Conselho da
União Europeia

**Bruxelas, 20 de abril de 2023**
**(OR. en)**

**8512/23**

**Dossiê interinstitucional:**
**2023/0109(COD)**

**CYBER 92**
**TELECOM 108**
**CADREFIN 51**
**FIN 448**
**BUDGET 6**
**IND 181**
**JAI 471**
**MI 314**
**DATAPROTECT 110**
**RELEX 481**
**CODEC 662**

**PROPOSTA**

| | |
|---|---|
| de: | Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora |
| data de receção: | 19 de abril de 2023 |
| para: | Thérèse BLANCHET, secretária-geral do Conselho da União Europeia |
| n.° doc. Com.: | COM(2023) 209 final |
| Assunto: | Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança |

Envia-se em anexo, à atenção das delegações, o documento COM(2023) 209 final.

Anexo: COM(2023) 209 final

COMISSÃO
EUROPEIA

Estrasburgo, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Proposta de

# REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

## que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança

# EXPOSIÇÃO DE MOTIVOS

## 1. CONTEXTO DA PROPOSTA

### • Razões e objetivos da proposta

A presente exposição de motivos acompanha a proposta de Regulamento Cibersolidariedade. A utilização e a dependência de tecnologias da informação e comunicação tornaram-se características fundamentais de todos os setores de atividade económica, uma vez que as nossas administrações públicas, as nossas empresas e os nossos cidadãos nunca estiveram tão interligados e dependentes de outros setores e países. Esta maior adoção das tecnologias digitais aumenta a exposição a incidentes de cibersegurança e os seus potenciais impactos. Ao mesmo tempo, os Estados-Membros enfrentam riscos de cibersegurança crescentes e um cenário de ameaças global complexo, com um claro risco de rápida disseminação dos ciberincidentes de um Estado-Membro para outro.

Além disso, as ciberoperações estão cada vez mais integradas em estratégias híbridas e de guerra, com efeitos significativos no alvo. Em especial, a agressão militar da Rússia contra a Ucrânia foi precedida e está a ser acompanhada de uma estratégia de ciberoperações hostis, o que constitui um fator de mudança para a perceção e a avaliação do grau de preparação da UE em matéria de gestão coletiva de crises de cibersegurança e um apelo à adoção de medidas urgentes. A ameaça de um eventual incidente em grande escala que cause perturbações e danos consideráveis às infraestruturas críticas exige uma maior preparação a todos os níveis do ecossistema de cibersegurança da UE. Essa ameaça vai além da agressão militar da Rússia contra a Ucrânia e inclui ciberameaças contínuas de intervenientes estatais e não estatais, que provavelmente persistirão, dada a multiplicidade de intervenientes associados ao Estado, criminosos e ativistas háquer envolvidos nas atuais tensões geopolíticas. Nos últimos anos, o número de ciberataques aumentou drasticamente, incluindo ataques de ciberespionagem, sequestro por programas maliciosos ou perturbação da cadeia de abastecimento. Em 2020, o ataque contra a cadeia de abastecimento da SolarWinds afetou mais de 18 000 organizações a nível mundial, incluindo organismos governamentais e grandes empresas. Os incidentes de cibersegurança significativos podem ser demasiado disruptivos para que um único ou vários Estados-Membros afetados os possam abordar sozinhos. Por esse motivo, é necessária uma solidariedade reforçada à escala da União, que permita uma melhor deteção, preparação e resposta a ameaças e incidentes de cibersegurança.

No que diz respeito à deteção de ciberameaças e ciberincidentes, é urgente aumentar o intercâmbio de informações e melhorar as nossas capacidades coletivas a fim de reduzir drasticamente o tempo necessário para detetar ciberameaças, antes de estas poderem causar danos e custos em grande escala [1]. Apesar de muitas ameaças e incidentes de cibersegurança terem uma potencial dimensão transfronteiriça, devido à interligação das infraestruturas

[1] De acordo com um relatório do Ponemon Institute e da IBM Security, em 2022, o tempo médio para identificar uma violação da segurança foi de 207 dias, tendo a sua contenção exigido mais 70 dias. Ao mesmo tempo, em 2022, as violações de dados com um ciclo de vida superior a 200 dias tiveram um custo médio de 4,86 milhões de EUR, em comparação com 3,74 milhões de EUR quando o ciclo de vida foi inferior a 200 dias. (*Cost of a data breach 2022*, https://www.ibm.com/reports/data-breach).

digitais, a partilha de informações pertinentes entre os Estados-Membros continua a ser limitada. A criação de uma rede de centros de operações de segurança (SOC, do inglês *Security Operations Centres*) transfronteiriços para reforçar as capacidades de deteção e resposta visa ajudar a resolver este problema.

No que diz respeito à preparação e resposta a incidentes de cibersegurança, existe atualmente um apoio limitado à escala da União e uma solidariedade limitada entre os Estados-Membros. As conclusões do Conselho de outubro de 2021 salientaram a necessidade de colmatar estas lacunas, convidando a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança [2].

O presente regulamento aplica igualmente a Estratégia de Cibersegurança da UE, adotada em dezembro de 2020 [3], que anunciava a criação de um ciberescudo europeu, reforçando as capacidades de deteção de ciberameaças e de partilha de informações na União Europeia através de uma federação de SOC nacionais e transfronteiriços.

O presente regulamento baseia-se nas primeiras medidas já elaboradas em estreita colaboração com as principais partes interessadas e apoiadas pelo Programa Europa Digital. Em especial, no que diz respeito aos SOC, no âmbito do programa de trabalho em matéria de cibersegurança do Programa Europa Digital para 2021-2022, foi lançado um convite à manifestação de interesse para a aquisição conjunta de ferramentas e infraestruturas para a criação de SOC transfronteiriços, bem como um convite à apresentação de propostas para a concessão de subvenções para permitir o reforço das capacidades dos SOC ao serviço de organizações públicas e privadas. No que diz respeito à preparação e à resposta a incidentes, a Comissão criou um programa de curto prazo para apoiar os Estados-Membros, mediante a afetação de financiamento adicional à Agência da União Europeia para a Cibersegurança (ENISA), a fim de reforçar a título imediato a preparação e as capacidades de resposta a ciberincidentes graves. Ambas as ações foram preparadas em estreita coordenação com os Estados-Membros. O presente regulamento vem colmatar as lacunas e integrar as informações extraídas dessas ações.

Por último, a presente proposta dá cumprimento ao compromisso, em consonância com a Comunicação Conjunta sobre Ciberdefesa [4] adotada em 10 de novembro, de preparar uma proposta de iniciativa da UE em matéria de cibersolidariedade com os seguintes objetivos: reforçar as capacidades comuns de deteção, conhecimento da situação e resposta da UE, criar progressivamente uma reserva de cibersegurança a nível da UE com serviços de fornecedores privados de confiança e apoiar a avaliação das entidades críticas.

---

2 Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, aprovadas pelo Conselho na sua reunião de 23 de maio de 2022 (9364/22).

3 Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Estratégia de cibersegurança da UE para a década digital» [JOIN(2020) 18 final].

4 Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Política de ciberdefesa da UE» [JOIN(2022) 49 final].

Neste contexto, a Comissão apresenta o presente Regulamento Cibersolidariedade para reforçar a solidariedade à escala da União a fim de melhor detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança através dos seguintes objetivos específicos:

- reforçar a deteção e o conhecimento da situação comuns a nível da UE relativamente a ciberameaças e ciberincidentes, contribuindo assim para a soberania tecnológica europeia no domínio da cibersegurança,
- aumentar o grau de preparação das entidades críticas em toda a UE e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente ao disponibilizar apoio à resposta a incidentes a países terceiros associados ao Programa Europa Digital,
- reforçar a resiliência da União e contribuir para uma resposta eficaz mediante a análise e avaliação de incidentes significativos ou em grande escala, inclusive retirando ensinamentos e, se for caso disso, formulando recomendações.

Esses objetivos são executados através das seguintes ações:

- implantação de uma infraestrutura pan-europeia de SOC (ciberescudo europeu) para criar e reforçar capacidades comuns de deteção e conhecimento da situação,
- criação de um mecanismo de ciberemergência para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala. O apoio à resposta a incidentes deve também ser disponibilizado às instituições, órgãos e organismos da União,
- criação de um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala específicos.

O ciberescudo europeu e o mecanismo de ciberemergência serão apoiados por financiamento do Programa Europa Digital, que o presente instrumento legislativo alterará a fim de estabelecer as ações acima referidas, prever apoio financeiro para o seu desenvolvimento e clarificar as condições para beneficiar do apoio financeiro.

**• Coerência com as disposições existentes da mesma política setorial**

O quadro da UE inclui vários atos legislativos já em vigor ou propostos a nível da União para reduzir as vulnerabilidades, aumentar a resiliência das entidades críticas contra os riscos de cibersegurança e apoiar a gestão coordenada de incidentes e crises de cibersegurança em grande escala, nomeadamente a Diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação na União (SRI 2) [5], o Regulamento

[5] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2).

Cibersegurança [6], a Diretiva relativa a ataques contra os sistemas de informação [7] e a Recomendação (UE) 2017/1584 da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala [8].

As ações propostas ao abrigo do Regulamento Cibersolidariedade abrangem o conhecimento da situação, a partilha de informações e o apoio à preparação e resposta a ciberincidentes. Estas ações apoiam e são coerentes com os objetivos do quadro regulamentar em vigor a nível da União, nomeadamente ao abrigo da Diretiva (UE) 2022/2555 («Diretiva SRI 2»). O Regulamento Cibersolidariedade terá por base e apoiará especialmente os quadros de cooperação operacional e de gestão de crises existentes em matéria de cibersegurança, em particular a Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe) e a rede de equipas de resposta a incidentes de segurança informática (CSIRT).

As plataformas de SOC transfronteiriças devem constituir uma nova capacidade complementar à rede de CSIRT mediante a mutualização e partilha de dados sobre ameaças à cibersegurança provenientes de entidades públicas e privadas, a valorização desses dados através de análises de peritos e de ferramentas de ponta, bem como o contributo para o desenvolvimento das capacidades e da soberania tecnológica da União.

Por último, a presente proposta é coerente com a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas [9], que convida os Estados-Membros a tomarem medidas urgentes e eficazes, bem como a cooperarem leal e eficientemente, de forma solidária e coordenada, entre si, com a Comissão e com outras autoridades públicas competentes a fim de reforçar a resiliência das infraestruturas críticas utilizadas para prestar serviços essenciais no mercado interno.

- **Coerência com outras políticas da União**

A proposta é coerente com outros mecanismos e protocolos de emergência em situações de crise, como o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR). O Regulamento Cibersolidariedade complementará estes quadros e protocolos de gestão de crises, prestando apoio específico à preparação e resposta a incidentes de cibersegurança. A proposta será igualmente coerente com a ação externa da UE em resposta a incidentes em

---

6 Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança).

7 Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.

8 Proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera o Regulamento (UE) 2019/1020 [COM(2022) 454 final].

9 Recomendação do Conselho, de 8 de dezembro de 2022, relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas (Texto relevante para efeitos do EEE) (2023/C 20/01).

grande escala no quadro da política externa e de segurança comum (PESC), nomeadamente através do conjunto de instrumentos de ciberdiplomacia da UE. A proposta complementará as ações executadas no contexto do artigo 42.º, n.º 7, do Tratado da União Europeia ou nas situações definidas no artigo 222.º do Tratado sobre o Funcionamento da União Europeia.

Complementa igualmente o Mecanismo de Proteção Civil da União (MPCU) [10], criado em dezembro de 2013 e completado por um novo ato legislativo adotado em maio de 2021 [11], que reforça os pilares de prevenção, preparação e resposta do MPCU, confere à UE capacidades adicionais para responder a novos riscos na Europa e no mundo e fomenta a reserva rescEU.

## 2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

### • Base jurídica

A base jurídica da presente proposta é constituída pelo artigo 173.º, n.º 3, e pelo artigo 322.º, n.º 1, alínea a), do Tratado sobre o Funcionamento da União Europeia (TFUE). O artigo 173.º do TFUE prevê que a União e os Estados-Membros zelem por que sejam asseguradas as condições necessárias ao desenvolvimento da capacidade concorrencial da indústria da União. O presente regulamento visa reforçar a posição competitiva dos setores da indústria e dos serviços europeus na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Em especial, visa aumentar a resiliência dos cidadãos, das empresas e das entidades que operam em setores críticos e altamente críticos contra as ameaças crescentes à cibersegurança, que podem ter impactos societais e económicos devastadores.

A proposta baseia-se também no artigo 322.º, n.º 1, alínea a), do TFUE, uma vez que contém regras específicas de transição que derrogam o princípio da anualidade estabelecido no Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho («Regulamento Financeiro») [12]. Para efeitos de boa gestão financeira e tendo em conta a natureza imprevisível, excecional e específica do panorama da cibersegurança e das ciberameaças, o mecanismo de emergência em matéria de cibersegurança deve beneficiar de um certo grau de flexibilidade em relação à gestão orçamental, em especial, ao permitir que as dotações de autorização e de pagamento não utilizadas para ações que prossigam os objetivos estabelecidos no regulamento transitem automaticamente para o exercício seguinte. Uma vez que esta nova regra levanta questões relacionadas com o Regulamento Financeiro, este assunto poderá ser abordado no contexto das atuais negociações da reformulação do mesmo.

---

10 Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (Texto relevante para efeitos do EEE).

11 Regulamento (UE) 2021/836 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que altera a Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União Europeia (Texto relevante para efeitos do EEE).

12 Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União (JO L 193 de 30.7.2018, p. 1).

- **Subsidiariedade (no caso de competência não exclusiva)**

A natureza marcadamente transfronteiriça das ameaças de cibersegurança e o número crescente de riscos e incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos da presente intervenção não podem ser eficazmente alcançados pelos Estados-Membros de forma isolada e exigem uma ação comum e solidariedade à escala da União.

A experiência no combate a ciberameaças decorrente da guerra contra a Ucrânia, juntamente com os ensinamentos retirados de um exercício de cibersegurança realizado durante a Presidência francesa (EU CyCLES), demonstrou que devem ser criados mecanismos concretos de apoio mútuo, incluindo a cooperação com o setor privado, para alcançar a solidariedade à escala da UE. Perante este cenário, as Conclusões do Conselho, de 23 de maio de 2022, sobre o desenvolvimento da postura da União Europeia no ciberespaço convidam a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança.

O apoio e as ações a nível da União que visam uma melhor deteção das ameaças à cibersegurança e um aumento das capacidades de preparação e resposta proporcionam valor acrescentado, uma vez que evitam a duplicação de esforços em toda a União e nos Estados-Membros, conduzindo a uma melhor exploração dos ativos existentes e a uma maior coordenação e intercâmbio de informações sobre os ensinamentos retirados. O mecanismo de ciberemergência prevê igualmente a prestação de apoio a países terceiros associados ao Programa Europa Digital a partir da Reserva de Cibersegurança da UE.

O apoio prestado através das várias iniciativas a criar e a financiar a nível da União complementará e não duplicará as capacidades nacionais em matéria de deteção, conhecimento da situação, preparação e resposta a ciberameaças e ciberincidentes.

- **Proporcionalidade**

As ações não vão além do que é necessário para alcançar os objetivos gerais e específicos do regulamento. As ações previstas no presente regulamento não afetam as responsabilidades dos Estados-Membros em matéria de segurança nacional, segurança pública, prevenção, investigação, deteção e repressão de infrações penais. Também não afetam as obrigações jurídicas das entidades que operam em setores críticos e altamente críticos de adotarem medidas de cibersegurança, em conformidade com a Diretiva SRI 2.

As ações abrangidas pelo presente regulamento complementam esses esforços e medidas, apoiando a criação de infraestruturas para uma melhor deteção e análise de ameaças e prestando apoio a ações de preparação e resposta em caso de incidentes significativos ou em grande escala.

- **Escolha do instrumento**

A proposta assume a forma de um regulamento do Parlamento Europeu e do Conselho. Trata-se do instrumento jurídico mais adequado, dado que só um regulamento, com as suas

disposições jurídicas diretamente aplicáveis, pode proporcionar o nível de uniformidade necessário para o estabelecimento e o funcionamento de um ciberescudo e de um mecanismo de ciberemergência europeus, prevendo apoio do Programa Europa Digital para a sua criação, bem como condições claras para a utilização e atribuição desse apoio.

