UNIÃO EUROPEIA

PARLAMENTO EUROPEU **CONSELHO**

Bruxelas, 19 de dezembro de 2024
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO QUE CRIA MEDIDAS DESTINADAS A REFORÇAR A SOLIDARIEDADE E AS CAPACIDADES DA UNIÃO PARA DETETAR, PREPARAR E DAR RESPOSTA A CIBERAMEAÇAS E INCIDENTES DE CIBERSEGURANÇA E QUE ALTERA O REGULAMENTO (UE) 2021/694 (REGULAMENTO DE CIBERSOLIDARIEDADE)

REGULAMENTO (UE) 2024/…
DO PARLAMENTO EUROPEU E DO CONSELHO

de 19 de dezembro de 2024

que cria medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ciberameaças e incidentes de cibersegurança e que altera o Regulamento (UE) 2021/694 (Regulamento de Cibersolidariedade)

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[4],

---

1 Parecer de 18 de abril de 2023 (ainda não publicado no Jornal Oficial).
2 JO C 349 de 29.9.2023, p. 167.
3 JO C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Posição do Parlamento Europeu de 24 de abril de 2024 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 2 de dezembro de 2024.

Considerando o seguinte:

(1) A utilização e dependência de tecnologias da informação e comunicação tornaram-se características fundamentais de todos os sectores de atividade económica e da sociedade, à luz da crescente interligação e interdependência das administrações públicas, das empresas e dos cidadãos dos Estados-Membros a nível intersectorial e transfronteiriço, introduzindo simultaneamente possíveis vulnerabilidades.

(2) A magnitude, a frequência e o impacto dos incidentes de cibersegurança, incluindo ataques à cadeia de abastecimento para efeitos de ciberespionagem, *software* de sequestro (*ransomware* em inglês) ou perturbação, estão a aumentar a nível da União e a nível mundial. 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 de cibersegurança em grande escala que causem perturbações ou danos significativos às infraestruturas críticas exige uma maior preparação do regime de cibersegurança da União. Esta ameaça vai além da guerra de agressão da Rússia contra a Ucrânia e é provável que persista, dada a multiplicidade de intervenientes associados envolvidos nas atuais tensões geopolíticas. Tais incidentes podem impedir a prestação de serviços públicos, uma vez que os ciberataques são frequentemente dirigidos a infraestruturas e serviços públicos locais, regionais ou nacionais, sendo as autoridades locais particularmente vulneráveis, nomeadamente devido aos seus recursos limitados. Podem impedir igualmente o exercício das atividades económicas, incluindo em sectores de importância crítica ou noutros sectores críticos, gerar perdas financeiras importantes, minar a confiança dos utilizadores, causar graves prejuízos à economia e aos regimes democráticos 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 rapidamente, não se confinando a uma área geográfica específica e ocorrendo em simultâneo ou alastrando-se imediatamente por vários países. É importante criar uma estreita cooperação entre sector público, sector privado, meio académico, sociedade civil e meios de comunicação social.

(3) É necessário reforçar a posição concorrencial dos sectores da indústria e dos serviços da União na economia digital e apoiar a sua transformação digital, através do reforço do nível de cibersegurança no mercado único digital, como recomendado em três propostas diferentes da Conferência sobre o Futuro da Europa. É necessário aumentar a resiliência dos cidadãos, das empresas, nomeadamente das microempresas e pequenas e médias empresas e as empresas em fase de arranque, e das entidades que operam infraestruturas críticas relativamente ao aumento das ciberameaças, que podem ter um impacto societal e económico devastador. Por conseguinte, é necessário investir em infraestruturas e serviços e reforçar capacidades para desenvolver competências em matéria de cibersegurança que apoiem uma deteção e uma resposta mais rápidas a ciberameaças e incidentes de cibersegurança. Além disso, os Estados-Membros necessitam de assistência para se prepararem melhor e responderem a incidentes de cibersegurança significativos e a incidentes de cibersegurança em grande escala, bem como de assistência na recuperação inicial tanto de uns como de outros. Com base nas estruturas existentes e em estreita cooperação com as mesmas, a União deverá também aumentar as suas capacidades nesses domínios, em especial no que diz respeito à recolha e análise de dados sobre ciberameaças e incidentes de cibersegurança.

