrias e outras comunidades a especialistas em cibersegurança. O alinhamento da educação e das competências ajudará a desenvolver uma força de trabalho qualificada no domínio da cibersegurança na UE — um ativo fundamental para empresas de cibersegurança e para outras indústrias com interesses neste domínio.

1.6. Duração e impacto financeiro

☒ Proposta/iniciativa de duração limitada

– ☒ Proposta/iniciativa válida entre 1.1.2021 e 31.12.2029

– ☒ Impacto financeiro de 2021 a 2027 em termos de dotações de autorização e de 2021 a 2031 em termos de dotações de pagamento.

☐ Proposta/iniciativa de duração ilimitada

– Aplicação com um período de arranque progressivo entre AAAA e AAAA,

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

1.7. Modalidade(s) de gestão prevista(s)[37]

☐ Gestão direta por parte da Comissão

– ☐ por parte dos seus serviços, incluindo do seu pessoal nas delegações da União;

– ☐ por parte das agências de execução;

☐ Gestão partilhada com os Estados-Membros

☒

Gestão indireta confiando tarefas de execução orçamental:

– ☐ em países terceiros ou nos organismos por estes designados;

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

– ☐ no BEI e no Fundo Europeu de Investimento;

– ☒ nos organismos referidos nos artigos 70.º e 71.º do Regulamento Financeiro;

– ☐ nos organismos de direito público;

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

– ☐ nos 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;

– ☐ nas 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.

– *Se assinalar mais de uma modalidade de gestão, queira especificar na secção «Observações».*

[37] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições

O artigo 28.º contém disposições pormenorizadas em matéria de acompanhamento e prestação de informações.

2.2. Sistema de gestão e de controlo

2.2.1. Risco(s) identificado(s)

A fim de reduzir os riscos relacionados com o funcionamento do Centro de Competências após a sua criação e os atrasos ocorridos, a Comissão apoiará o Centro de Competências durante esta fase para assegurar o recrutamento rápido do pessoal principal e a criação de um sistema de controlo interno eficiente e de procedimentos sólidos.

2.2.2. Informações sobre o sistema de controlo interno criado

O diretor executivo é responsável pelas operações e pela gestão quotidiana do Centro de Competências e é o seu representante legal. O diretor é responsável perante o Conselho de Administração, ao qual presta contas regularmente sobre o andamento das atividades do Centro de Competências.

O Conselho de Administração assume a responsabilidade global pela orientação estratégica e pelo funcionamento do Centro de Competências e supervisiona a realização das suas atividades.

Após consulta da Comissão, o Conselho de Administração aprova as regras financeiras aplicáveis ao Centro de Competências. Estas regras só podem divergir do Regulamento (UE) n.º 1271/2013 se o funcionamento do Centro de Competências especificamente o exigir e a Comissão o tiver previamente autorizado.

O auditor interno da Comissão exerce relativamente ao Centro de Competências as mesmas competências que exerce em relação à Comissão. 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 do Centro de Competências.

2.2.3. Estimativa dos custos e benefícios dos controlos e avaliação do nível previsto de risco de erro

Custos e benefícios dos controlos

Os custos relativos ao controlo para o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança são repartidos entre o custo de supervisão a nível da Comissão e o custo dos controlos operacionais a nível do organismo de execução.

Os custos dos controlos a nível do Centro de Competências são estimados em cerca de 1,19 % das dotações de pagamento operacionais implementadas a nível do Centro de Competências.

O custo de supervisão a nível da Comissão está estimado em 1,20 % das dotações de pagamento operacionais implementadas a nível do Centro de Competências.

No pressuposto de que as atividades fossem inteiramente geridas pela Comissão sem apoio do organismo de execução, os custos do controlo seriam substancialmente superiores e poderiam fixar-se em cerca de 7,7 % das dotações de pagamento.

Os controlos previstos visam assegurar uma supervisão fluida e efetiva pela Comissão das entidades responsáveis pela execução e assegurar o necessário grau de garantias a nível da Comissão.

Os benefícios dos controlos são:

- Evitar a seleção de propostas mais fracas ou desadequadas.
- Otimizar o planeamento e a utilização dos fundos da UE, por forma a preservar o valor acrescentado da UE.
- Garantir a qualidade dos acordos de subvenção, evitando erros na identificação das entidades jurídicas, assegurando a correta determinação das contribuições da UE e acautelando as garantias necessárias para o correto funcionamento dos mecanismos de subvenção.
- Deteção de custos não elegíveis na fase de pagamento.
- Deteção de erros que afetem a legalidade e regularidade das operações na fase de auditoria.