## 3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- **Consultas das partes interessadas**

As ações do presente regulamento serão apoiadas pelo Programa Europa Digital, que foi objeto de uma ampla consulta. Além disso, basear-se-ão nas primeiras medidas que foram preparadas em estreita cooperação com as principais partes interessadas. No que diz respeito aos SOC, a Comissão elaborou um documento de reflexão sobre a criação de plataformas de SOC transfronteiriças e um convite à manifestação de interesse em estreita cooperação com os Estados-Membros no quadro do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC). Neste contexto, foi realizado um inquérito sobre as capacidades dos SOC nacionais e foram debatidas abordagens e requisitos técnicos comuns no âmbito do grupo de trabalho técnico do ECCC, que reúne representantes dos Estados-Membros. Adicionalmente, realizaram-se intercâmbios com a indústria, nomeadamente através do grupo de peritos sobre SOC criado pela ENISA e pela Organização Europeia para Cibersegurança (ECSO).

Em segundo lugar, no que diz respeito à preparação e à resposta a incidentes, a Comissão criou um programa de curto prazo para apoiar os Estados-Membros, mediante a afetação de financiamento adicional à ENISA ao abrigo do Programa Europa Digital, a fim de reforçar a título imediato a preparação e as capacidades de resposta a ciberincidentes graves. As opiniões dos Estados-Membros e da indústria recolhidas durante a execução deste programa de curto prazo fornecem já informações valiosas que contribuíram para a preparação da proposta de regulamento a fim de colmatar as lacunas identificadas. Tratou-se de um primeiro passo em consonância com as Conclusões do Conselho sobre a postura no ciberespaço, nas quais se convida a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança.

Além disso, em 16 de fevereiro de 2023, com base num documento de reflexão, realizou-se um seminário com peritos dos Estados-Membros sobre o mecanismo de ciberemergência. Todos os Estados-Membros participaram neste seminário e onze forneceram contribuições adicionais por escrito.

- **Avaliação de impacto**

Dada a natureza urgente da proposta, não foi efetuada uma avaliação de impacto. As ações do presente regulamento serão apoiadas pelo Programa Europa Digital e estão em consonância com as estabelecidas no Regulamento Programa Europa Digital, que foi objeto de uma avaliação de impacto específica. O presente regulamento não terá impactos administrativos ou

ambientais significativos para além dos já avaliados na avaliação de impacto do Regulamento Programa Europa Digital.

Além disso, baseia-se nas primeiras ações desenvolvidas em estreita colaboração com as principais partes interessadas, conforme acima referido, e dá seguimento ao convite dos Estados-Membros para que a Comissão apresente uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança até ao final do terceiro trimestre de 2022.

Especificamente, no que respeita ao conhecimento da situação e à deteção no quadro do ciberescudo europeu, no âmbito do programa de trabalho em matéria de cibersegurança do Programa Europa Digital para 2021-2022, foi lançado um convite à manifestação de interesse para a aquisição conjunta de ferramentas e infraestruturas para a criação de SOC transfronteiriços, bem como um convite à apresentação de propostas para a concessão de subvenções para permitir o reforço das capacidades dos SOC ao serviço de organizações públicas e privadas.

No domínio da preparação e resposta a incidentes, tal como acima referido, a Comissão criou um programa de curto prazo para apoiar os Estados-Membros no âmbito do Programa Europa Digital, que está a ser executado pela ENISA. Os serviços abrangidos incluem ações de preparação, como testes de penetração de entidades críticas para identificar vulnerabilidades. O programa reforça igualmente as possibilidades de assistência aos Estados-Membros em caso de incidentes graves que afetem entidades críticas. A execução deste programa de curto prazo pela ENISA está em curso e já forneceu informações pertinentes que foram tidas em conta na preparação do presente regulamento.

- **Direitos fundamentais**

Ao contribuir para a segurança da informação digital, a presente proposta contribuirá para proteger o direito à liberdade e à segurança, em conformidade com o artigo 6.º da Carta dos Direitos Fundamentais da União Europeia, e o direito ao respeito pela vida privada e familiar, em conformidade com o artigo 7.º da Carta dos Direitos Fundamentais da União Europeia. Ao proteger as empresas de ciberataques economicamente prejudiciais, a proposta contribuirá igualmente para a liberdade de empresa, em conformidade com o artigo 16.º da Carta dos Direitos Fundamentais da União Europeia, e para o direito de propriedade, em conformidade com o artigo 17.º da Carta dos Direitos Fundamentais da União Europeia. Por último, ao proteger a integridade das infraestruturas críticas face aos ciberataques, a proposta contribuirá para o direito à proteção da saúde, em conformidade com o artigo 35.º da Carta dos Direitos Fundamentais da União Europeia, e para o direito de acesso a serviços de interesse económico geral, em conformidade com o artigo 36.º da Carta dos Direitos Fundamentais da União Europeia.

## 4. INCIDÊNCIA ORÇAMENTAL

As ações do presente regulamento serão apoiadas por financiamento concedido ao abrigo do objetivo estratégico «Cibersegurança» do Programa Europa Digital.

O orçamento total inclui um aumento de 100 milhões de EUR que o presente regulamento propõe reafetar de outros objetivos estratégicos do Programa Europa Digital. Deste modo, o novo montante total disponível para ações de cibersegurança no âmbito do Programa Europa Digital ascenderá a 842,8 milhões de EUR.

Parte do montante adicional de 100 milhões de EUR reforçará o orçamento gerido pelo ECCC para executar ações em matéria de SOC e de preparação no âmbito do(s) seu(s) programa(s) de trabalho. Além disso, o financiamento adicional servirá para apoiar a criação da Reserva de Cibersegurança da UE.

Complementa o orçamento já previsto para ações semelhantes no programa de trabalho principal do Programa Europa Digital e do Programa para a Cibersegurança do período 2023-2027, o que poderá elevar o montante total para 551 milhões para o período 2023-2027, enquanto 115 milhões foram já afetados sob a forma de projetos-piloto para 2021-2022. Incluindo as contribuições dos Estados-Membros, o orçamento global poderá ascender a 1 109 milhões de EUR.

É disponibilizada uma panorâmica geral dos custos envolvidos na «ficha financeira legislativa» que acompanha a presente proposta.

## 5. OUTROS ELEMENTOS

### • Planos de execução e acompanhamento, avaliação e prestação de informações

A Comissão acompanhará a execução, a aplicação e a conformidade com as referidas novas disposições com vista a avaliar a sua eficácia. A Comissão apresenta um relatório sobre a avaliação e a revisão do presente regulamento ao Parlamento Europeu e ao Conselho no prazo de quatro anos a contar da data da sua aplicação.

### • Explicação pormenorizada das disposições específicas da proposta

Objetivos gerais, objeto e definições (capítulo I)

O capítulo I estabelece os objetivos do regulamento para reforçar a solidariedade a nível da União a fim de melhor detetar, preparar e responder a ameaças e incidentes de cibersegurança e, em especial, reforçar a deteção e o conhecimento da situação na União relativamente a ciberameaças e ciberincidentes, aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos na União e reforçar a solidariedade mediante o desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala e aumentar a resiliência da União mediante a análise e avaliação de incidentes significativos ou em grande escala. Este capítulo define igualmente as ações através das quais estes objetivos serão alcançados: a implantação de um ciberescudo europeu, a criação de um mecanismo de ciberemergência e o estabelecimento de um mecanismo de análise de incidentes de cibersegurança. Também estabelece as definições utilizadas no instrumento.

O ciberescudo europeu (capítulo II)

O capítulo II estabelece o ciberescudo europeu e enuncia os seus diversos elementos e as condições de participação. Em primeiro lugar, anuncia o objetivo geral do ciberescudo europeu, que consiste em desenvolver capacidades avançadas para a União detetar, analisar e tratar dados sobre ciberameaças e ciberincidentes na União, bem como os objetivos operacionais específicos. Especifica que o financiamento da União para o ciberescudo europeu deve ser executado em conformidade com o Regulamento Programa Europa Digital.

Além disso, o capítulo descreve o tipo de entidades que devem constituir o ciberescudo europeu. O escudo deve ser constituído pelos centros de operações de segurança nacionais («SOC nacionais») e pelos centros de operações de segurança transfronteiriços («SOC transfronteiriços»). Cada Estado-Membro participante designa um SOC nacional. O SOC designado servirá de ponto de referência e de acesso a outras organizações públicas e privadas a nível nacional para recolher e analisar informações sobre ameaças e incidentes de cibersegurança e contribuir para um SOC transfronteiriço. Na sequência de um convite à manifestação de interesse, o ECCC pode selecionar um SOC nacional para participar numa aquisição conjunta de ferramentas e infraestruturas, juntamente com o ECCC, e para receber uma subvenção para a utilização das ferramentas e infraestruturas. Se um SOC nacional beneficiar do apoio da União, compromete-se a candidatar-se a participar num SOC transfronteiriço no prazo de dois anos.

Os SOC transfronteiriços consistem num consórcio de, pelo menos, três Estados-Membros, representados por SOC nacionais, que se comprometem a trabalhar em conjunto para coordenar as suas atividades de ciberdeteção e de monitorização de ameaças. Na sequência de um convite inicial à manifestação de interesse, o ECCC pode selecionar um consórcio de acolhimento para participar numa aquisição conjunta de ferramentas e infraestruturas, juntamente com o ECCC, e para receber uma subvenção para a utilização das ferramentas e infraestruturas. Os membros do consórcio de acolhimento devem celebrar, por escrito, um acordo de consórcio que defina as suas disposições internas. Em seguida, este capítulo especifica os requisitos para a partilha de informações entre os participantes num SOC transfronteiriço e para a partilha de informações entre um SOC transfronteiriço e outros SOC transfronteiriços, bem como com as entidades pertinentes da UE. Os SOC nacionais que participem num SOC transfronteiriço devem partilhar entre si informações pertinentes relacionadas com ciberameaças, devendo os pormenores, incluindo o compromisso de partilhar uma quantidade significativa de dados e as respetivas condições, ser definidos num acordo de consórcio. Os SOC transfronteiriços devem assegurar um elevado nível de interoperabilidade entre si. Devem também celebrar acordos de cooperação com outros SOC transfronteiriços, especificando os princípios que orientam a partilha de informações. Caso obtenham informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, os SOC transfronteiriços devem fornecer informações pertinentes à UE-CyCLONe, à rede de CSIRT e à Comissão, tendo em conta as respetivas funções de gestão de crises, em conformidade com a Diretiva (UE) 2022/2555. No final do capítulo II são especificadas as condições de segurança para a participação no ciberescudo europeu.

Mecanismo de emergência em matéria de cibersegurança (capítulo III)

O capítulo III cria o mecanismo de ciberemergência para melhorar a resiliência da União a ameaças graves à cibersegurança e preparar e atenuar, num espírito de solidariedade, o impacto a curto prazo de incidentes ou crises de cibersegurança significativos e em grande escala. As ações de execução do mecanismo de ciberemergência são apoiadas por financiamento Programa Europa Digital. O mecanismo prevê ações de apoio à preparação, incluindo testes coordenados de entidades que operam em setores altamente críticos, resposta e recuperação imediata de incidentes de cibersegurança significativos ou em grande escala ou atenuação de ciberameaças significativas e ações de assistência mútua.

As ações de preparação do mecanismo de ciberemergência incluem testes coordenados de preparação de entidades que operam em setores altamente críticos. Após consulta da ENISA e do grupo de cooperação SRI, a Comissão deve identificar regularmente os setores ou subsetores pertinentes com base nos setores de importância crítica enumerados no anexo I da Diretiva (UE) 2022/2555, consoante os quais as entidades podem ser sujeitas a testes coordenados de preparação a nível da UE.

Para efeitos da execução das ações de resposta a incidentes propostas, o presente regulamento cria uma Reserva de Cibersegurança da UE, constituída por serviços de resposta a incidentes de prestadores de confiança selecionados em conformidade com os critérios estabelecidos no presente regulamento. Os utilizadores dos serviços da Reserva de Cibersegurança da UE devem incluir as autoridades dos Estados-Membros responsáveis pela gestão de cibercrises, as CSIRT e as instituições, órgãos e organismos da União. A Comissão deve assumir a responsabilidade geral pela execução da Reserva de Cibersegurança da UE e pode confiar, no todo ou em parte, o funcionamento e a administração da Reserva de Cibersegurança da UE à ENISA.

Para receberem apoio da Reserva de Cibersegurança da UE, os utilizadores devem tomar as suas próprias medidas para atenuar os efeitos do incidente para o qual o apoio é solicitado. Os pedidos de apoio da Reserva de Cibersegurança da UE devem incluir as informações pertinentes necessárias sobre o incidente e as medidas já tomadas pelos utilizadores. O capítulo descreve igualmente as modalidades de execução, incluindo a avaliação dos pedidos à Reserva de Cibersegurança da UE.

O regulamento prevê ainda os princípios de contratação pública e os critérios de seleção relativos aos prestadores de confiança da Reserva de Cibersegurança da UE.

Os países terceiros podem solicitar apoio da Reserva de Cibersegurança da UE sempre que os acordos de associação celebrados relativamente à sua participação no Programa Europa Digital o prevejam. Este capítulo descreve outras condições e as modalidades dessa participação.

Mecanismo de análise de incidentes de cibersegurança (capítulo IV)

A pedido da Comissão, da UE-CyCLONe ou da rede de CSIRT, a ENISA deve analisar e avaliar as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. A ENISA deve apresentar a análise e avaliação sob a forma de um relatório de análise de incidentes à rede de CSIRT, à UE-CyCLONe e à Comissão a fim de as apoiar no desempenho das suas funções. Se o incidente disser respeito a um país terceiro, a Comissão deve partilhar o relatório com o alto representante. O relatório deve incluir os ensinamentos retirados e, se for caso disso, recomendações para melhorar a postura da União no ciberespaço.

Disposições finais (capítulo V)

O capítulo V contém alterações do Regulamento Programa Europa Digital e uma obrigação que recai sobre a Comissão de elaborar relatórios periódicos de avaliação e reexame do regulamento, a apresentar ao Parlamento Europeu e ao Conselho. A Comissão está habilitada a adotar atos de execução em conformidade com o procedimento de exame a que se refere o artigo 21.º para: especificar as condições desta interoperabilidade entre os SOC transfronteiriços; determinar as modalidades processuais da partilha de informações relacionadas com um incidente de cibersegurança em grande escala, potencial ou em curso, entre os SOC transfronteiriços e as entidades da União; estabelecer requisitos técnicos que garantam um elevado nível de segurança física e de dados da infraestrutura e protejam os interesses de segurança da União aquando da partilha de informações com entidades que não sejam organismos públicos dos Estados-Membros; especificar os tipos e o número de serviços de resposta necessários para a Reserva de Cibersegurança da UE; e especificar mais pormenorizadamente as modalidades de atribuição dos serviços de apoio da Reserva de Cibersegurança da UE.

2023/0109 (COD)

Proposta de

# REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

## que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança

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 322.º, n.º 1, alínea a),

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Tribunal de Contas [1],

Tendo em conta o parecer do Comité Económico e Social Europeu [2],

Tendo em conta o parecer do Comité das Regiões [3],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) A utilização e a dependência de tecnologias da informação e comunicação tornaram-se características fundamentais de todos os setores de atividade económica, uma vez que as nossas administrações públicas, as nossas empresas e os nossos cidadãos nunca estiveram tão interligados e dependentes de outros setores e países.

(2) A magnitude, a frequência e o impacto dos incidentes de cibersegurança estão a aumentar, incluindo ataques de ciberespionagem, sequestro por programas maliciosos ou perturbação da cadeia de abastecimento. Os referidos incidentes constituem uma grave ameaça ao funcionamento dos sistemas de rede e informação. Tendo em conta a rápida evolução do cenário de ameaças, a ameaça de eventuais incidentes em grande escala que causem perturbações ou danos significativos às infraestruturas críticas exige uma maior preparação a todos os níveis do quadro de cibersegurança da União. Esta ameaça vai além da agressão militar da Rússia contra a Ucrânia e é provável que persista, dada a multiplicidade de intervenientes associados ao Estado, criminosos e ativistas háquer envolvidos nas atuais tensões geopolíticas. Tais incidentes podem impedir a prestação de serviços públicos e o exercício das atividades económicas, incluindo em setores críticos ou altamente críticos, gerar perdas financeiras importantes, minar a confiança dos utilizadores, causar graves prejuízos à economia da União e até ter consequências para a saúde ou ser potencialmente fatais. Além disso, os incidentes de cibersegurança são imprevisíveis, dado que, muitas vezes, surgem e evoluem em prazos muito curtos, não se confinam a uma área geográfica específica e ocorrem em simultâneo ou alastram-se imediatamente por vários países.