(4) A União tomou já uma série de medidas de redução das vulnerabilidades e acréscimo da resiliência das infraestruturas e entidades críticas contra os riscos, nomeadamente o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[5], as Diretivas 2013/40/UE[6] e (UE) 2022/2555[7] do Parlamento Europeu e do Conselho e a Recomendação (UE) 2017/1584 da Comissão[8]. Além disso, a Recomendação do Conselho de 8 de dezembro de 2022 relativa a uma abordagem coordenada à escala da União para reforço da resiliência das infraestruturas críticas convida os Estados-Membros a tomarem medidas, bem como a cooperarem 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 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).

6 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).

7 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, p. 80).

8 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).

(5) Os riscos de cibersegurança crescentes e um cenário de ameaças global complexo, com um risco claro de rápida disseminação dos incidentes de um Estado-Membro para outro e de um país terceiro para a União, exigem que a solidariedade seja reforçada à escala da União para uma melhor deteção, preparação e resposta a ciberameaças e incidentes de cibersegurança, e recuperação destes, em particular através do reforço das capacidades das estruturas existentes. Além disso, as Conclusões do Conselho de 23 de maio de 2022 sobre o desenvolvimento da postura da União Europeia no ciberespaço convidaram a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança.

(6) A Comunicação Conjunta da Comissão e do alto representante da União para os Negócios Estrangeiros e a Política de Segurança de 10 de novembro de 2022 ao Parlamento Europeu e ao Conselho sobre a política de ciberdefesa da UE, anunciava uma iniciativa da UE em matéria de cibersolidariedade com os objetivos de reforço das capacidades comuns de deteção, conhecimento situacional e resposta da UE mediante a promoção da implantação de uma infraestrutura de centros de operações de segurança (SOC, do inglês *Security Operation* Centres) 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 situacional relativamente a ciberameaças e incidentes de cibersegurança na União e intensificar a solidariedade, aumentando a preparação e as capacidades dos Estados-Membros e da União para prevenir e dar resposta a incidentes de cibersegurança significativos e incidentes de cibersegurança em grande escala. Por conseguinte, há que estabelecer uma rede pan-europeia de plataformas de cibersegurança («Sistema Europeu de Alerta em matéria de Cibersegurança») para criar capacidades coordenadas de deteção e conhecimento situacional, reforçando as capacidades da União de deteção de ameaças e de partilha de informações; criar um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros, caso o solicitem, na preparação, resposta, atenuação do impacto e recuperação inicial de incidentes de cibersegurança significativos e de incidentes de cibersegurança em grande escala, bem como para apoiar outros utilizadores na resposta a incidentes de cibersegurança significativos e a incidentes equivalentes a um incidente de cibersegurança em grande escala; e criar um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes de cibersegurança significativos ou incidentes de cibersegurança em grande escala específicos. As ações tomadas ao abrigo do presente regulamento deverão ser realizadas no devido respeito pelas competências dos Estados-Membros e deverão complementar e não duplicar as atividades realizadas pela rede de CSIRT (do inglês *computer security incident response teams*), pela Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe) ou pelo grupo de cooperação (“grupo de cooperação SRI”), todos criadas nos termos da Diretiva (UE) 2022/2555. 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 necessário alterar o Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho[9] em determinados domínios. Concretamente, o presente regulamento deverá alterar o Regulamento (UE) 2021/694 no que respeita ao aditamento de novos objetivos operacionais relacionados com o Sistema Europeu de Alerta em matéria de Cibersegurança e o mecanismo de emergência em matéria de cibersegurança no âmbito do objetivo específico n.º 3 do Programa Europa Digital (PED), que visa garantir a resiliência, a integridade e a fiabilidade do mercado único digital, reforçar as capacidades para monitorizar os ciberataques e as ciberameaças e dar resposta aos mesmos, bem como promover a cooperação e coordenação transfronteiriças em matéria de cibersegurança. O Sistema Europeu de Alerta em matéria de Cibersegurança pode apoiar de forma significativa os Estados-Membros na previsão de ciberameaças e na proteção contra as mesmas, e a Reserva de Cibersegurança da UE pode desempenhar um papel importante no apoio aos Estados-Membros, às instituições, aos órgãos e organismos da União e aos países terceiros associados ao PED no âmbito da resposta e atenuação do impacto de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala. Esse impacto pode incluir danos materiais ou imateriais consideráveis e riscos graves para a segurança e proteção públicas. Dadas as funções específicas que o Sistema Europeu de Alerta em matéria de Cibersegurança e a Reserva de Cibersegurança da UE poderão desempenhar, o presente regulamento deverá alterar o Regulamento (UE) 2021/694 no que diz respeito à participação de entidades jurídicas estabelecidas na União, mas controladas a partir de países terceiros, sempre que exista um risco real de não estarem disponíveis, na União, as ferramentas, as infraestruturas e os serviços ou a tecnologia, os conhecimentos especializados e as capacidades que são necessários e suficientes e de os benefícios da inclusão dessas entidades superarem o risco para a segurança. Deverão ser criadas as condições específicas em que poderá ser concedido apoio financeiro às ações que visam a implantação do Sistema Europeu de Alerta em matéria de Cibersegurança e da Reserva de Cibersegurança da UE e definidos os mecanismos de governação e coordenação necessários para alcançar os objetivos pretendidos. Outras alterações do Regulamento (UE) 2021/694 deverão incluir descrições das ações propostas no âmbito dos novos objetivos operacionais, bem como indicadores mensuráveis para acompanhar a execução destes novos objetivos operacionais.