Nível de erro estimado

O objetivo será manter a taxa de erro residual abaixo do limiar de 2 % ao longo de todo o programa, limitando ao mesmo tempo o ónus dos controlos para os beneficiários, por forma a assegurar o correto equilíbrio entre o objetivo de legalidade e regularidade e outros objetivos como a atratividade do programa, em particular para as PME, e a contenção do custo dos controlos.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas

O OLAF pode realizar inquéritos, incluindo verificações e inspeções no local, em conformidade com as disposições e os procedimentos previstos 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, 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 verificar a existência de fraudes, de atos de corrupção ou de outras atividades ilegais lesivas dos interesses financeiros da União no âmbito de uma convenção de subvenção ou de um contrato financiado pelo Centro de Competências.

Os acordos, decisões e contratos resultantes da execução do presente regulamento devem conter as disposições que habilitem expressamente a Comissão, o Centro de Competências, o Tribunal de Contas e o OLAF a realizarem auditorias e inquéritos, de acordo com as respetivas competências.

O Centro de Competências deve assegurar que os interesses financeiros dos seus membros sejam devidamente protegidos, realizando ou mandando realizar controlos internos e externos adequados.

O Centro de Competências adere 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). O Centro de Competências adota as medidas necessárias para facilitar os inquéritos internos efetuados pelo OLAF.

O Centro de Competências adotará uma estratégia antifraude, com base na análise dos riscos de fraude e considerações de custo-benefício. Esta estratégia deve proteger os interesses financeiros da União mediante a aplicação de medidas preventivas contra a fraude, a corrupção e quaisquer outras atividades ilegais, 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.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica do quadro financeiro plurianual e nova(s) rubrica(s) orçamental(ais) de despesas proposta(s)

- Novas rubricas orçamentais, cuja criação é solicitada

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			
	Número	DD/DND[38]	dos países EFTA[39]	dos países candidatos [40]	de países terceiros	na aceção do artigo [21.º, n.º 2, alínea b)], do Regulamento Financeiro
Rubrica 1: Mercado Único, Inovação e Digitalização	01 02 XX XX Horizonte Europa — Centro de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança — apoio financeiro 01 02 XX XX Horizonte Europa — Centro de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança 02 06 01 XX Programa Europa Digital — Centro de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança — apoio financeiro 02 06 01 XX Programa Europa Digital — Centro de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança	Dif.	SIM	SIM (se especificado no programa de trabalho anual)	SIM (limitado a algumas partes do programa)	NÃO

[38] DD = dotações diferenciadas/DND = dotações não diferenciadas.
[39] EFTA: Associação Europeia de Comércio Livre.
[40] Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

- Prevê-se que as contribuições para estas rubricas orçamentais provenham de:

Em milhões de EUR (três casas decimais)

Rubrica orçamental	Ano de 2021	Ano de 2022	Ano de 2023	Ano de 2024	Ano de 2025	Ano de 2026	Ano de 2027	**Total**
01 01 01 01 Despesas relacionadas com funcionários e agentes temporários na área da investigação — Horizonte Europa	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	**p.m.**
01 01 01 02 Pessoal externo que executa programas de investigação — Horizonte Europa	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	**p.m.**
01 01 01 03 Outras despesas de gestão para investigação – Horizonte Europa	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	**p.m.**
01 02 02 Desafios Globais e Competitividade Industrial	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	p.m.	**p.m.**
02 01 04 apoio administrativo — Programa Europa Digital	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Cibersegurança — Programa Europa Digital	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Total da despesa	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

A contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), será proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político. A proposta terá por base o resultado do processo de planeamento estratégico conforme definido no artigo 6.º, n.º 6. do Regulamento XXX [programa-quadro Horizonte Europa].

Os montantes supra não incluem a contribuição dos Estados-Membros para os custos operacionais e administrativos do Centro de Competências, proporcionais à contribuição financeira da União.

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**	**1**	Mercado Único, Inovação e Digitalização

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Após 2027***	**TOTAL**
Título 1 (Despesas com pessoal)	Autorizações = Pagamentos	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Título 2 (Infraestruturas e despesas operacionais)	Autorizações = Pagamentos	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Título 3 (Despesas operacionais)	Autorizações	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Pagamentos	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
TOTAL das dotações para o	Autorizações	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**

[41] As dotações de pessoal apenas são contabilizadas para um semestre em 2021

enquadramento financeiro dos programas[42]	Pagamentos	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

[42] O total das dotações estabelecido apenas diz respeito aos recursos financeiros da UE dedicados à cibersegurança ao abrigo do programa Europa Digital. A contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 5.º, n.º 1, alínea b), será proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político. A proposta terá por base o resultado do processo de planeamento estratégico conforme definido no artigo 6.º, n.º 6. do Regulamento XXX [programa-quadro Horizonte Europa].