---

1 JO C […] de […], p. […].
2 JO C […] de […], p. […].
3 JO C […] de […], p. […].

(3) É necessário reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Tal como recomendado em três propostas diferentes da Conferência sobre o Futuro da Europa [4], é necessário aumentar a resiliência dos cidadãos, das empresas e das entidades que operam infraestruturas críticas contra as ameaças crescentes à cibersegurança, que podem ter impactos societais e económicos devastadores. Por conseguinte, é necessário investir em infraestruturas e serviços que apoiem uma deteção e uma resposta mais rápidas a ameaças e incidentes de cibersegurança, e os Estados-Membros necessitam de assistência para se prepararem melhor para incidentes de cibersegurança significativos e em grande escala, bem como para dar resposta aos mesmos. A União deve também aumentar as suas capacidades nestes domínios, nomeadamente no que diz respeito à recolha e análise de dados sobre ameaças e incidentes de cibersegurança.

(4) A União já tomou uma série de medidas para reduzir as vulnerabilidades e aumentar a resiliência das infraestruturas e entidades críticas contra os riscos de cibersegurança, nomeadamente a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho [5], a Recomendação (UE) 2017/1584 da Comissão [6], a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho [7] e o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho [8]. Além disso, a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas convida os Estados-Membros a tomarem medidas urgentes e eficazes, bem como a cooperarem leal e eficientemente, de forma solidária e coordenada, entre si, com a Comissão e com outras autoridades públicas competentes a fim de reforçar a resiliência das infraestruturas críticas utilizadas para prestar serviços essenciais no mercado interno.

(5) Os riscos de cibersegurança crescentes e um cenário de ameaças global complexo, com um claro risco de rápida disseminação dos ciberincidentes de um Estado-Membro para outro e de um país terceiro para a União, exigem uma solidariedade reforçada à escala da União para uma melhor deteção, preparação e resposta a ameaças e incidentes de cibersegurança. Os Estados-Membros também convidaram a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança nas Conclusões do Conselho sobre a postura da UE no ciberespaço [9].

---

4 https://futureu.europa.eu/pt.

5 Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (JO L 333 de 27.12.2022).

6 Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

7 Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, (JO L 218 de 14.8.2013, p. 8).

8 Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

9 Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, aprovadas pelo Conselho na sua reunião de 23 de maio de 2022 (9364/22).

(6) A Comunicação Conjunta sobre a política de ciberdefesa da UE [10], adotada em 10 de novembro de 2022, anunciava uma iniciativa da UE em matéria de cibersolidariedade com os seguintes objetivos: o reforço das capacidades comuns de deteção, conhecimento da situação e resposta da UE mediante a promoção da implantação de uma infraestrutura de centros de operações de segurança («SOC») na UE, o apoio à criação progressiva de uma reserva de cibersegurança a nível da UE com serviços de fornecedores privados de confiança e a avaliação das potenciais vulnerabilidades das entidades críticas com base em avaliações dos riscos da UE.

(7) É necessário reforçar a deteção e o conhecimento da situação relativamente a ciberameaças e ciberincidentes na União e intensificar a solidariedade, aumentando a preparação e as capacidades dos Estados-Membros e da União para dar resposta a incidentes de cibersegurança significativos e em grande escala. Por conseguinte, importa implantar uma infraestrutura pan-europeia de SOC (ciberescudo europeu) para criar e reforçar capacidades comuns de deteção e conhecimento da situação; criar um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala; e criar um mecanismo de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala específicos. As referidas ações não prejudicam os artigos 107.º e 108.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

(8) Para alcançar estes objetivos, é igualmente necessário alterar o Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho [11] em determinados domínios. Concretamente, o presente regulamento deve alterar o Regulamento (UE) 2021/694 no que respeita ao aditamento de novos objetivos operacionais relacionados com o ciberescudo europeu e o mecanismo de ciberemergência no âmbito do objetivo específico n.º 3 do Programa Europa Digital, que visa garantir a resiliência, a integridade e a fiabilidade do mercado único digital, reforçar as capacidades para monitorizar os ciberataques e as ameaças e dar resposta aos mesmos, bem como promover a cooperação transfronteiriça em matéria de cibersegurança. Devem ser estabelecidas as condições específicas em que poderá ser concedido apoio financeiro a essas ações e definidos os mecanismos de governação e coordenação necessários para alcançar os objetivos pretendidos. Outras alterações do Regulamento (UE) 2021/694 devem incluir descrições das ações propostas no âmbito dos novos objetivos operacionais, bem como indicadores mensuráveis para acompanhar a execução destes novos objetivos operacionais.

(9) O financiamento de ações ao abrigo do presente regulamento deve estar previsto no Regulamento (UE) 2021/694, que deve continuar a ser o ato de base que rege as ações consagradas no objetivo específico n.º 3 do Programa Europa Digital. Os programas de trabalho conexos estabelecerão condições específicas de participação para cada ação, em conformidade com as disposições aplicáveis do Regulamento (UE) 2021/694.

(10) São aplicáveis ao presente regulamento as regras financeiras horizontais adotadas pelo Parlamento Europeu e pelo Conselho com base no artigo 322.º do TFUE. Essas regras

---

[10] Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Política de ciberdefesa da UE» [JOIN(2022) 49 final].

[11] Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240 (JO L 166 de 11.5.2021, p. 1).

encontram-se enunciadas no Regulamento Financeiro e definem, nomeadamente, as modalidades relativas à elaboração e execução do orçamento da União, bem como o controlo da responsabilidade dos intervenientes financeiros. As regras adotadas com base no artigo 322.º do TFUE incluem igualmente um regime geral de condicionalidade para a proteção do orçamento da União como estabelecido no Regulamento (UE, Euratom) 2020/2092 do Parlamento Europeu e do Conselho.

(11) Para efeitos de boa gestão financeira, devem ser estabelecidas regras específicas para a transição de dotações de autorização e de pagamento não utilizadas. Respeitando o princípio de que o orçamento da União é fixado anualmente, o presente regulamento deve, devido à natureza imprevisível, excecional e específica do panorama da cibersegurança, prever possibilidades de transição de fundos não utilizados para além dos previstos no Regulamento Financeiro, maximizando assim a capacidade do mecanismo de emergência em matéria de cibersegurança para ajudar os Estados-Membros a lutar eficazmente contra as ciberameaças.

(12) Para prevenir, avaliar e responder de forma mais eficaz às ciberameaças e ciberincidentes, é necessário desenvolver um conhecimento mais aprofundado sobre as ameaças a ativos e infraestruturas críticos no território da União, incluindo a sua distribuição geográfica, interligação e potenciais efeitos em caso de ciberataques que afetem essas infraestruturas. Deve ser implantada uma infraestrutura de SOC de grande escala na União («ciberescudo europeu»), composta por várias plataformas transfronteiriças interoperáveis, cada uma agrupando vários SOC nacionais. Essa infraestrutura deve servir os interesses e necessidades nacionais e da União em matéria de cibersegurança, tirando partido de tecnologias de ponta para ferramentas avançadas de recolha e análise de dados, reforçando as capacidades de deteção e gestão da cibersegurança e proporcionando um conhecimento da situação em tempo real. Essa infraestrutura deve servir para aumentar a deteção de ameaças e incidentes de cibersegurança e, assim, complementar e apoiar as entidades e redes da União responsáveis pela gestão de crises na União, nomeadamente a Rede de Organizações de Coordenação de Cibercrises da UE («UE-CyCLONe»), tal como definida na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho [12].

(13) Cada Estado-Membro deve designar um organismo público a nível nacional encarregado de coordenar as atividades de deteção de ciberameaças nesse Estado-Membro. Estes SOC nacionais devem funcionar como ponto de referência e acesso a nível nacional para a participação no ciberescudo europeu e assegurar que as informações sobre ciberameaças provenientes de entidades públicas e privadas são partilhadas e recolhidas a nível nacional de forma eficaz e simplificada.

(14) No âmbito do ciberescudo europeu, devem ser criados vários centros de operações de cibersegurança transfronteiriços («SOC transfronteiriços»), que devem reunir os SOC nacionais de, pelo menos, três Estados-Membros para que os benefícios da deteção de ameaças transfronteiras e da partilha e gestão de informações possam ser plenamente alcançados. O objetivo geral dos SOC transfronteiriços deve ser o reforço das capacidades de análise, prevenção e deteção de ameaças à cibersegurança e o apoio à produção de informações de alta qualidade sobre ameaças à cibersegurança,

[12] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

nomeadamente através da partilha de dados de várias fontes, públicas ou privadas, bem como da partilha e utilização conjunta de ferramentas de ponta, e do desenvolvimento conjunto de capacidades de deteção, análise e prevenção num ambiente de confiança. Os SOC transfronteiriços devem proporcionar novas capacidades adicionais, tendo por base e complementando os SOC existentes, as equipas de resposta a incidentes informáticos («CSIRT») e outros intervenientes relevantes.

(15) A nível nacional, a monitorização, a deteção e a análise das ciberameaças são normalmente asseguradas pelos SOC de entidades públicas e privadas, em combinação com as CSIRT. Além disso, as CSIRT trocam informações no contexto da rede de CSIRT, em conformidade com a Diretiva (UE) 2022/2555. Os SOC transfronteiriços devem constituir uma nova capacidade complementar à rede de CSIRT mediante a mutualização e partilha de dados sobre ameaças à cibersegurança provenientes de entidades públicas e privadas, a valorização desses dados através de análises de peritos e de ferramentas de ponta e infraestruturas adquiridas conjuntamente, e o contributo para o desenvolvimento das capacidades e da soberania tecnológica da União.

(16) Os SOC transfronteiriços devem funcionar como um ponto central que permita uma ampla mutualização de dados pertinentes e informações sobre ciberameaças, possibilitar a divulgação de informações sobre ameaças entre um conjunto vasto e diversificado de intervenientes [por exemplo, equipas de resposta a emergências informáticas («CERT»), CSIRT, centros de partilha e análise de informações («ISAC») e operadores de infraestruturas críticas]. As informações trocadas entre os participantes num SOC transfronteiriço podem incluir dados de redes e sensores, fluxos de informações sobre ameaças, indicadores de exposição a riscos e informações contextualizadas sobre incidentes, ameaças e vulnerabilidades. Além disso, os SOC transfronteiriços devem também celebrar acordos de cooperação com outros SOC transfronteiriços.

(17) A partilha do conhecimento da situação entre as autoridades competentes é uma condição prévia indispensável para a preparação e coordenação a nível da União no que diz respeito a incidentes de cibersegurança significativos e em grande escala. A Diretiva (UE) 2022/2555 cria a UE-CyCLONe para apoiar a gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível operacional e para assegurar o intercâmbio regular de informações pertinentes entre os Estados-Membros e as instituições, órgãos e organismos da União. A Recomendação (UE) 2017/1584 sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala aborda o papel de todos os intervenientes relevantes. A Diretiva (UE) 2022/2555 recorda igualmente as responsabilidades da Comissão no âmbito do Mecanismo de Proteção Civil da União (MPCU), criado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, bem como no que se refere à apresentação de relatórios analíticos para o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR) ao abrigo da Decisão de Execução (UE) 2018/1993. Por conseguinte, nas situações em que os SOC transfronteiriços obtenham informações relacionadas com um incidente de cibersegurança em grande escala, potencial ou em curso, devem fornecer informações pertinentes à UE-CyCLONe, à rede de CSIRT e à Comissão. Concretamente, dependendo da situação, as informações a partilhar podem incluir informações técnicas, informações sobre a natureza e os motivos do agressor ou potencial agressor, bem como informações não técnicas de nível mais elevado sobre um incidente de cibersegurança em grande escala, potencial ou em curso. Neste

contexto, deve ser dada a devida atenção ao princípio da necessidade de conhecer e à natureza potencialmente sensível das informações partilhadas.

(18) As entidades que participam no ciberescudo europeu devem assegurar um nível elevado de interoperabilidade entre si, incluindo, se for caso disso, no que diz respeito aos formatos dos dados, à taxonomia, às ferramentas de tratamento e análise de dados e aos canais de comunicação seguros, a um nível mínimo de segurança da camada de aplicação, a um painel de controlo de conhecimento da situação e a indicadores. A adoção de uma taxonomia comum e a elaboração de um modelo de relatórios de situação para descrever a causa técnica e os impactos dos incidentes de cibersegurança devem ter em conta os trabalhos em curso sobre a notificação de incidentes no contexto da aplicação da Diretiva (UE) 2022/2555.

(19) A fim de permitir o intercâmbio de dados sobre ameaças à cibersegurança provenientes de várias fontes, em grande escala e num ambiente de confiança, as entidades que participam no ciberescudo europeu devem estar equipadas com ferramentas, equipamentos e infraestruturas de ponta e altamente seguros. Tal deverá permitir a melhoria das capacidades de deteção coletivas e alertas atempados às autoridades e entidades pertinentes, nomeadamente através da utilização das mais recentes tecnologias de inteligência artificial e de análise de dados.

(20) Ao recolher, partilhar e trocar dados, o ciberescudo europeu deverá reforçar a soberania tecnológica da União. A mutualização de dados selecionados de alta qualidade deverá também contribuir para o desenvolvimento de tecnologias avançadas de inteligência artificial e de análise de dados. A referida mutualização de dados deve ser facilitada através da ligação do ciberescudo europeu à infraestrutura pan-europeia de computação de alto desempenho criada pelo Regulamento (UE) 2021/1173 do Conselho [13].

(21) Embora o ciberescudo europeu seja um projeto de caráter civil, a comunidade de ciberdefesa poderá beneficiar do desenvolvimento de capacidades civis mais fortes de deteção e de conhecimento da situação para proteger as infraestruturas críticas da UE. Os SOC transfronteiriços, com o apoio da Comissão e do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança («ECCC»), e em cooperação com o alto representante da União para a Política Externa e a Política de Segurança («alto representante»), devem desenvolver progressivamente protocolos e normas específicos para permitir a cooperação com a comunidade de ciberdefesa, incluindo condições de investigação e de segurança. O desenvolvimento do ciberescudo europeu deve ser acompanhado de uma reflexão que permita uma futura colaboração com as redes e plataformas responsáveis pela partilha de informações na comunidade de ciberdefesa, em estreita cooperação com o alto representante.

(22) A partilha de informações entre os participantes no ciberescudo europeu deve cumprir os requisitos legais em vigor e, em especial, a legislação nacional e da União relativa à proteção de dados, bem como as regras da União em matéria de concorrência que regem o intercâmbio de informações. O destinatário das informações deve aplicar, na medida em que o tratamento de dados pessoais seja necessário, medidas técnicas e organizativas que salvaguardem os direitos e liberdades dos titulares dos dados,

[13] Regulamento (UE) 2021/1173 do Conselho, de 13 de julho de 2021, que cria a Empresa Comum para a Computação Europeia de Alto Desempenho e revoga o Regulamento (UE) 2018/1488 (JO L 256 de 19.7.2021, p. 3).

destruir os dados assim que deixem de ser necessários para a finalidade indicada e informar o organismo que disponibiliza os dados de que os mesmos foram destruídos.

(23) Sem prejuízo do artigo 346.º do TFUE, a troca de informações classificadas como confidenciais nos termos das regras da União ou de regras nacionais deve limitar-se ao que for pertinente e proporcionado em relação ao objetivo desse intercâmbio. Essa troca de informações deve ser conduzida de modo a preservar a confidencialidade das informações e a proteger a segurança e os interesses comerciais das entidades envolvidas, no pleno respeito dos segredos comerciais e de negócios.