---

[9] 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).

(9) Para reforçar a resposta da União a ciberameaças e incidentes de cibersegurança, é fundamental a cooperação com organizações internacionais, bem como com parceiros internacionais de confiança que partilham as mesmas ideias. Neste contexto, os parceiros internacionais de confiança que partilham as mesmas ideias deverão ser entendidos como países que partilham os princípios que inspiraram a criação da União, a saber, a democracia, o Estado de direito, a universalidade e indivisibilidade dos direitos humanos e das liberdades fundamentais, o respeito pela dignidade humana, os princípios da igualdade e solidariedade e o respeito pelos princípios da Carta das Nações Unidas e do direito internacional, e que não comprometem os interesses essenciais de segurança da União ou dos seus Estados-Membros. Essa cooperação pode também ser benéfica no que diz respeito às ações tomadas nos termos do presente regulamento, em especial o Sistema Europeu de Alerta em matéria de Cibersegurança e a Reserva de Cibersegurança da UE. O Regulamento (UE) 2021/694 deverá, se estiverem preenchidas determinadas condições de disponibilidade e segurança, prever concursos para o Sistema Europeu de Alerta em matéria de Cibersegurança e a Reserva de Cibersegurança da UE que possam ser abertos a entidades jurídicas controladas a partir de países terceiros, desde que sejam cumpridos determinados requisitos de segurança. Ao avaliar o risco para a segurança decorrente da abertura de concursos desta forma, é importante ter em conta os princípios e valores que a União partilha com os parceiros internacionais que partilham as mesmas ideias, sempre que esses princípios e valores estejam relacionados com interesses essenciais de segurança da União. Além disso, caso esses requisitos de segurança sejam examinados ao abrigo do Regulamento (UE) 2021/694, podem ser tidos em conta vários elementos, como a estrutura empresarial e o processo decisório de uma entidade, a segurança dos dados e das informações classificadas ou sensíveis e a garantia de que os resultados da ação não estão sujeitos a controlo ou restrições por parte de países terceiros não elegíveis.