Rubrica do quadro financeiro **plurianual**	7	«Despesas administrativas»

Em milhões de EUR (três casas decimais)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Após 2027***	**TOTAL**
Recursos humanos		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Outras despesas administrativas		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
TOTAL das dotações no âmbito da RUBRICA 7 do quadro financeiro plurianual	(Total das autorizações = total dos pagamentos)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

Em milhões de EUR (três casas decimais)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Após 2027***	**TOTAL**
TOTAL das dotações **das RUBRICAS** do quadro financeiro plurianual	Autorizações	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Pagamentos	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 ²061,715**	**2 005,637**

3.2.2. Síntese do impacto estimado nas dotações de natureza administrativa

– ☐ 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)

Anos	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
RUBRICA 7 **do quadro financeiro plurianual**								
Recursos humanos	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Outras despesas administrativas	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Subtotal da RUBRICA 7 **do quadro financeiro plurianual**	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**
Com exclusão da RUBRICA 7[43] do quadro financeiro plurianual								
Recursos humanos								
Outras despesas de natureza administrativa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Subtotal com exclusão da RUBRICA 7 **do quadro financeiro plurianual**	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**
TOTAL	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

As dotações necessárias para recursos humanos e outras despesas administrativas serão cobertas pelas dotações da DG já afetadas à gestão da ação e/ou reafetadas internamente na DG, se necessário em conjunto com eventuais dotações adicionais que sejam atribuídas à DG gestora no âmbito dos procedimentos anuais de afetação e em função das limitações orçamentais.

As dotações supracitadas necessárias para recursos humanos e outras despesas de natureza administrativa, com exclusão da rubrica 7, correspondem aos montantes abrangidos pela contribuição financeira do programa Europa Digital.

As dotações necessárias para recursos humanos e outras despesas de natureza administrativa, com exclusão da rubrica 7, serão acrescidas dos montantes abrangidos pela contribuição financeira da União proveniente do programa Horizonte Europa, assim que a contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e

[43] Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), for proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político.

Os montantes supracitados de dotações necessárias para recursos humanos e outras despesas de natureza administrativa, com exclusão da rubrica 7, não incluem a contribuição dos Estados-Membros para as despesas administrativas do Centro de Competências, proporcional à contribuição financeira da União.

3.2.2.1. Necessidades estimadas de recursos humanos para a Comissão

– ☐ 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 termos de equivalente a tempo completo

Anos		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Lugares do quadro do pessoal (funcionários e agentes temporários)								
Sede e gabinetes de representação da Comissão		20	21	21	21	21	21	22
Delegações								
Investigação								
• Pessoal externo (em equivalente a tempo completo: **ETC) — AC, AL, PND, TT e JPD**[44] Rubrica 7								
Financiado a partir da RUBRICA 7 do quadro financeiro plurianual	- na sede	3	3	3	3	3	3	3
	- nas delegações							
Financiado a partir da dotação financeira do programa[45]	- na sede							
	- nas delegações							
Investigação								
Outros (especificar)								
TOTAL		**23**	**23**	**24**	**24**	**24**	**25**	**25**

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

Funcionários e agentes temporários	Coordenação, monitorização e direção das atribuições confiadas ao Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, incluindo custos de apoio e coordenação. Desenvolvimento e coordenação da política no domínio da cibersegurança relativamente às atribuições confiadas ao Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, por exemplo, no que diz respeito à fixação de prioridades para a política industrial e de investigação, à cooperação geral entre Estados-Membros e operadores económicos, à coerência com o futuro quadro de certificação da cibersegurança da UE, aos trabalhos em matéria de responsabilidade e dever de diligência, ou à coordenação com as políticas em matéria de CAD, IA e competências

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

45 Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»)

	digitais. .
Pessoal externo	Coordenação, monitorização e direção das atribuições confiadas ao Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, incluindo custos de apoio e coordenação. Desenvolvimento e coordenação da política no domínio da cibersegurança relativamente às atribuições confiadas ao Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, por exemplo, no que diz respeito à fixação de prioridades para a política industrial e de investigação, à cooperação geral entre Estados-Membros e operadores económicos, à coerência com o futuro quadro de certificação da cibersegurança da UE, aos trabalhos em matéria de responsabilidade e dever de diligência, ou à coordenação com as políticas em matéria de CAD, IA e competências digitais. .