(24) Tendo em conta o aumento dos riscos e do número de ciberincidentes que afetam os Estados-Membros, é necessário criar um instrumento de apoio a situações de crise para melhorar a resiliência da União a incidentes de cibersegurança significativos e em grande escala e complementar as ações dos Estados-Membros através de apoio financeiro de emergência para a preparação, resposta e recuperação imediata de serviços essenciais. Esse instrumento deve permitir a rápida mobilização da assistência em circunstâncias definidas e condições claras e permitir um acompanhamento e uma avaliação cuidados da forma como os recursos foram utilizados. Embora a principal responsabilidade pela prevenção, preparação e resposta a incidentes e crises de cibersegurança caiba aos Estados-Membros, o mecanismo de ciberemergência promove a solidariedade entre Estados-Membros, nos termos do artigo 3.º, n.º 3, do Tratado da União Europeia («TUE»).

(25) O mecanismo de ciberemergência deve prestar apoio aos Estados-Membros em complemento das suas próprias medidas e recursos, assim como de outras opções de apoio existentes para a resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala, tais como os serviços prestados pela Agência da União Europeia para a Cibersegurança (ENISA) em conformidade com o seu mandato, a resposta coordenada e a assistência da rede de CSIRT, o apoio à atenuação por parte da UE-CyCLONe, bem como a assistência mútua entre os Estados-Membros, nomeadamente no contexto do artigo 42.º, n.º 7, do TUE, das equipas de resposta rápida a ciberataques no âmbito da CEP [14] e das equipas de resposta rápida às ameaças híbridas. Deve atender à necessidade de assegurar a disponibilidade de meios especializados para apoiar a preparação e a resposta a incidentes de cibersegurança em toda a União e em países terceiros.

(26) O presente instrumento não prejudica os procedimentos e quadros de coordenação da resposta a situações de crise a nível da União, em especial o MPCU [15], o IPCR [16,] e a Diretiva (UE) 2022/2555. Pode contribuir para, ou complementar, ações executadas no contexto do artigo 42.º, n.º 7, do TUE ou nas situações definidas no artigo 222.º do TFUE. A utilização deste instrumento deve também ser coordenada com a aplicação das medidas do conjunto de instrumentos de ciberdiplomacia, se for caso disso.

(27) A assistência prestada ao abrigo do presente regulamento deve apoiar e complementar as ações empreendidas pelos Estados-Membros a nível nacional. Para o efeito, deve ser assegurada uma estreita cooperação e consulta entre a Comissão e o Estado-

---

14 DECISÃO (PESC) 2017/2315 DO CONSELHO, de 11 de dezembro de 2017, que estabelece uma cooperação estruturada permanente (CEP) e determina a lista de Estados- Membros participantes.

15 Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 347 de 20.12.2013, p. 924).

16 Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR) e em conformidade com a Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala.

Membro afetado. Ao solicitar apoio ao abrigo do mecanismo de ciberemergência, o Estado-Membro deve fornecer informações pertinentes que justifiquem a necessidade de apoio.

(28) A Diretiva (UE) 2022/2555 exige que os Estados-Membros designem ou criem uma ou mais autoridades de gestão de cibercrises e se certifiquem de que dispõem dos recursos adequados para desempenhar as suas funções de forma eficaz e eficiente. Exige igualmente que os Estados-Membros identifiquem as capacidades, os ativos e os procedimentos que podem ser utilizados em caso de crise, bem como que adotem um plano nacional de resposta a crises e incidentes de cibersegurança em grande escala que estabeleça os objetivos e as modalidades de gestão de crises e de incidentes de cibersegurança em grande escala. Os Estados-Membros são igualmente obrigados a criar uma ou várias CSIRT responsáveis pelo tratamento de incidentes de acordo com um processo bem definido e que abranja, pelo menos, os setores, subsetores e tipos de entidades incluídos no âmbito de aplicação da referida diretiva, bem como a assegurar que as mesmas dispõem dos recursos adequados para desempenharem eficazmente as suas funções. O presente regulamento não prejudica o papel da Comissão na garantia do cumprimento, pelos Estados-Membros, das obrigações decorrentes da Diretiva (UE) 2022/2555. O mecanismo de ciberemergência deve prestar assistência para ações destinadas a reforçar a preparação, bem como para ações de resposta a incidentes que visem atenuar o impacto dos incidentes de cibersegurança significativos e em grande escala, apoiar a recuperação imediata e/ou restabelecer o funcionamento dos serviços essenciais.

(29) No âmbito das ações de preparação, a fim de promover uma abordagem coerente e de reforçar a segurança em toda a União e o seu mercado interno, deve ser prestado apoio para testar e avaliar de forma coordenada a cibersegurança das entidades que operam nos setores altamente críticos identificados nos termos da Diretiva (UE) 2022/2555. Para o efeito, a Comissão, com o apoio da ENISA e em colaboração com o grupo de cooperação SRI criado pela Diretiva (UE) 2022/2555, deve identificar regularmente os setores ou subsetores pertinentes que devem ser elegíveis para receber apoio financeiro para a realização de testes coordenados a nível da União. Os setores ou subsetores devem ser selecionados do anexo I da Diretiva (UE) 2022/2555 («setores de importância crítica»). Os exercícios de teste coordenados devem basear-se em cenários e metodologias de risco comuns. A seleção dos setores e o desenvolvimento de cenários de risco devem ter em conta as avaliações dos riscos e os cenários de risco pertinentes à escala da União, incluindo a necessidade de evitar duplicações, como a avaliação dos riscos e os cenários de risco exigidos nas Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, a realizar pela Comissão, pelo alto representante e pelo grupo de cooperação SRI, em coordenação com os organismos e agências civis e militares competentes e com as redes estabelecidas, incluindo a UE-CyCLONe, bem como a avaliação do risco das redes e infraestruturas de comunicação solicitada pelo apelo ministerial conjunto de Nevers e realizada pelo grupo de cooperação SRI, com o apoio da Comissão e da ENISA, e em cooperação com o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE), as avaliações coordenadas dos riscos a realizar nos termos do artigo 22.º da Diretiva (UE) 2022/2555 e os testes de resiliência operacional digital

previstos no Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho [17]. A seleção dos setores deve também ter em conta a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas.

(30) Além disso, o mecanismo de ciberemergência deve prestar apoio a outras ações de preparação e apoiar a preparação noutros setores não abrangidos pelos testes coordenados de entidades que operam em setores altamente críticos. Essas ações poderão incluir vários tipos de atividades de preparação nacionais.

(31) O mecanismo de ciberemergência deve também prestar apoio a ações de resposta a incidentes para atenuar o impacto de incidentes de cibersegurança significativos e em grande escala, apoiar a recuperação imediata ou restabelecer o funcionamento dos serviços essenciais. Se for caso disso, deve complementar o MPCU, a fim de assegurar uma abordagem abrangente para dar resposta aos impactos dos ciberincidentes nos cidadãos.

(32) O mecanismo de ciberemergência deve apoiar a assistência prestada pelos Estados-Membros a um Estado-Membro afetado por um incidente de cibersegurança significativo ou em grande escala, incluindo pela rede de CSIRT estabelecida no artigo 15.º da Diretiva (UE) 2022/2555. Os Estados-Membros que prestam assistência devem ser autorizados a apresentar pedidos para cobrir os custos relacionados com o envio de equipas de peritos no quadro da assistência mútua. Os custos elegíveis podem incluir as despesas de viagem, alojamento e as ajudas de custo diárias dos peritos em cibersegurança.

(33) Deve ser criada progressivamente uma reserva de cibersegurança a nível da União, composta por prestadores privados de serviços de segurança geridos para apoiar ações de resposta e recuperação imediata em caso de incidentes de cibersegurança significativos ou em grande escala. A Reserva de Cibersegurança da UE deve assegurar a disponibilidade e prontidão dos serviços. Os serviços da Reserva de Cibersegurança da UE devem servir para apoiar as autoridades nacionais na prestação de assistência às entidades afetadas que operam em setores críticos ou altamente críticos em complemento das suas próprias ações a nível nacional. Ao solicitarem o apoio da Reserva de Cibersegurança da UE, os Estados-Membros devem especificar o apoio prestado à entidade afetada a nível nacional, que deve ser tido em conta na avaliação do pedido do Estado-Membro. Os serviços da Reserva de Cibersegurança da UE podem também servir para apoiar as instituições, órgãos e organismos da União em condições semelhantes.

(34) Para efeitos da seleção de prestadores de serviços privados para a prestação de serviços no contexto da Reserva de Cibersegurança da UE, importa estabelecer um conjunto de critérios mínimos que devem ser incluídos no convite à apresentação de propostas correspondente, a fim de assegurar que as necessidades das autoridades e entidades dos Estados-Membros que operam em setores críticos ou altamente críticos são satisfeitas.

(35) A fim de apoiar a criação da Reserva de Cibersegurança da UE, a Comissão poderá ponderar a possibilidade de solicitar à ENISA a preparação de um projeto de sistema

[17] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011.

de certificação nos termos do Regulamento (UE) 2019/881 para os serviços de segurança geridos nos domínios abrangidos pelo mecanismo de ciberemergência.

(36) A fim de apoiar os objetivos do presente regulamento de promover o conhecimento comum da situação, reforçar a resiliência da União e permitir uma resposta eficaz a incidentes de cibersegurança significativos e em grande escala, a UE-CyCLONe, a rede de CSIRT ou a Comissão devem poder solicitar à ENISA a análise e avaliação de ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA deve elaborar um relatório de análise de incidentes em colaboração com as partes interessadas pertinentes, incluindo representantes do setor privado, dos Estados-Membros, da Comissão e de outras instituições, órgãos e organismos competentes da UE. No que diz respeito ao setor privado, a ENISA está a desenvolver canais para o intercâmbio de informações com prestadores especializados, incluindo prestadores de soluções de segurança geridas e fornecedores, a fim de contribuir para a missão da ENISA de alcançar um elevado nível comum de cibersegurança na União. Com base na colaboração com as partes interessadas, incluindo o setor privado, o relatório de análise de incidentes específicos deve ter por objetivo avaliar as causas, os impactos e as medidas de atenuação de um incidente após a sua ocorrência. Deve ser prestada especial atenção aos contributos e ensinamentos partilhados pelos prestadores de serviços de segurança geridos que satisfaçam as condições de maior integridade profissional, imparcialidade e conhecimentos técnicos necessários, conforme exigido pelo presente regulamento. O relatório deve ser apresentado e contribuir para o trabalho da UE-CyCLONe, da rede de CSIRT e da Comissão. Se o incidente disser respeito a um país terceiro, será igualmente partilhado pela Comissão com o alto representante.

(37) Tendo em conta a natureza imprevisível dos ataques à cibersegurança e o facto de frequentemente não se confinarem a uma área geográfica específica e representarem um elevado risco de disseminação, o reforço da resiliência dos países vizinhos e da sua capacidade para responder eficazmente a incidentes de cibersegurança significativos em grande escala contribuem para a proteção da União no seu conjunto. Por conseguinte, os países terceiros associados ao Programa Europa Digital podem receber apoio da Reserva de Cibersegurança da UE sempre que tal esteja previsto no respetivo acordo de associação ao Programa Europa Digital. O financiamento dos países terceiros associados deve ser apoiado pela União no quadro de parcerias e instrumentos de financiamento pertinentes para esses países. O apoio deve abranger serviços no domínio da resposta a incidentes de cibersegurança significativos ou em grande escala e da recuperação imediata dos mesmos. Aquando da prestação de apoio aos países terceiros associados ao Programa Europa Digital, devem aplicar-se as condições estabelecidas no presente regulamento relativamente à Reserva de Cibersegurança da UE aos prestadores de confiança.

(38) A fim de assegurar condições uniformes para a execução do presente regulamento, devem ser atribuídas competências de execução à Comissão para especificar as condições de interoperabilidade entre os SOC transfronteiriços; determinar as modalidades processuais da partilha de informações relacionadas com um incidente de cibersegurança em grande escala, potencial ou em curso, entre os SOC transfronteiriços e as entidades da União; estabelecer requisitos técnicos para garantir a segurança do ciberescudo europeu; especificar os tipos e o número de serviços de resposta necessários para a Reserva de Cibersegurança da UE; e especificar mais pormenorizadamente as modalidades de atribuição dos serviços de apoio da Reserva

de Cibersegurança da UE. Essas competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho.

(39) O objetivo do presente regulamento pode ser mais bem alcançado ao nível da União do que ao nível dos Estados-Membros. Consequentemente, a União pode adotar medidas de acordo com os princípios da subsidiariedade e da proporcionalidade, consagrados no artigo 5.º do Tratado da União Europeia. O presente regulamento não excede o necessário para atingir esse objetivo,

ADOTARAM O PRESENTE REGULAMENTO:

## *Capítulo I*

## *OBJETIVOS GERAIS, OBJETO E DEFINIÇÕES*

### *Artigo 1.º*

### **Objeto e objetivos**

1. O presente regulamento estabelece medidas para reforçar as capacidades da União em matéria de deteção, preparação e resposta a ameaças e incidentes de cibersegurança, nomeadamente através das seguintes ações:

a) Implantação de uma infraestrutura pan-europeia de centros de operações de segurança («ciberescudo europeu») a fim de criar e reforçar capacidades comuns de deteção e conhecimento da situação;

b) Criação de um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala;

c) Criação de um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala.

2. O presente regulamento visa reforçar a solidariedade à escala da União através dos seguintes objetivos específicos:

a) Reforçar a deteção e o conhecimento da situação comuns a nível da União relativamente a ciberameaças e ciberincidentes, permitindo assim reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e contribuir para a soberania tecnológica da União no domínio da cibersegurança;

b) Aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos na União e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente mediante a disponibilização de apoio da União para resposta a incidentes de cibersegurança a países terceiros associados ao Programa Europa Digital;

c) Reforçar a resiliência da União e contribuir para uma resposta eficaz mediante a análise e avaliação de incidentes significativos ou em grande escala, inclusive retirando ensinamentos e, se for caso disso, formulando recomendações.

3. O presente regulamento não prejudica a responsabilidade que incumbe em primeiro lugar aos Estados-Membros em matéria de segurança nacional, segurança pública e prevenção, investigação, deteção e repressão de infrações penais.

*Artigo 2.º*

**Definições**

Para efeitos do presente regulamento, entende-se por:

(1) **«Centro de operações de segurança transfronteiriço» («SOC transfronteiriço»)**, uma plataforma plurinacional que reúne, numa estrutura de rede coordenada, SOC nacionais de, pelo menos, três Estados-Membros, que formam um consórcio de acolhimento, e que é concebida para prevenir ciberameaças e ciberincidentes e apoiar a produção de informações de alta qualidade, nomeadamente através do intercâmbio de dados de várias fontes, públicas e privadas, bem como através da partilha de ferramentas de ponta e do desenvolvimento conjunto de cibercapacidades de deteção, análise, prevenção e proteção num ambiente de confiança;

(2) **«Organismo público»**, um organismo de direito público na aceção do artigo 2.º, n.º 1, ponto 4, da Diretiva 2014/24/UE do Parlamento Europeu e do Conselho [18];

(3) **«Consórcio de acolhimento»**, um consórcio composto por Estados participantes, representados por SOC nacionais, que acordaram em criar e contribuir para a aquisição de ferramentas e infraestruturas e para o funcionamento de um SOC transfronteiriço;

(4) **«Entidade»**, uma entidade na aceção do artigo 6.º, ponto 38, da Diretiva (UE) 2022/2555;

(5) **«Entidades que operam em setores críticos ou altamente críticos»**, os tipos de entidades enumerados nos anexos I e II da Diretiva (UE) 2022/2555;

(6) **«Ciberameaça»**, uma ciberameaça na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/881;

(7) **«Incidente de cibersegurança significativo»**, um incidente de cibersegurança que preencha os critérios estabelecidos no artigo 23.º, n.º 3, da Diretiva (UE) 2022/2555;

(8) **«Incidente de cibersegurança em grande escala»**, um incidente na aceção do artigo 6.º, ponto 7, da Diretiva (UE) 2022/2555;

(9) **«Preparação»**, o estado de prontidão e a capacidade de assegurar uma resposta rápida e eficaz a um incidente de cibersegurança significativo ou em grande escala, obtido em resultado da avaliação do risco e das medidas de acompanhamento tomadas antecipadamente;

(10) **«Resposta»**, uma ação em caso de incidente de cibersegurança significativo ou em grande escala, ou durante ou após esse incidente, para fazer face às suas consequências adversas imediatas e a curto prazo;

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

(11) **«Prestadores de confiança»**, os prestadores de serviços de segurança geridos na aceção do artigo 6.º, ponto 40, da Diretiva (UE) 2022/2555, selecionados em conformidade com o artigo 16.º do presente regulamento.