(10) O financiamento de ações no âmbito do presente regulamento deverá estar previsto no Regulamento (UE) 2021/694, que deverá continuar a ser o ato de base que rege as ações consagradas no objetivo específico n.º 3 do PED. Os programas de trabalho pertinentes deverão prever condições específicas de participação relativas a cada ação, em conformidade com o Regulamento (UE) 2021/694.

(11) 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 encontram-se enunciadas no Regulamento (UE, Euratom) 2024/2509 do Parlamento Europeu e do Conselho[10] 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].

---

[10] Regulamento (UE, Euratom) 2024/2509 do Parlamento Europeu e do Conselho, de 23 de setembro de 2024, relativo às regras financeiras aplicáveis ao orçamento geral da União (JO L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Regulamento (UE, Euratom) 2020/2092 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2020, relativo a um regime geral de condicionalidade para a proteção do orçamento da União (JO L 433 I de 22.12.2020, p. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Embora as medidas de prevenção e preparação sejam essenciais para reforçar a resiliência da União na resposta a incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala, a ocorrência, o momento e a magnitude desses incidentes são, pela sua natureza, imprevisíveis. Os recursos financeiros necessários para assegurar uma resposta adequada podem variar significativamente de ano para ano e deverão poder ser disponibilizados imediatamente. Conciliar o princípio orçamental da previsibilidade com a necessidade de reagir rapidamente a novas necessidades exige que a execução financeira dos programas de trabalho seja adaptada. Por conseguinte, para além da transição de dotações autorizadas nos termos do artigo 12.º, n.º 4, do Regulamento (UE, Euratom) 2024/2509, é adequado autorizar a transição de dotações não utilizadas apenas para o exercício seguinte e apenas para a Reserva de Cibersegurança da UE e as ações de apoio à assistência mútua.

(13) Para prevenir, avaliar e responder de forma mais eficaz a ciberameaças e incidentes de cibersegurança, e recuperar dos mesmos, 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. Uma abordagem pró-ativa para identificar, atenuar e prevenir ciberameaças inclui um aumento da capacidade de deteção avançada. O Sistema Europeu de Alerta em matéria de Cibersegurança deverá ser composto por várias plataformas de cibersegurança transfronteiriças interoperáveis, cada uma agrupando três ou mais plataformas de cibersegurança nacionais. Essa infraestrutura deverá servir os interesses e necessidades nacionais e da União em matéria de cibersegurança, tirando partido de tecnologias de ponta para a recolha avançada de dados e informações pertinentes, se for caso disso anonimizados, e de ferramentas de análise, reforçando as capacidades coordenadas de ciberdeteção e de gestão e proporcionando um conhecimento situacional em tempo real. Essa infraestrutura deverá servir para melhorar a ciberpostura aumentando a deteção, agregação e a análise de dados e informações com o objetivo de prevenir ciberameaças e incidentes de cibersegurança e, assim, complementar e apoiar as entidades e redes da União responsáveis pela gestão de cibercrises na União, nomeadamente a UE-CyCLONe.