3.2.2.2. Necessidades estimadas de recursos humanos no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança

	2021	2022	2023	2024	2025	2026	2027
Funcionários da Comissão							
Dos quais AD							
Dos quais AST							
Dos quais AST-SC							
Agentes temporários							
Dos quais AD	10	11	13	13	13	13	13
Dos quais AST							
Dos quais AST-SC							
Agentes contratuais	26	32	39	39	39	39	39
PND	1	1	1	1	1	1	1
Total	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Descrição das tarefas a executar:

Funcionários e agentes temporários	Execução operacional das atribuições confiadas ao Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança nos termos do artigo 4.º do presente regulamento, incluindo custos de apoio e coordenação.
Pessoal externo	Execução operacional das atribuições confiadas ao Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança nos termos do artigo 4.º do presente regulamento, incluindo custos de apoio e coordenação.

As necessidades acima estimadas de recursos humanos no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança correspondem às necessidades estimadas para executar a contribuição financeira da União ao abrigo do programa Europa Digital.

As necessidades acima estimadas de recursos humanos no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança serão acrescidos das necessidades estimadas para executar a contribuição financeira da União ao abrigo do Horizonte Europa, assim que a contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), for proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político.

3.2.2.3. Quadro de pessoal do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança

Grupo de funções e graus	2021	2022	2023	2024	2025	2025	2025
AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
Total AD	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
Total AST							

AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
Totais AST/SC							
TOTAL GERAL	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Impacto estimado no pessoal (adicional) — pessoal externo do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança

Agentes contratuais	2021	2022	2023	2024	2025	2026	2027
Grupo de funções IV	20	22	29	29	29	29	29
Grupo de funções III	2	4	4	4	4	4	4
Grupo de funções II	4	6	6	6	6	6	6
Grupo de funções I							
Total	**26**	**32**	**39**	**39**	**39**	**39**	**39**

A fim de assegurar a neutralidade no plano dos efetivos, o reforço de pessoal no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança será parcialmente compensado pela redução no número de funcionários e pessoal externo (ou seja, do presente quadro de efetivos e de pessoal externo) nos serviços da Comissão relevantes.
Os números de pessoal no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança nos pontos 3.2.2.2 e 3.2.2.4 serão compensados como se segue[46]:

TOTAL	2021	2022	2023	2024	2025	2026	2027
Funcionários da Comissão	5	5	6	6	6	6	6
Agentes temporários							
Agentes contratuais	14	17	20	20	20	20	20

[46] Sujeito ao montante final do orçamento cuja execução será delegada no Centro de Competências

PND							
Total ETC	19	22	26	26	26	26	26
Efetivo	19	22	26	26	26	26	26

A compensação dos recursos humanos no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança será proporcional à quota-parte da contribuição financeira da União, ou seja, 50 %.

A compensação supra diz respeito às necessidades estimadas de recursos humanos no Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança para executar a contribuição financeira da União ao abrigo do Europa Digital.

A compensação supra será acrescida das necessidades estimadas para executar a contribuição financeira da União ao abrigo do Horizonte Europa, assim que a contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), for proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político.

3.2.3. Participação de terceiros no financiamento

A proposta/iniciativa:

– ☐ não prevê o cofinanciamento por terceiros

– ☒ prevê o cofinanciamento por terceiros[47] estimado a seguir:

Dotações em milhões de EUR (três casas decimais)

Anos	2021	2022	2023	2024	2025	2026	2027	TOTAL
Estados-Membros — contribuição para despesas com pessoal	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Estados-Membros — contribuição para infraestruturas e despesas operacionais	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Estados-Membros — contribuição para despesas operacionais	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
TOTAL das dotações cofinanciadas	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

A contribuição de terceiros supracitada diz apenas respeito ao cofinanciamento proporcional aos recursos financeiros da UE dedicados à cibersegurança ao abrigo do programa Europa Digital. A contribuição de terceiros supracitada será aumentada assim que a contribuição da dotação financeira do agregado «Sociedade Inclusiva e Segura» do Pilar II «Desafios Globais e Competitividade Industrial» do Horizonte Europa (dotação total de 2 800 000 000 EUR) referida no artigo 21.º, n.º 1, alínea b), for proposta pela Comissão durante o processo legislativo e, em qualquer caso, antes de alcançar um acordo político. A proposta terá por base o resultado do processo de planeamento estratégico conforme definido no artigo 6.º, n.º 6. do Regulamento XXX [programa-quadro Horizonte Europa].

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

☐ nas outras receitas

indicar se as receitas são afetadas a rubricas de despesas ☐

Em milhões de EUR (três casas decimais)

Rubrica orçamental das	Impacto da proposta/iniciativa[48]

[47] Contribuições em espécie estimada dos Estados-Membros

[48] No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 20 % a título de despesas de cobrança.

receitas:	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artigo …….							

Relativamente às receitas afetadas, especificar a(s) rubrica(s) orçamental(ais) de despesas envolvida(s).

Outras observações (p. ex.: método/fórmula utilizado/a para o cálculo do impacto sobre as receitas ou qualquer outra informação).