## *Capítulo II*

## *O CIBERESCUDO EUROPEU*

### *Artigo 3.º*

### Criação do ciberescudo europeu

1. Deve ser criada uma infraestrutura pan-europeia interligada de centros de operações de segurança («ciberescudo europeu») a fim de desenvolver capacidades avançadas que permitam à União detetar, analisar e tratar dados sobre ciberameaças e ciberincidentes no seu território. A referida infraestrutura deve ser constituída por todos os centros de operações de segurança nacionais («SOC nacionais») e centros de operações de segurança transfronteiriços («SOC transfronteiriços»).

As ações de execução do ciberescudo europeu são apoiadas por financiamento do Programa Europa Digital e executadas em conformidade com o Regulamento (UE) 2021/694 e, em especial, com o objetivo específico n.º 3 do mesmo regulamento.

2. O ciberescudo europeu deve:

a) Mutualizar e partilhar dados sobre ciberameaças e ciberincidentes provenientes de várias fontes através dos SOC transfronteiriços;

b) Produzir informações de alta qualidade e utilizáveis e informações sobre ciberameaças através da utilização de ferramentas de ponta, nomeadamente tecnologias de inteligência artificial e de análise de dados;

c) Contribuir para uma melhor proteção e para uma melhor resposta às ciberameaças;

d) Contribuir para uma deteção mais rápida das ciberameaças e para o conhecimento da situação na União;

e) Prestar serviços e levar a cabo atividades para a comunidade de cibersegurança na União, nomeadamente contribuindo para o desenvolvimento de ferramentas avançadas de inteligência artificial e de análise de dados.

O ciberescudo europeu deve ser desenvolvido em cooperação com a infraestrutura pan-europeia de computação de alto desempenho estabelecida nos termos do Regulamento (UE) 2021/1173.

*Artigo 4.º*

**Centros de operações de segurança nacionais**

1. Para participar no ciberescudo europeu, cada Estado-Membro deve designar, pelo menos, um SOC nacional. O SOC nacional é um organismo público.

Tem capacidade para atuar como ponto de referência e de acesso a outras organizações públicas e privadas a nível nacional para recolher e analisar informações sobre ameaças e incidentes de cibersegurança e contribuir para um SOC transfronteiriço. Deve estar equipado com tecnologias de ponta capazes de detetar, agregar e analisar dados relevantes para as ameaças e incidentes de cibersegurança.

2. Na sequência de um convite à manifestação de interesse, os SOC nacionais são selecionados pelo Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança («ECCC») para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder subvenções aos SOC nacionais selecionados para financiar o funcionamento dessas ferramentas e infraestruturas. A contribuição financeira da União cobre até 50 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo Estado-Membro. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o SOC nacional devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.

3. Um SOC nacional selecionado nos termos do n.º 2 deve comprometer-se a candidatar-se a participar num SOC transfronteiriço no prazo de dois anos a contar da data de aquisição das ferramentas e infraestruturas, ou da data em que recebe financiamento através de subvenções, consoante o que ocorrer primeiro. Se, até essa data, um SOC nacional não participar num SOC transfronteiriço, não é elegível para apoio adicional da União ao abrigo do presente regulamento.

*Artigo 5.º*

**Centros de operações de segurança transfronteiriços**

1. Um consórcio de acolhimento composto por, pelo menos, três Estados-Membros, representados por SOC nacionais, empenhados em trabalhar em conjunto para coordenar as suas atividades de ciberdeteção e monitorização de ameaças, é elegível para participar em ações destinadas a estabelecer um SOC transfronteiriço.

2. Na sequência de um convite à manifestação de interesse, o ECCC seleciona um consórcio de acolhimento para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder ao consórcio de acolhimento uma subvenção para financiar o funcionamento das ferramentas e infraestruturas. A contribuição financeira da União cobre até 75 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo consórcio de acolhimento. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o consórcio de acolhimento devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.

3. Os membros do consórcio de acolhimento devem celebrar, por escrito, um acordo de consórcio que estabeleça as suas disposições internas para a execução da convenção de acolhimento e utilização.

4. Para efeitos jurídicos, um SOC transfronteiriço é representado por um SOC nacional que atue como coordenador, ou pelo consórcio de acolhimento, se este último tiver personalidade jurídica. O SOC coordenador é responsável pelo cumprimento dos requisitos da convenção de acolhimento e utilização e do presente regulamento.

*Artigo 6.º*

**Cooperação e partilha de informações entre os SOC transfronteiriços e no seio dos mesmos**

1. Os membros de um consórcio de acolhimento trocam entre si informações pertinentes no âmbito do SOC transfronteiriço, nomeadamente informações relacionadas com ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques, desde que tal partilha de informações:

a) Tenha como objetivo evitar, detetar, dar resposta e recuperar de incidentes ou atenuar o seu impacto;

b) Reforce o nível de cibersegurança, em especial ao sensibilizar para as ciberameaças, limitar ou impedir a sua capacidade de disseminação, apoiar um leque de capacidades defensivas, a correção e divulgação de vulnerabilidades, as técnicas de deteção, contenção e prevenção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação, ou promover a investigação colaborativa de ameaças entre entidades públicas e privadas.

2. O acordo de consórcio por escrito a que se refere o artigo 5.º, n.º 3, estabelece:

a) O compromisso de partilhar uma quantidade significativa de dados referidos no n.º 1, bem como as condições em que essas informações devem ser trocadas;

b) Um quadro de governação que incentive a partilha de informações por todos os participantes;

c) Metas de contribuição para o desenvolvimento de ferramentas avançadas de inteligência artificial e de análise de dados.

3. A fim de incentivar o intercâmbio de informações entre os SOC transfronteiriços, estes devem assegurar um elevado nível de interoperabilidade entre si. Para facilitar a interoperabilidade entre os SOC transfronteiriços, a Comissão pode, por meio de atos de execução, após consulta do ECCC, especificar as condições dessa interoperabilidade. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2, do presente regulamento.

4. Os SOC transfronteiriços devem celebrar acordos de cooperação entre si, especificando os princípios que orientam a partilha de informações entre as plataformas transfronteiriças.

*Artigo 7.º*

**Cooperação e partilha de informações com entidades da União**

1. Caso obtenham informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, os SOC transfronteiriços devem fornecer, sem demora injustificada, informações pertinentes à UE-CyCLONe, à rede de CSIRT e à Comissão, tendo em conta as respetivas funções de gestão de crises, em conformidade com a Diretiva (UE) 2022/2555.

2. A Comissão pode, por meio de atos de execução, estabelecer as modalidades processuais da partilha de informações prevista no n.º 1. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2, do presente regulamento.

*Artigo 8.º*

**Segurança**

1. Os Estados-Membros que participam no ciberescudo europeu devem garantir um elevado nível de segurança dos dados e de segurança física da infraestrutura do ciberescudo europeu e assegurar que a infraestrutura seja adequadamente gerida e controlada de forma a protegê-la de ameaças e a garantir a sua segurança e a segurança dos sistemas, incluindo a dos dados trocados através da infraestrutura.

2. Os Estados-Membros que participam no ciberescudo europeu devem assegurar que a partilha de informações no âmbito do ciberescudo europeu com entidades que não sejam organismos públicos dos Estados-Membros não afeta negativamente os interesses de segurança da União.

3. A Comissão pode adotar atos de execução que estabeleçam requisitos técnicos que os Estados-Membros devem respeitar para cumprir a obrigação que lhes incumbe por força dos n.os 1 e 2. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2, do presente regulamento. Ao fazê-lo, a Comissão, apoiada pelo alto representante, tem em conta as normas de segurança pertinentes a nível da defesa, a fim de facilitar a cooperação com intervenientes militares.

***Capítulo III***

***MECANISMO DE CIBEREMERGÊNCIA***

*Artigo 9.º*

**Criação do mecanismo de ciberemergência**

1. É criado um mecanismo de ciberemergência para melhorar a resiliência da União a ameaças graves à cibersegurança e para preparar e atenuar, num espírito de solidariedade, o impacto a curto prazo de incidentes de cibersegurança significativos e em grande escala («mecanismo»).

2. As ações de execução do mecanismo de ciberemergência são apoiadas por financiamento do Programa Europa Digital e executadas em conformidade com o Regulamento (UE) 2021/694 e, em especial, com o objetivo específico n.º 3 do mesmo regulamento.

*Artigo 10.º*

**Tipo de ações**

1. O mecanismo apoia os seguintes tipos de ações:

a) Ações de preparação, nomeadamente testes coordenados de preparação de entidades que operam em setores altamente críticos na União;

b) Ações de resposta, que apoiem a resposta e a recuperação imediata de incidentes de cibersegurança significativos e em grande escala, a fornecer por prestadores de confiança que participem na Reserva de Cibersegurança da UE criada nos termos do artigo 12.º;

c) Ações de assistência mútua que consistam na prestação de assistência por parte das autoridades nacionais de um Estado-Membro a outro Estado-Membro, em especial nos termos do artigo 11.º, n.º 3, alínea f), da Diretiva (UE) 2022/2555.

*Artigo 11.º*

**Testes coordenados de preparação das entidades**

1. A fim de apoiar os testes coordenados de preparação das entidades a que se refere o artigo 10.º, n.º 1, alínea a), na União, a Comissão, após consulta do grupo de cooperação SRI e da ENISA, deve identificar os setores ou subsetores em causa com base nos setores de importância crítica enumerados no anexo I da Diretiva (UE) 2022/2555, consoante os quais as entidades podem ser sujeitas aos testes coordenados de preparação, tendo em conta as avaliações coordenadas dos riscos e os testes de resiliência existentes e planeados a nível da União.

2. O grupo de cooperação SRI, em colaboração com a Comissão, a ENISA e o alto representante, deve desenvolver cenários e metodologias de risco comuns para os exercícios de teste coordenados.

*Artigo 12.º*

**Criação da Reserva de Cibersegurança da UE**

1. É criada uma Reserva de Cibersegurança da UE, a fim de ajudar os utilizadores a que se refere o n.º 3 a responder ou a prestar apoio para responder a incidentes de cibersegurança significativos ou em grande escala e para recuperar imediatamente desses incidentes.

2. A Reserva de Cibersegurança da UE é constituída por serviços de resposta a incidentes de prestadores de confiança selecionados de acordo com os critérios estabelecidos no artigo 16.º. A reserva inclui serviços previamente afetados. Os serviços devem poder ser disponibilizados em todos os Estados-Membros.

3. Os utilizadores dos serviços da Reserva de Cibersegurança da UE incluem:

a) Autoridades de gestão de cibercrises e CSIRT dos Estados-Membros a que se referem o artigo 9.º, n.os 1 e 2, e o artigo 10.º da Diretiva (UE) 2022/2555, respetivamente;

b) Instituições, órgãos e organismos da União.

4. Os utilizadores a que se refere o n.º 3, alínea a), devem utilizar os serviços da Reserva de Cibersegurança da UE a fim de responder ou prestar apoio para a resposta e a recuperação imediata de incidentes significativos ou em grande escala que afetem entidades que operam em setores críticos ou altamente críticos.

5. Incumbe à Comissão a responsabilidade global pela execução da Reserva de Cibersegurança da UE. A Comissão determina as prioridades e a evolução da Reserva de Cibersegurança da UE em consonância com os requisitos dos utilizadores referidos no n.º 3, supervisiona a sua execução e assegura a complementaridade, a coerência, as sinergias e as ligações com outras ações de apoio ao abrigo do presente regulamento, bem como com outras ações e programas da União.

6. A Comissão pode confiar o funcionamento e a administração da Reserva de Cibersegurança da UE, no todo ou em parte, à ENISA, através de acordos de contribuição.

7. A fim de apoiar a Comissão na criação da Reserva de Cibersegurança da UE, a ENISA prepara um levantamento dos serviços necessários, após consulta dos Estados-Membros e da Comissão. A ENISA prepara um levantamento semelhante, após consulta da Comissão, para identificar as necessidades dos países terceiros elegíveis para apoio da Reserva de Cibersegurança da UE, nos termos do artigo 17.º. Se for caso disso, a Comissão consulta o alto representante.

8. A Comissão pode, por meio de atos de execução, especificar os tipos e o número de serviços de resposta necessários para a Reserva de Cibersegurança da UE. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2.

*Artigo 13.º*

**Pedidos de apoio ao abrigo da Reserva de Cibersegurança da UE**

1. Os utilizadores a que se refere o artigo 12.º, n.º 3, podem solicitar serviços à Reserva de Cibersegurança da UE para apoiar a resposta e a recuperação imediata de incidentes de cibersegurança significativos ou em grande escala.

2. Para receberem apoio da Reserva de Cibersegurança da UE, os utilizadores a que se refere o artigo 12.º, n.º 3, devem tomar medidas para atenuar os efeitos do incidente para o qual o apoio é solicitado, incluindo a prestação de assistência técnica direta e outros recursos para apoiar a resposta ao incidente e os esforços de recuperação imediata.

3. Os pedidos de apoio dos utilizadores a que se refere o artigo 12.º, n.º 3, alínea a), do presente regulamento são transmitidos à Comissão e à ENISA através do ponto de contacto único designado ou criado pelo Estado-Membro em conformidade com o artigo 8.º, n.º 3, da Diretiva (UE) 2022/2555.

4. Os Estados-Membros informam a rede de CSIRT e, se for caso disso, a UE-CyCLONe dos seus pedidos de apoio para resposta a incidentes e recuperação imediata nos termos do presente artigo.

5. Os pedidos de apoio para resposta a incidentes e recuperação imediata devem incluir:

a) Informações adequadas sobre a entidade afetada, os potenciais impactos do incidente e a utilização prevista do apoio solicitado, incluindo uma indicação das necessidades estimadas;

b) Informações sobre as medidas tomadas para atenuar o incidente para o qual o apoio é solicitado, conforme referido no n.º 2;

c) Informações sobre outras formas de apoio à disposição da entidade afetada, incluindo disposições contratuais em vigor para a resposta a incidentes e serviços de recuperação imediata, bem como contratos de seguro que cubram potencialmente esse tipo de incidente.

6. A ENISA, em colaboração com a Comissão e o grupo de cooperação SRI, deve elaborar um modelo para facilitar a apresentação de pedidos de apoio ao abrigo da Reserva de Cibersegurança da UE.

7. A Comissão pode, por meio de atos de execução, especificar mais pormenorizadamente as modalidades de atribuição dos serviços de apoio da Reserva de Cibersegurança da UE. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2.

*Artigo 14.º*

**Execução do apoio da Reserva de Cibersegurança da UE**

1. Os pedidos de apoio da Reserva de Cibersegurança da UE são avaliados pela Comissão, com o apoio da ENISA ou conforme definido nos acordos de contribuição previstos no artigo 12.º, n.º 6, e a resposta é transmitida sem demora aos utilizadores a que se refere o artigo 12.º, n.º 3.

2. Para estabelecer uma ordem de prioridade para os pedidos, no caso de múltiplos pedidos simultâneos, devem ser tidos em conta, se for caso disso, os seguintes critérios:

a) A gravidade do incidente de cibersegurança;

b) O tipo de entidade afetada, dando maior prioridade aos incidentes que afetem entidades essenciais na aceção do artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555;

c) O potencial impacto no(s) Estado(s)-Membro(s) ou nos utilizadores afetados;

d) A potencial natureza transfronteiriça do incidente e o risco de disseminação para outros Estados-Membros ou utilizadores;

e) As medidas tomadas pelo utilizador para apoiar a resposta e os esforços de recuperação imediata, conforme referido no artigo 13.º, n.º 2, e no artigo 13.º, n.º 5, alínea b).

3. Os serviços da Reserva de Cibersegurança da UE são prestados em conformidade com acordos específicos entre o prestador de serviços e o utilizador ao qual é prestado apoio ao abrigo da Reserva de Cibersegurança da UE. Estes acordos incluem condições de responsabilidade.