(14) A participação dos Estados-Membros no Sistema Europeu de Alerta em matéria de Cibersegurança é de cariz voluntário. Cada Estado-Membro deverá designar uma entidade única a nível nacional encarregada de coordenar as atividades de deteção de ciberameaças nesse Estado-Membro. Essas plataformas de cibersegurança nacionais deverão funcionar como ponto de referência e acesso a nível nacional para a participação no Sistema Europeu de Alerta em matéria de Cibersegurança e deverão assegurar que as informações sobre ciberameaças provenientes de entidades públicas e privadas são partilhadas e recolhidas a nível nacional de forma eficaz e simplificada. As plataformas de cibersegurança nacionais podem reforçar a cooperação e a partilha de informações entre entidades públicas e privadas, bem como apoiar o intercâmbio de dados e informações pertinentes com as comunidades sectoriais e transectoriais pertinentes, incluindo os centros de partilha e análise de informações (ISAC, do inglês *Information Sharing and Analysis Centers*) sectoriais pertinentes. A cooperação estreita e coordenada entre entidades públicas e privadas é fundamental para reforçar a ciber-resiliência da União. Tal cooperação é particularmente valiosa no contexto da partilha de informações sobre ciberameaças destinada a melhorar a ciberproteção ativa. No âmbito de tal cooperação e partilha de informações, as plataformas de cibersegurança nacionais podem solicitar e receber informações específicas. O presente regulamento não obriga nem habilita essas plataformas de cibersegurança nacionais a executar esses pedidos. Se for caso disso, e em conformidade com o direito nacional e da União, as informações solicitadas ou recebidas podem incluir dados de telemetria, sensores e registos de entidades, como os prestadores de serviços de segurança geridos, que operam em sectores de importância crítica ou noutros sectores críticos nesse Estado-Membro, a fim de reforçar a deteção rápida de potenciais ciberameaças e incidentes de cibersegurança numa fase precoce, melhorando assim o conhecimento situacional. Se a plataforma de cibersegurança nacional não for a autoridade competente designada ou estabelecida pelo Estado-Membro em causa nos termos do artigo 8.º, n.º 1, da Diretiva (UE) 2022/2555, é fundamental que coordene com essa autoridade competente os pedidos e a receção desses dados.

(15) No âmbito do Sistema de Alerta em matéria de Cibersegurança, deverão ser criadas várias plataformas de cibersegurança transfronteiriças. Tais plataformas deverão reunir as plataformas de cibersegurança nacionais de, pelo menos, três Estados-Membros para assegurar que os benefícios da deteção de ameaças transfronteiriças e da partilha e gestão de informações possam ser plenamente alcançados. O objetivo geral das plataformas de cibersegurança transfronteiriças deverá ser o reforço das capacidades de análise, prevenção e deteção de ciberameaças e o apoio à produção de informações de alta qualidade sobre ciberameaças, principalmente através da partilha de informações pertinentes, anonimizadas se for caso disso, num ambiente de confiança e seguro, 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 e seguro. As plataformas de cibersegurança transfronteiriças deverão proporcionar novas capacidades adicionais, tendo por base e complementando os SOC existentes, as CSIRT e outros intervenientes relevantes, incluindo a rede de CSIRT.

(16) Um Estado-Membro selecionado pelo Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC, do inglês *European Cybersecurity Competence Centre*) criado pelo Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho[12], na sequência de um convite à manifestação de interesse para criar, ou reforçar as capacidades de uma plataforma de cibersegurança nacional deverá adquirir ferramentas, infraestruturas ou serviços pertinentes em conjunto com o ECCC. Esse Estado-Membro deverá ser elegível para receber uma subvenção para operar as ferramentas, infraestruturas ou serviços. Um consórcio de acolhimento, composto por, pelo menos, três Estados-Membros, que tenha sido selecionado pelo ECCC na sequência de um convite à manifestação de interesse para criar ou reforçar as capacidades de uma plataforma de cibersegurança transfronteiriça, deverá adquirir ferramentas, infraestruturas ou serviços pertinentes em conjunto com o ECCC. O consórcio de acolhimento deverá ser elegível para receber uma subvenção para operar as ferramentas, infraestruturas ou serviços. O procedimento de contratação para a aquisição das ferramentas, infraestruturas ou serviços pertinentes deverá ser realizado conjuntamente pelo ECCC e pelas entidades adjudicantes competentes dos Estados-Membros selecionados na sequência desses convites à manifestação de interesse. Essa contratação deverá estar em conformidade com o artigo 168.º, n.º 2, do Regulamento (UE, Euratom) 2024/2509 e com as regras financeiras do ECCC. Por conseguinte, as entidades privadas não deverão ser elegíveis para participar nos convites à manifestação de interesse para adquirir ferramentas, infraestruturas ou serviços em conjunto com o ECCC, ou para receber subvenções para operar essas ferramentas, infraestruturas ou serviços. No entanto, os Estados-Membros deverão poder envolver entidades privadas na criação, no reforço e na operação das suas plataformas de cibersegurança nacionais e das plataformas de cibersegurança transfronteiriças de outras formas que considerem ser adequadas, em conformidade com o direito nacional e da União. As entidades privadas podem também ser elegíveis para receber financiamento da União nos termos do Regulamento (UE) 2021/887, a fim de prestar apoio às plataformas de cibersegurança nacionais.