4. Os acordos a que se refere o n.º 3 podem basear-se em modelos elaborados pela ENISA, após consulta dos Estados-Membros.

5. A Comissão e a ENISA não assumem qualquer responsabilidade contratual por danos causados a terceiros pelos serviços prestados no âmbito da execução da Reserva de Cibersegurança da UE.

6. No prazo de um mês a contar do termo da ação de apoio, os utilizadores apresentam à Comissão e à ENISA um relatório de síntese sobre o serviço prestado, os resultados obtidos e os ensinamentos retirados. Se o utilizador for de um país terceiro, conforme previsto no artigo 17.º, esse relatório deve ser partilhado com o alto representante.

7. A Comissão informa regularmente o grupo de cooperação SRI sobre a utilização e os resultados do apoio.

*Artigo 15.º*

**Coordenação com mecanismos de gestão de crises**

1. Nos casos em que incidentes de cibersegurança significativos ou em grande escala tenham origem ou resultem em catástrofes, na aceção da Decisão n.º 1313/2013/UE [19], o apoio prestado ao abrigo do presente regulamento para dar resposta a tais incidentes complementa as ações previstas na referida decisão, sem prejuízo da mesma.

2. Em caso de incidente de cibersegurança transfronteiriço em grande escala em que seja acionado o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR), o apoio prestado ao abrigo do presente regulamento para dar resposta a esse incidente é tratado em conformidade com os protocolos e procedimentos aplicáveis do IPCR.

3. Em consulta com o alto representante, o apoio prestado no âmbito do mecanismo de ciberemergência pode complementar a assistência prestada no contexto da política externa e de segurança comum e da política comum de segurança e defesa, nomeadamente através das equipas de resposta rápida a ciberataques. Pode igualmente complementar ou contribuir para a assistência prestada por um Estado-Membro a outro Estado-Membro no contexto do artigo 42.º, n.º 7, do Tratado da União Europeia.

4. O apoio prestado ao abrigo do mecanismo de ciberemergência pode fazer parte da resposta conjunta da União e dos Estados-Membros nas situações referidas no artigo 222.º do Tratado sobre o Funcionamento da União Europeia.

*Artigo 16.º*

**Prestadores de confiança**

1. Nos procedimentos de contratação pública para efeitos da criação da Reserva de Cibersegurança da UE, a entidade adjudicante age em conformidade com os princípios estabelecidos no Regulamento (UE, Euratom) 2018/1046 e com os seguintes princípios:

a) Assegurar que a Reserva de Cibersegurança da UE inclui serviços que podem ser disponibilizados em todos os Estados-Membros, tendo em conta, em especial, os

[19] Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 347 de 20.12.2013, p. 924).

requisitos nacionais para a prestação desses serviços, incluindo a certificação ou a acreditação;

b) Assegurar a proteção dos interesses essenciais de segurança da União e dos seus Estados-Membros;

c) Assegurar que a Reserva de Cibersegurança da UE proporciona valor acrescentado da UE, contribuindo para a consecução dos objetivos estabelecidos no artigo 3.º do Regulamento (UE) 2021/694, incluindo a promoção do desenvolvimento de competências em matéria de cibersegurança na UE.

2. Ao adjudicar serviços para a Reserva de Cibersegurança da UE, a entidade adjudicante deve incluir nos documentos do concurso os seguintes critérios de seleção:

a) O prestador deve demonstrar que o seu pessoal possui o mais elevado grau de integridade profissional, independência, responsabilidade e a competência técnica necessária para realizar as atividades no seu domínio específico, e assegura a permanência/continuidade dos conhecimentos especializados, bem como os recursos técnicos necessários;

b) O prestador, as suas filiais e subcontratantes devem dispor de um quadro para proteger as informações sensíveis relacionadas com o serviço, nomeadamente elementos de prova, conclusões e relatórios, que seja conforme com as regras de segurança da União em matéria de proteção das informações classificadas da UE;

c) O prestador deve fornecer provas suficientes de que a sua estrutura de governação é transparente, não suscetível de comprometer a sua imparcialidade e a qualidade dos seus serviços ou de causar conflitos de interesses;

d) O prestador deve dispor de uma credenciação de segurança adequada, pelo menos para o pessoal destinado à disponibilização dos serviços;

e) O prestador deve ter o nível de segurança pertinente para os seus sistemas informáticos;

f) O prestador deve estar equipado com o equipamento técnico de *hardware* e *software* necessário para apoiar o serviço solicitado;

g) O prestador deve ser capaz de demonstrar que possui experiência na prestação de serviços semelhantes às autoridades nacionais competentes ou às entidades que operam em setores críticos ou altamente críticos;

h) O prestador deve ser capaz de prestar o serviço num curto espaço de tempo no(s) Estado(s)-Membro(s) onde pode prestar o serviço;

i) O prestador deve ser capaz de prestar o serviço na língua local do(s) Estado(s)-Membro(s) onde pode prestar o serviço;

j) Quando estiver em vigor um sistema de certificação da UE para os serviços de segurança geridos [Regulamento (UE) 2019/881], o prestador deve obter certificação em conformidade com esse sistema.

*Artigo 17.º*

**Apoio a países terceiros**

1. Os países terceiros podem solicitar apoio da Reserva de Cibersegurança da UE sempre que os acordos de associação celebrados relativamente à sua participação no Programa Europa Digital o prevejam.

2. O apoio da Reserva de Cibersegurança da UE deve estar em conformidade com o presente regulamento e cumprir quaisquer condições específicas estabelecidas nos acordos de associação a que se refere o n.º 1.

3. Os utilizadores de países terceiros associados elegíveis para beneficiar de serviços da Reserva de Cibersegurança da UE incluem autoridades competentes como as CSIRT e as autoridades de gestão de cibercrises.

4. Cada país terceiro elegível para apoio da Reserva de Cibersegurança da UE designa uma autoridade para atuar como ponto de contacto único para efeitos do presente regulamento.

5. Antes de receberem qualquer apoio da Reserva de Cibersegurança da UE, os países terceiros devem fornecer à Comissão e ao alto representante informações sobre a sua ciber-resiliência e as suas capacidades de gestão de riscos, incluindo, pelo menos, informações sobre as medidas nacionais tomadas para se prepararem para incidentes de cibersegurança significativos ou em grande escala, bem como informações sobre as entidades nacionais responsáveis, incluindo as CSIRT ou entidades equivalentes, as suas capacidades e os recursos que lhes são afetados. Sempre que as disposições dos artigos 13.º e 14.º do presente regulamento façam referência aos Estados-Membros, aplicam-se aos países terceiros, conforme enunciado no n.º 1.

6. A Comissão coordena com o alto representante os pedidos recebidos e a execução do apoio concedido a países terceiros ao abrigo da Reserva de Cibersegurança da UE.

## *Capítulo IV*

## *MECANISMO DE ANÁLISE DE INCIDENTES DE CIBERSEGURANÇA*

*Artigo 18.º*

**Mecanismo de análise de incidentes de cibersegurança**

1. A pedido da Comissão, da UE-CyCLONe ou da rede de CSIRT, a ENISA analisa e avalia as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA apresenta um relatório de análise do incidente à rede de CSIRT, à UE-CyCLONe e à Comissão, a fim de as apoiar no desempenho das suas funções, em especial tendo em conta as enunciadas nos artigos 15.º e 16.º da Diretiva (UE) 2022/2555. Se for caso disso, a Comissão partilha o relatório com o alto representante.

2. Para elaborar o relatório de análise do incidente referido no n.º 1, a ENISA colabora com todas as partes interessadas pertinentes, incluindo representantes dos Estados-Membros, a Comissão, outras instituições, órgãos e organismos competentes da UE, prestadores de serviços de segurança geridos e utilizadores de serviços de cibersegurança. Se for caso disso, a ENISA colabora igualmente com as entidades afetadas por incidentes de cibersegurança

significativos ou em grande escala. Para apoiar a análise, a ENISA pode também consultar outros tipos de partes interessadas. Os representantes consultados devem divulgar qualquer potencial conflito de interesses.

3. O relatório inclui uma revisão e análise do incidente de cibersegurança significativo ou em grande escala específico, incluindo as principais causas, vulnerabilidades e ensinamentos retirados. O relatório deve proteger as informações confidenciais, nos termos do direito da União ou do direito nacional relativo à proteção de informações sensíveis ou classificadas.

4. Se for caso disso, o relatório formula recomendações para melhorar a postura da União no ciberespaço.

5. Sempre que possível, é disponibilizada ao público uma versão do relatório. Essa versão deve incluir apenas informação pública.

## *Capítulo V*

## *DISPOSIÇÕES FINAIS*

### *Artigo 19.º*

### **Alterações do Regulamento (UE) 2021/694**

O Regulamento (UE) 2021/694 é alterado do seguinte modo:

(1) O artigo 6.º é alterado do seguinte modo:

a) O n.º 1 é alterado do seguinte modo:

(1) É inserida a seguinte alínea a-A):

«a-A) Apoiar o desenvolvimento de um ciberescudo da UE, incluindo o desenvolvimento, a implantação e o funcionamento de plataformas de centros de operações de segurança (SOC, do inglês *Security Operations Centres*) nacionais e transfronteiriços que contribuam para o conhecimento da situação na União e para o reforço das capacidades da União em matéria de informações sobre ciberameaças;»;

(2) É aditada a seguinte alínea g):

«g) Criar e operar um mecanismo de ciberemergência para apoiar os Estados-Membros na preparação e resposta a incidentes significativos de cibersegurança, em complemento dos recursos e capacidades nacionais e de outras formas de apoio disponíveis a nível da União, incluindo a criação de uma Reserva de Cibersegurança da UE.»;

a) O n.º 2 passa a ter a seguinte redação:

«2. As medidas tomadas no âmbito do objetivo específico n.º 3 são executadas principalmente através do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC) e da Rede de Centros Nacionais de Coordenação, nos termos do Regulamento (UE) 2021/887 do Parlamento Europeu e do

Conselho [20], com exceção das medidas que executam a Reserva de Cibersegurança da UE, que são executadas pela Comissão e pela ENISA.»;

(2) O artigo 9.º é alterado do seguinte modo:

a) No n.º 2, as alíneas b), c) e d) passam a ter a seguinte redação:

«b) 1 776 956 000 EUR para o objetivo específico n.º 2, Inteligência artificial;

c) 1 629 566 000 EUR para o objetivo específico n.º 3, Cibersegurança e confiança;

d) 482 347 000 EUR para o objetivo específico n.º 4, Competências digitais avançadas;»;

b) É aditado o n.º 8 com a seguinte redação:

«8. Em derrogação do artigo 12.º, n.º 4, do Regulamento (UE, Euratom) 2018/1046, as dotações de autorização e de pagamento não utilizadas para ações que visem a consecução dos objetivos estabelecidos no artigo 6.º, n.º 1, alínea g), do presente regulamento transitam automaticamente e podem ser autorizadas e pagas até 31 de dezembro do exercício seguinte.»;

(3) No artigo 14.º, o n.º 2 passa a ter a seguinte redação:

«2. O Programa pode conceder financiamento sob qualquer uma das formas previstas no Regulamento Financeiro, em especial por via de contratos públicos ou por via de subvenções e prémios.

Caso a concretização de um objetivo da ação exija a contratação de bens e serviços inovadores, as subvenções apenas podem ser atribuídas a beneficiários que sejam autoridades adjudicantes ou entidades adjudicantes na aceção das Diretivas 2014/24/UE [(27)] e 2014/25/UE [(28)] do Parlamento Europeu e do Conselho.

Caso seja necessário o fornecimento de bens e serviços inovadores que ainda não estão comercialmente disponíveis em grande escala para a concretização dos objetivos da ação, a autoridade ou a entidade adjudicante podem autorizar a adjudicação de diversos contratos no âmbito do mesmo procedimento de contratação pública.

Nos casos devidamente justificados de segurança pública, a autoridade ou a entidade adjudicante podem estabelecer que o local de execução do contrato se situe no território da União.

Ao executarem os procedimentos de contratação pública relativos à Reserva de Cibersegurança da UE criada pelo artigo 12.º do Regulamento (UE) 2023/XX, a

[20] Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação (JO L 202 de 8.6.2021, p. 1).

Comissão e a ENISA podem atuar como central de compras para efetuar aquisições por conta ou em nome de países terceiros associados ao Programa, em conformidade com o artigo 10.º. A Comissão e a ENISA podem também agir na qualidade de grossistas, adquirindo, armazenando e revendendo ou doando fornecimentos e serviços, incluindo de arrendamento/aluguer, a esses países terceiros. Em derrogação do artigo 169.º, n.º 3, do Regulamento (UE) XXX/XXXX [RF reformulação], o pedido de um único país terceiro é suficiente para mandatar a Comissão ou a ENISA para agir.

Ao executarem procedimentos de contratação pública para a Reserva de Cibersegurança da UE criada pelo artigo 12.º do Regulamento (UE) 2023/XX, a Comissão e a ENISA podem atuar como central de compras para efetuar aquisições por conta ou em nome de instituições, órgãos e organismos da União. A Comissão e a ENISA podem também agir na qualidade de grossistas, adquirindo, armazenando e revendendo ou doando fornecimentos e serviços, incluindo de arrendamento/aluguer, a instituições, órgãos e organismos da União. Em derrogação do artigo 169.º, n.º 3, do Regulamento (UE) XXX/XXXX [RF reformulação], o pedido de uma única instituição, órgão ou organismo da União é suficiente para mandatar a Comissão ou a ENISA para agir.

O Programa pode também prestar o financiamento sob a forma de instrumentos financeiros no âmbito de operações de financiamento misto.»;

(4) É aditado o seguinte artigo 16.º-A:

«No caso das ações de execução do ciberescudo europeu criado pelo artigo 3.º do Regulamento (UE) 2023/XX, as regras aplicáveis são as estabelecidas nos artigos 4.º e 5.º do Regulamento (UE) 2023/XX. Em caso de conflito entre as disposições do presente regulamento e as dos artigos 4.º e 5.º do Regulamento (UE) 2023/ XX, estas últimas prevalecem, aplicando-se a essas ações específicas.»;

(5) O artigo 19.º passa a ter a seguinte redação:

«As subvenções ao abrigo do Programa são concedidas e geridas de acordo com o título VIII do Regulamento Financeiro e podem cobrir até 100 % dos custos elegíveis, sem prejuízo do princípio do cofinanciamento estabelecido no artigo 190.º do Regulamento Financeiro. Tais subvenções são concedidas e geridas tal como especificado para cada objetivo específico.

O ECCC pode conceder apoio sob a forma de subvenções diretamente, sem convite à apresentação de propostas, aos SOC nacionais a que se refere o artigo 4.º do Regulamento XXXX e ao consórcio de acolhimento a que se refere o artigo 5.º do Regulamento XXXX, em conformidade com o artigo 195.º, n.º 1, alínea d), do Regulamento Financeiro.

O ECCC pode conceder apoio sob a forma de subvenções para o mecanismo de ciberemergência enunciado no artigo 10.º do Regulamento XXXX diretamente aos

Estados-Membros, sem convite à apresentação de propostas, em conformidade com o artigo 195.º, n.º 1, alínea d), do Regulamento Financeiro.

Para as ações especificadas no artigo 10.º, n.º 1, alínea c), do Regulamento 202X/XXXX, o ECCC deve informar a Comissão e a ENISA sobre os pedidos de subvenções diretas apresentados pelos Estados-Membros sem convite à apresentação de propostas.

Para apoiar a assistência mútua em resposta a um incidente de cibersegurança significativo ou em grande escala, tal como definido no artigo 10.º, alínea c), do Regulamento XXXX, e em conformidade com o artigo 193.º, n.º 2, segundo parágrafo, alínea a), do Regulamento Financeiro, em casos devidamente justificados, os custos podem ser considerados elegíveis ainda que tenham sido incorridos antes da apresentação do pedido de subvenção.»;

(6) Os anexos I e II são alterados em conformidade com o anexo do presente regulamento.

*Artigo 20.º*

**Avaliação**

Até [quatro anos após a data de aplicação do presente regulamento], a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão do presente regulamento.

*Artigo 21.º*

**Procedimento de comité**

1. A Comissão é assistida pelo Comité de Coordenação do Programa Europa Digital criado pelo Regulamento (UE) 2021/694. O referido comité é um comité na aceção do Regulamento (UE) n.º 182/2011.
2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

*Artigo 22.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 Estrasburgo, em

| | |
|---|---|
| *Pelo Parlamento Europeu* | *Pelo Conselho* |
| *A Presidente* | *O Presidente* |

# FICHA FINANCEIRA LEGISLATIVA

## 1. CONTEXTO DA PROPOSTA/INICIATIVA

### 1.1. Denominação da proposta/iniciativa

### 1.2. Domínio(s) de intervenção abrangidos

### 1.3. A proposta/iniciativa refere-se:

### 1.4. Objetivo(s)

*1.4.1. Objetivo(s) geral(ais)*

*1.4.2. Objetivo(s) específico(s)*

*1.4.3. Resultados e impacto esperados*

*1.4.4. Indicadores de desempenho*

### 1.5. Justificação da proposta/iniciativa

*1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa*

*1.5.2. Valor acrescentado da intervenção da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.*

*1.5.3. Ensinamentos retirados de experiências anteriores semelhantes*

*1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados*

*1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação*

### 1.6. Duração e impacto financeiro da proposta/iniciativa

### 1.7. Métodos de execução orçamental previstos

## 2. MEDIDAS DE GESTÃO

### 2.1. Disposições em matéria de acompanhamento e prestação de informações

### 2.2. Sistema(s) de gestão e de controlo

*2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos*

*2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar*

*2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo ÷ valor dos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)*

### 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(ais) de despesas envolvida(s)

### 3.2. Impacto financeiro estimado da proposta nas dotações

*3.2.1. Síntese do impacto estimado nas dotações operacionais*

*3.2.2. Estimativa das realizações financiadas com dotações operacionais*

*3.2.3. Síntese do impacto estimado nas dotações administrativas*

*3.2.3.1. Necessidades estimadas de recursos humanos*

*3.2.4. Compatibilidade com o atual quadro financeiro plurianual*

*3.2.5. Participação de terceiros no financiamento*

### 3.3. Impacto estimado nas receitas

## 1. CONTEXTO DA PROPOSTA/INICIATIVA

### 1.1. Denominação da proposta/iniciativa

Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança

### 1.2. Domínio(s) de intervenção abrangidos

Uma Europa Preparada para a Era Digital

Investimentos Estratégicos Europeus

Atividade: construir o futuro digital da Europa

### 1.3. A proposta/iniciativa refere-se:

☒ **a uma nova ação**

☐ **a uma nova ação na sequência de um projeto-piloto/ação preparatória** [33]

☐ **à prorrogação de uma ação existente**

☐ **à fusão ou reorientação de uma ou mais ações para outra/uma nova ação**

### 1.4. Objetivo(s)

*1.4.1. Objetivo(s) geral(ais)*

O Regulamento Cibersolidariedade reforçará a solidariedade à escala da União a fim de melhor detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança. Tem por objetivo:

a) Reforçar a deteção e o conhecimento da situação comuns a nível da UE relativamente a ciberameaças e ciberincidentes;

b) Aumentar o grau de preparação das entidades críticas em toda a UE e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente ao disponibilizar apoio à resposta a incidentes a países terceiros associados ao Programa Europa Digital;

c) Reforçar a resiliência da União e contribuir para uma resposta eficaz mediante a análise e avaliação de incidentes significativos ou em grande escala, inclusive retirando ensinamentos e, se for caso disso, formulando recomendações.

*1.4.2. Objetivo(s) específico(s)*

O Regulamento Cibersolidariedade concretizará o conjunto de objetivos através das seguintes medidas:

[33] Tal como referido no artigo 58.º, n.º 2, alínea a) ou b), do Regulamento Financeiro.

a) Implantação de uma infraestrutura pan-europeia de centros de operações de segurança («ciberescudo europeu») a fim de criar e reforçar capacidades comuns de deteção e conhecimento da situação;

b) Criação de um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala. O apoio à resposta a incidentes deve também ser disponibilizado às instituições, órgãos e organismos da União.

Estas ações serão apoiadas por financiamento do Programa Europa Digital, que o presente instrumento legislativo alterará a fim de estabelecer as ações supracitadas, prever apoio financeiro para o seu desenvolvimento e clarificar as condições para beneficiar do apoio financeiro;

c) Criação de um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala.

### *1.4.3. Resultados e impacto esperados*

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

A proposta gerará vantagens significativas para as várias partes interessadas. O ciberescudo europeu melhorará as capacidades de deteção de ciberameaças dos Estados-Membros. O mecanismo de ciberemergência complementará as ações dos Estados-Membros através do apoio de emergência para a preparação, resposta e recuperação imediata/restabelecimento do funcionamento dos serviços essenciais.

Estas ações reforçarão a posição competitiva da indústria e das empresas europeias na economia digital e apoiarão a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Concretamente, a proposta visa aumentar a resiliência dos cidadãos, das empresas e das entidades que operam em setores críticos ou altamente críticos às crescentes ameaças à cibersegurança, que podem ter impactos societais e económicos devastadores. Para tal, investirá em instrumentos que apoiem uma deteção e uma resposta mais rápidas às ameaças e incidentes de cibersegurança, e ajudará os Estados-Membros a prepararem-se melhor e a responderem a incidentes de cibersegurança significativos e em grande escala. Estas ações deverão também apoiar o reforço das capacidades da Europa nestes domínios, nomeadamente no que diz respeito à recolha e análise de dados sobre ameaças e incidentes de cibersegurança.

### *1.4.4. Indicadores de desempenho*

*Especificar os indicadores que permitem acompanhar os progressos e os resultados.*

A fim de promover a solidariedade à escala da União, podem ser tidos em conta vários indicadores:

1) O número de infraestruturas ou ferramentas de cibersegurança, ou ambas, adquiridas conjuntamente;

2) O número de ações de apoio à preparação e resposta a incidentes de cibersegurança no âmbito do mecanismo de ciberemergência.

## 1.5. Justificação da proposta/iniciativa

*1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa*

| |
|---|
| O regulamento deve ser aplicável na íntegra pouco tempo depois da sua adoção, isto é, no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*. |

*1.5.2. Valor acrescentado da intervenção da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.*

A natureza marcadamente transfronteiriça das ameaças de cibersegurança em geral e o número crescente de riscos e incidentes com repercussões além-fronteiras e entre setores e produtos significam que os objetivos da presente intervenção não podem ser eficazmente alcançados pelos Estados-Membros de forma isolada e exigem uma ação comum e solidariedade à escala da União. A experiência no combate a ciberameaças decorrente da guerra contra a Ucrânia, juntamente com os ensinamentos retirados de um exercício de cibersegurança realizado durante a Presidência francesa (EU CyCLES), demonstrou que devem ser criados mecanismos concretos de apoio mútuo, incluindo a cooperação com o setor privado, para alcançar a solidariedade à escala da UE. Perante este cenário, as Conclusões do Conselho, de 23 de maio de 2022, sobre o desenvolvimento da postura da União Europeia no ciberespaço convidam a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança. O apoio e as ações a nível da União que visam uma melhor deteção das ameaças à cibersegurança e um aumento das capacidades de preparação e resposta proporcionam valor acrescentado, uma vez que evitam a duplicação de esforços em toda a União e nos Estados-Membros, conduzindo a uma melhor exploração dos ativos existentes e a uma maior coordenação e intercâmbio de informações sobre os ensinamentos retirados.

*1.5.3. Ensinamentos retirados de experiências anteriores semelhantes*

| |
|---|
| No que diz respeito ao conhecimento da situação e à deteção no âmbito do ciberescudo europeu, foram lançados, ao abrigo do programa de trabalho em matéria de cibersegurança do Programa Europa Digital para 2021-2022, um convite à manifestação de interesse para a aquisição conjunta de ferramentas e infraestruturas para a criação de SOC transfronteiriços, e um convite à apresentação de propostas para a concessão de subvenções para permitir o reforço das capacidades dos SOC ao serviço de organizações públicas e privadas. |

No que diz respeito à preparação e à resposta a incidentes, a Comissão criou um programa de curto prazo para apoiar os Estados-Membros, mediante a afetação de financiamento adicional à ENISA, a fim de reforçar a título imediato a preparação e as capacidades de resposta a ciberincidentes graves. Os serviços abrangidos incluem ações de preparação, como testes de penetração de entidades críticas para identificar vulnerabilidades. O programa reforça igualmente as possibilidades de assistência aos Estados-Membros em caso de incidentes graves que afetem entidades críticas. A execução deste programa de curto prazo pela ENISA está em curso e já forneceu

informações valiosas, que foram tidas em conta na preparação do presente regulamento.

*1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados*

O Regulamento Cibersolidariedade basear-se-á nas ações atualmente apoiadas pela União e pelos Estados-Membros para melhorar o conhecimento da situação e a deteção de ciberameaças, bem como para dar resposta a incidentes de cibersegurança em grande escala e transfronteiriços. Além disso, o instrumento é coerente com outros quadros de gestão de crises, nomeadamente o IPCR, a política comum de segurança e defesa, incluindo as equipas de resposta rápida a ciberataques, e a assistência prestada por um Estado-Membro a outro no contexto do artigo 42.º, n.º 7, do Tratado da União Europeia. A nova proposta também complementará e apoiará as estruturas desenvolvidas no âmbito de outros instrumentos de cibersegurança, como a Diretiva (UE) 2022/2555 (Diretiva SRI 2) ou o Regulamento (UE) 2019/881 (Regulamento Cibersegurança).

*1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação*

A gestão dos domínios de ação atribuídos à ENISA enquadra-se no seu atual mandato e atribuições gerais. Estes domínios de ação podem exigir perfis específicos ou novas atribuições, mas estes podem ser absorvidos pelos recursos existentes da ENISA e colmatados através da redistribuição ou da associação de várias atribuições. A ENISA está atualmente a executar um programa de curto prazo, criado em 2022 pela Comissão, para reforçar a título imediato a preparação e as capacidades de resposta a ciberincidentes graves. Os serviços abrangidos incluem possibilidades de assistência aos Estados-Membros em caso de incidentes graves que afetem entidades críticas. A execução deste programa de curto prazo pela ENISA está em curso e já forneceu informações valiosas, que foram tidas em conta na preparação do presente regulamento. Os recursos afetados ao programa de curto prazo poderão também ser utilizados no contexto do presente regulamento.

## 1.6. Duração e impacto financeiro da proposta/iniciativa

☒ **duração limitada**

– ☒ em vigor a partir da data de adoção da proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao reforço da solidariedade e das capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança («Regulamento Cibersolidariedade»),

– ☒ impacto financeiro no período compreendido entre 2023 e 2027 para as dotações de autorização e entre 2023 e 2031 para as dotações de pagamento [34].

☐ **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. Métodos de execução orçamental previstos [35]

☒ **Gestão direta** pela Comissão

– ☒ pelos seus serviços, incluindo o pessoal nas delegações da União;

– ☐ pelas agências de execução;

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

☒ **Gestão indireta** por delegação de tarefas de execução orçamental:

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

– ☐ em 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;

– ☐ em organismos de direito público;

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

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

– ☐ em 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».*

Observações

| |
|---|
| As ações relacionadas com o ciberescudo europeu serão executadas pelo ECCC. Enquanto o ECCC não tiver capacidade para executar o seu próprio orçamento, a Comissão Europeia executará as ações em regime de gestão direta em nome do ECCC. O ECCC pode selecionar |

[34] As ações previstas no regulamento devem ser apoiadas pelo próximo quadro financeiro plurianual.

[35] Para mais explicações sobre os métodos de execução orçamental e as referências ao Regulamento Financeiro, consultar o sítio BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

entidades com base em convites à manifestação de interesse para participar na aquisição conjunta de ferramentas. O ECCC pode conceder subvenções para o funcionamento dessas ferramentas.

Além disso, o ECCC pode conceder subvenções para ações de preparação no âmbito do mecanismo de emergência em matéria de cibersegurança.

Incumbe à Comissão a responsabilidade global pela execução da Reserva de Cibersegurança da UE. Através de acordos de contribuição, a Comissão pode confiar, no todo ou em parte, o funcionamento e a administração da Reserva de Cibersegurança da UE à ENISA. As ações atribuídas pelo presente regulamento à ENISA estão em conformidade com o seu atual mandato. Estas ações incluem: i) apoiar o grupo de cooperação SRI no desenvolvimento das ações de preparação de acordo com as avaliações dos riscos, ii) apoiar a Comissão na criação e supervisão da execução da Reserva de Cibersegurança da UE, incluindo na receção e no tratamento dos pedidos de apoio, iii) elaborar modelos para facilitar a apresentação de pedidos de apoio e acordos específicos a celebrar entre o prestador de serviços e o utilizador ao qual é prestado apoio ao abrigo da Reserva de Cibersegurança da UE e iv) analisar e avaliar as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a incidentes de cibersegurança significativos ou em grande escala específicos e elaborar relatórios sobre os mesmos.

Prevê-se que todas estas tarefas representem cerca de sete ETC provenientes dos recursos existentes da ENISA, tirando já partido dos conhecimentos especializados e dos trabalhos preparatórios atualmente realizados por esta agência no âmbito do projeto-piloto de apoio de emergência para a preparação e a resposta a incidentes.

## 2. MEDIDAS DE GESTÃO

### 2.1. Disposições em matéria de acompanhamento e prestação de informações

*Especificar a periodicidade e as condições.*

A Comissão acompanhará a execução, a aplicação e a conformidade com as referidas novas disposições com vista a avaliar a sua eficácia. A Comissão apresenta um relatório sobre a avaliação e a revisão do presente regulamento ao Parlamento Europeu e ao Conselho no prazo de quatro anos a contar da data da sua aplicação.

### 2.2. Sistema(s) de gestão e de controlo

*2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos*

O regulamento introduz um quadro para a execução do financiamento da UE com vista a aumentar a resiliência em matéria de cibersegurança através de ações que reforcem as capacidades de deteção, resposta e recuperação em caso de incidentes de cibersegurança significativos e em grande escala. As unidades da DG CNECT responsáveis pelo domínio de intervenção farão a gestão da aplicação da diretiva.

Para desempenhar as novas funções, é necessário dotar os serviços da Comissão dos recursos adequados. A execução do novo regulamento deverá exigir seis ETC (três AD e três AC) de modo a abranger as seguintes tarefas:

- determinar as ações de preparação de acordo com as avaliações dos riscos,
- assegurar a interoperabilidade entre as plataformas de SOC transfronteiriças,
- elaborar potenciais atos de execução (dois para os SOC e dois para o mecanismo de emergência em matéria de cibersegurança),
- gerir as convenções de acolhimento e utilização dos SOC,
- criar e gerir a Reserva de Cibersegurança da UE, diretamente ou através de um acordo de contribuição para a ENISA. Em caso de acordo de contribuição para a ENISA, elaborar e supervisionar a execução do acordo de contribuição para as funções atribuídas à ENISA,
- participar nos grupos de consulta convocados pela ENISA para analisar e avaliar incidentes de cibersegurança significativos e em grande escala e preparar os relatórios.

*2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar*

Um risco identificado para o ciberescudo europeu é o de os Estados-Membros não partilharem uma quantidade suficiente de informações pertinentes sobre ciberameaças no âmbito das plataformas de SOC transfronteiriças ou entre as plataformas transfronteiriças e outras entidades pertinentes a nível da UE. A fim de atenuar estes riscos, a atribuição de financiamento será feita na sequência de um convite à manifestação de interesse em que os Estados-Membros se comprometem a partilhar uma certa quantidade de informações a nível da UE. Este compromisso será então formalizado numa convenção de acolhimento e utilização, que conferirá ao ECCC poderes para realizar auditorias a fim de assegurar que as ferramentas e infraestruturas adquiridas conjuntamente estão a ser utilizadas em consonância com o

acordo. Os compromissos relativos a um elevado nível de partilha de informações no âmbito dos SOC transfronteiriços serão formalizados num acordo de consórcio.

Um risco identificado para o mecanismo de ciberemergência é o de os utilizadores que participam no mecanismo não tomarem medidas suficientes para assegurar a preparação para ciberataques. Por esse motivo, a fim de poderem receber apoio da Reserva de Cibersegurança da UE, os utilizadores são obrigados a tomar essas medidas de preparação. Ao apresentarem os pedidos de apoio à Reserva de Cibersegurança da UE, os utilizadores têm de explicar que medidas já foram tomadas para dar resposta ao incidente, as quais serão tidas em conta durante a avaliação dos pedidos à Reserva de Cibersegurança da UE.

*2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo ÷ valor dos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)*

Uma vez que as regras de participação no Programa Europa Digital aplicáveis ao apoio ao abrigo do Regulamento Cibersolidariedade são idênticas às que a Comissão utilizará nos seus programas de trabalho, e que a população de beneficiários apresenta um perfil de risco comparável ao dos programas em regime de gestão direta, pode esperar-se que a margem de erro seja semelhante à prevista pela Comissão para o Programa Europa Digital, ou seja, uma garantia razoável de que o risco de erro, no período plurianual de despesas, se mantenha, anualmente, entre 2 % e 5 %, sendo o objetivo último a consecução de uma taxa de erro residual o mais próxima possível dos 2 % no encerramento dos programas plurianuais, uma vez tido em conta o impacto financeiro de todas as medidas de auditoria, correção e recuperação.

## 2.3. Medidas de prevenção de fraudes e irregularidades

*Especificar as medidas de prevenção e de proteção existentes ou previstas, por exemplo, na estratégia antifraude.*

No caso do ciberescudo europeu, o ECCC terá poderes para auditar, com base no acesso à informação e em verificações no local, as ferramentas e infraestruturas adquiridas conjuntamente, em conformidade com a convenção de acolhimento e utilização a assinar entre o consórcio de acolhimento e o ECCC.

As atuais medidas de prevenção da fraude aplicáveis às instituições, órgãos e organismos da União cobrirão as dotações adicionais necessárias para efeitos do presente regulamento.

## 3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

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

- Atuais rubricas orçamentais

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

| Rubrica do quadro financeiro plurianual | Rubrica orçamental | Tipo de despesas | Participação | | | |
|---|---|---|---|---|---|---|
| | Número | DD/DND [36]. | dos países da EFTA [37] | de países candidatos e países candidatos potenciais [38] | de outros países terceiros | outras receitas afetadas |
| 1 | 02 04 01 10 – Programa Europa Digital – Cibersegurança | DD | SIM | SIM | NÃO | NÃO |
| 1 | 02 04 01 11 – Programa Europa Digital – Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança | DD | SIM | SIM | NÃO | NÃO |
| 1 | 02 04 03 – Programa Europa Digital – Inteligência artificial | DD | SIM | SIM | NÃO | NÃO |
| 1 | 02 04 04 – Programa Europa Digital – Competências | DD | SIM | SIM | NÃO | NÃO |
| 1 | 02 01 30 – Despesas de apoio ao Programa Europa Digital | DND | SIM | SIM | NÃO | NÃO |

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

### 3.2. Impacto financeiro estimado da proposta nas dotações

*3.2.1. Síntese do impacto estimado nas dotações operacionais*

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

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

Em milhões de EUR (três casas decimais)

| **Rubrica do quadro financeiro plurianual** | Número | 1 **Mercado único, Inovação e Digital** |
|---|---|---|

A proposta não aumentará o nível total de autorizações no âmbito do Programa Europa Digital. Com efeito, a contribuição para esta iniciativa corresponde a uma redistribuição das autorizações procedentes do OE2 e do OE4 para reforçar o orçamento do OE3 e do ECCC. Qualquer aumento de autorizações no âmbito do Programa Europa Digital resultante de uma revisão do QFP poderá ser utilizado para efeitos desta iniciativa.

| DG CNECT | | | Ano **2025** | Ano **2026** | Ano **2027** | Ano **2028+** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ Dotações operacionais | | | | | | | | | | |
| Rubrica orçamental [39] 02.040110 (redistribuição de 02.0403 e 02.0404) | Autorizações | (1a) | 15,000 | 15,000 | 6,000 | p.m. | | | | **36,000** |
| | Pagamentos | (2a) | 15,000 | 15,000 | 6,000 | | | | | **36,000** |
| Rubrica orçamental 02.040111.02 (redistribuição de 02.0403 e 02.0404) | Autorizações | (1b) | 13,000 | 23,000 | 28,000 | p.m. | | | | **64,000** |
| | Pagamentos | (2b) | 8,450 | 18,200 | 25,250 | 12,100 | | | | **64,000** |
| Dotações de natureza administrativa financiadas a partir da dotação de programas específicos [40] | | | | | | | | | | |
| Rubrica orçamental 02.0130 | | (3) | 0,150 | 0,150 | 0,150 | p.m. | | | | 0,450 |

[39] De acordo com a nomenclatura orçamental oficial.

[40] 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.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **TOTAL das dotações para a DG CNECT** | Autorizações | =1a+1b +3 | **28,150** | **38,150** | **34,150** | **p.m.** | | | | **100,450** |
| | Pagamentos | =2a+2b +3 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ TOTAL das dotações operacionais | Autorizações | (4) | 28,000 | 38,000 | 34,000 | p.m. | | | | **100,000** |
| | Pagamentos | (5) | 23,450 | 33,200 | 31,250 | 12,100 | | | | **100,000** |
| ○ TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos | | (6) | 0,150 | 0,150 | 0,150 | p.m. | | | | **0,450** |
| **TOTAL das dotações da RUBRICA 1** do quadro financeiro plurianual | Autorizações | =4+ 6 | **28,150** | **38,150** | **34,150** | **p.m.** | | | | **100,450** |
| | Pagamentos | =5+ 6 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

**<u>Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica operacional, repetir a secção acima:</u>**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ TOTAL das dotações operacionais (todas as rubricas operacionais) | Autorizações | (4) | 28,000 | 38,000 | 34,000 | p.m. | | | | **100,000** |
| | Pagamentos | (5) | 23,450 | 33,200 | 31,250 | 12,100 | | | | **100,000** |
| TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos (todas as rubricas operacionais) | | (6) | 0,150 | 0,150 | 0,150 | | | | | **0,450** |
| **TOTAL das dotações das RUBRICAS 1 a 6** do quadro financeiro plurianual (quantia de referência) | Autorizações | =4+ 6 | **28,150** | **38,150** | **34,150** | **p.m.** | | | | **100,450** |
| | Pagamentos | =5+ 6 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

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

Esta secção deve ser preenchida com «dados orçamentais de natureza administrativa» a inserir em primeiro lugar no anexo da ficha financeira legislativa (anexo V da Decisão da Comissão que estabelece as regras internas sobre a execução da secção «Comissão» do orçamento geral da União Europeia), que é carregado na base DECIDE para efeitos das consultas interserviços.

Em milhões de EUR (três casas decimais)

| | | Ano **2025** | Ano **2026** | Ano **2027** | Ano **2028+** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| DG: CNECT | | | | | | | | | |
| ○ Recursos humanos | | 0,786 | 0,786 | 0,786 | p.m. | | | | **2,358** |
| ○ Outras despesas administrativas | | 0,035 | 0,035 | 0,035 | p.m. | | | | **0,105** |
| **TOTAL DG CNECT** | Dotações | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL das dotações da RUBRICA 7** do quadro financeiro plurianual | (Total das autorizações = Total dos pagamentos) | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

Em milhões de EUR (três casas decimais)

| | | Ano **2025** | Ano **2026** | Ano **2027** | Ano **2028+** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL das dotações das RUBRICAS 1 a 7** do quadro financeiro plurianual | Autorizações | **28,971** | **38,971** | **34,971** | **p.m.** | | | | **102,913** |
| | Pagamentos | **24,421** | **34,171** | **32,221** | **12,100** | | | | **102,913** |

*3.2.2. Estimativa das realizações financiadas com dotações operacionais*

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

| **Indicar os objetivos e as realizações** ⇩ | | | Ano **N** | | Ano **N+1** | | Ano **N+2** | | Ano **N+3** | | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | | | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **REALIZAÇÕES** | | | | | | | | | | | | | | | | | |
| | Tipo [41] | Custo médio | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º | Custo | N.º total | Custo total |
| OBJETIVO ESPECÍFICO N.º 1 [42]… | | | | | | | | | | | | | | | | | | |
| - Realização | | | | | | | | | | | | | | | | | | |
| - Realização | | | | | | | | | | | | | | | | | | |
| - Realização | | | | | | | | | | | | | | | | | | |
| Subtotal do objetivo específico n.º 1 | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO N.º 2 … | | | | | | | | | | | | | | | | | | |
| - Realização | | | | | | | | | | | | | | | | | | |
| Subtotal do objetivo específico n.º 2 | | | | | | | | | | | | | | | | | | |
| **TOTAIS** | | | | | | | | | | | | | | | | | | |

[41] As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[42] Tal como descrito no ponto 1.4.2., «Objetivo(s) específico(s)…».

### *3.2.3. Síntese do impacto estimado nas dotações administrativas*

– ☐ 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)

| | Ano 2025 | Ano 2026 | Ano 2027 | Ano N+3 | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| **RUBRICA 7 do quadro financeiro plurianual** | | | | | | | | |
| Recursos humanos | 0,786 | 0,786 | 0,786 | | | | | **2,358** |
| Outras despesas administrativas | 0,035 | 0,035 | 0,035 | | | | | **0,105** |
| **Subtotal RUBRICA 7 do quadro financeiro plurianual** | **0,821** | **0,821** | **0,821** | | | | | **2,463** |
| **Com exclusão da RUBRICA 7 [43] do quadro financeiro plurianual** | | | | | | | | |
| Recursos humanos | | | | | | | | |
| Outras despesas administrativas | 0,150 | 0,150 | 0,150 | | | | | **0,450** |
| **Subtotal com exclusão da RUBRICA 7 do quadro financeiro plurianual** | **0,150** | **0,150** | **0,150** | | | | | **0,450** |
| **TOTAL** | **0,971** | **0,971** | **0,971** | | | | | **2,913** |

As dotações relativas aos recursos humanos e outras despesas administrativas necessárias serão cobertas pelas dotações da DG já afetadas à gestão da ação e/ou reafetadas internamente na DG e, se necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no âmbito do processo de afetação anual e atendendo às disponibilidades orçamentais.

[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.

3.2.3.1. Necessidades estimadas de recursos humanos

– ☐ 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.*

| | | Ano **2025** | Ano **2026** | Ano **2027** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | |
|---|---|---|---|---|---|---|---|---|
| **O Lugares do quadro do pessoal (funcionários e agentes temporários)** | | | | | | | | |
| 20 01 02 01 (na sede e nos gabinetes de representação da Comissão) | | 3 | 3 | 3 | | | | |
| 20 01 02 03 (nas delegações) | | | | | | | | |
| 01 01 01 01 (investigação indireta) | | | | | | | | |
| 01 01 01 11 (investigação direta) | | | | | | | | |
| Outra rubrica orçamental (especificar) | | | | | | | | |
| **O Pessoal externo (em equivalente a tempo completo: ETC)** [44] | | | | | | | | |
| 20 02 01 (AC, PND e TT da «dotação global») | | 3 | 3 | 3 | | | | |
| 20 02 03 (AC, AL, PND, TT e JPD nas delegações) | | | | | | | | |
| **XX** 01 xx **yy zz** [45] | - na sede | | | | | | | |
| | - nas delegações | | | | | | | |
| 01 01 01 02 (AC, PND e TT – investigação indireta) | | | | | | | | |
| 01 01 01 12 (AC, PND e TT – investigação direta) | | | | | | | | |
| Outra rubrica orçamental (especificar) | | | | | | | | |
| **TOTAL** | | **6** | **6** | **6** | | | | |

**XX** constitui o domínio de intervenção ou rubrica orçamental em causa.

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 âmbito do processo de afetação anual e atendendo às disponibilidades orçamentais.

Descrição das tarefas a executar:

| | |
|---|---|
| Funcionários e agentes temporários | - determinar as ações de preparação de acordo com as avaliações dos riscos (artigo 11.º),<br>- elaborar potenciais atos de execução (dois para os SOC e dois para o mecanismo de emergência em matéria de cibersegurança),<br>- gerir as convenções de acolhimento e utilização dos SOC,<br>- criar e gerir a Reserva de Cibersegurança da UE, diretamente ou através de um acordo de contribuição para a ENISA. |
| Pessoal externo | Sob a supervisão de um funcionário,<br>- determinar as ações de preparação de acordo com as avaliações dos riscos (artigo 11.º),<br>- elaborar potenciais atos de execução (dois para os SOC e dois para o mecanismo de emergência em matéria de cibersegurança),<br>- gerir as convenções de acolhimento e utilização dos SOC,<br>- criar e gerir a Reserva de Cibersegurança da UE, diretamente ou através de um acordo de contribuição para a ENISA. |

[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»).

### 3.2.4. *Compatibilidade com o atual quadro financeiro plurianual*

A proposta/iniciativa:

– [X] pode ser integralmente financiada por meio da reafetação de fundos no quadro da rubrica pertinente do quadro financeiro plurianual (QFP).

| Explicitar a reprogramação necessária, especificando as rubricas orçamentais em causa e as quantias correspondentes. Em caso de reprogramação significativa, fornecer um quadro Excel. |
|---|

| | 2023 | 2024 | 2025 | 2026 | 2027 | total |
|---|---|---|---|---|---|---|
| OE1 | 16.232.897 | 20.528.765 | 17.406.899 | 16.223.464 | 10.022.366 | 80.414.391 |
| | | | | | | |
| OE2 inicial | 226.316.819 | 295.067.000 | 195.649.000 | 221.809.000 | 246.608.000 | 1.185.449.819 |
| Para iniciativa CIBER | | | 18.000.000 | 28.000.000 | 19.000.000 | 65.000.000 |
| **NOVO OE2** | **226.316.819** | **295.067.000** | **177.649.000** | **193.809.000** | **227.608.000** | **1.120.449.819** |
| | | | | | | |
| OE3 PO 24 | 24.361.553 | 35.596.172 | 3.638.000 | 3.638.000 | 11.175.000 | 78.408.725 |
| Do OE2-OE4 | | | 15.000.000 | 15.000.000 | 6.000.000 | 36.000.000 |
| **Novo OE3** | **24.361.553** | **35.596.172** | **18.638.000** | **18.638.000** | **17.175.000** | **114.408.725** |
| | | | | | | |
| ECCC inicial | 176.222.303 | 208.374.879 | 104.228.130 | 90.704.986 | 84.851.497 | 664.381.795 |
| Do OE2-OE4 | | | 13.000.000 | 23.000.000 | 28.000.000 | 64.000.000 |
| **Novo ECCC** | **176.222.303** | **208.374.879** | **117.228.130** | **113.704.986** | **112.851.497** | **728.381.795** |
| | | | | | | |
| OE4 inicial | 66.902.708 | 64.892.032 | 56.577.977 | 70.477.245 | 72.107.201 | 330.957.163 |
| Para iniciativa CIBER | | | 10.000.000 | 10.000.000 | 15.000.000 | 35.000.000 |
| **NOVO OE4** | **66.902.708** | **64.892.032** | **46.577.977** | **60.477.245** | **57.107.201** | **295.957.163** |

– [ ] requer o recurso à margem não afetada na rubrica em causa do QFP e/ou o recurso a instrumentos especiais tais como definidos no Regulamento QFP.

| Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes, bem como os instrumentos cuja utilização é proposta. |
|---|

– [ ] requer uma revisão do QFP.

| Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes. |
|---|

### 3.2.5. *Participação de terceiros no financiamento*

A proposta/iniciativa:

– [X] não prevê o cofinanciamento por terceiros

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

Dotações em milhões de EUR (três casas decimais)

| | Ano **N** [46] | Ano **N+1** | Ano **N+2** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | | Total |
|---|---|---|---|---|---|---|---|---|
| Especificar o organismo de cofinanciamento | | | | | | | | |

[46] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de aplicação previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| TOTAL das dotações cofinanciadas | | | | | | | | |

### 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

– ☐ noutras receitas

– indicar se as receitas são afetadas a rubricas de despesas ☐

Em milhões de EUR (três casas decimais)

| Rubrica orçamental das receitas: | Dotações disponíveis para o atual exercício | Impacto da proposta/iniciativa [47] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Ano **N** | Ano **N+1** | Ano **N+2** | Ano **N+3** | Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6) | | |
| 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 nas receitas ou quaisquer outras informações).

[…]

[47] 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.