---

[12] 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, 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) A fim de melhorar a deteção de ciberameaças e o conhecimento situacional na União, um Estado-Membro que, na sequência de um convite à manifestação de interesse, tenha sido selecionado para criar ou reforçar as capacidades de uma plataforma de cibersegurança nacional deverá comprometer-se a candidatar-se a participar numa plataforma de cibersegurança transfronteiriça. Se um Estado-Membro não participar numa plataforma de cibersegurança transfronteiriça no prazo de dois anos a contar da data de aquisição das ferramentas, infraestruturas ou serviços ou contar da data em que recebe financiamento através de subvenções, consoante o que ocorrer primeiro, não deverá ser elegível para participar noutras ações de apoio da União no âmbito do Sistema de Alerta em matéria de Cibersegurança destinadas a reforçar as capacidades da sua plataforma de cibersegurança nacional. Nesses casos, as entidades dos Estados-Membros podem ainda participar em convites à apresentação de propostas sobre outros temas no âmbito do PED ou de outros programas de financiamento da União, incluindo convites à apresentação de propostas para a ciberdeteção e a partilha de informações, desde que essas entidades cumpram os critérios de elegibilidade estabelecidos nesses programas.

(18) As CSIRT trocam informações no âmbito da rede de CSIRT, em conformidade com a Diretiva (UE) 2022/2555. O Sistema Europeu de Alerta em matéria de Cibersegurança deverá constituir uma nova capacidade complementar à rede de CSIRT, contribuindo para a criação de um conhecimento situacional da União que permita o reforço das capacidades da rede de CSIRT. As plataformas de cibersegurança transfronteiriças deverão coordenar-se e cooperar estreitamente com a rede de CSIRT. Deverão atuar mediante a mutualização de dados e a partilha de informações pertinentes, anonimizados se for caso disso, sobre ciberameaças provenientes de entidades públicas e privadas, a valorização desses dados e informações através de análises de peritos e de ferramentas de ponta e infraestruturas adquiridas conjuntamente, e o contributo para a soberania tecnológica da União, a sua autonomia estratégica aberta, competitividade e resiliência e o desenvolvimento das capacidades da União.

(19) As plataformas de cibersegurança transfronteiriças deverão funcionar como ponto central que permita uma ampla mutualização de dados pertinentes e informações sobre ciberameaças, e que possibilite a divulgação de informações sobre ameaças entre um conjunto vasto e diversificado de partes interessadas, por exemplo, equipas de resposta a emergências informáticas (CERT, do inglês *Computer Emergency Response Team*), CSIRT, ISAC e operadores de infraestruturas críticas. Os membros do consórcio de acolhimento deverão especificar no acordo de consórcio as informações pertinentes a partilhar entre os participantes da plataforma de cibersegurança transfronteiriça em causa. As informações trocadas entre os participantes numa plataforma de cibersegurança transfronteiriça podem incluir, por exemplo, dados de redes e sensores, fluxos de informações sobre ameaças, indicadores de exposição a riscos e informações contextualizadas sobre incidentes, ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, 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. Além disso, as plataformas de cibersegurança transfronteiriças deverão também celebrar acordos de cooperação entre si. Esses acordos de cooperação deverão, em especial, especificar os princípios de partilha de informações e a interoperabilidade. As suas cláusulas relativas à interoperabilidade, em particular os formatos e protocolos de partilha de informações, deverão ser orientadas e, por conseguinte, ter como ponto de partida as orientações de interoperabilidade emitidas pela Agência da União Europeia para a Cibersegurança (ENISA) criada pelo Regulamento (UE) 2019/881. Essas orientações deverão ser emitidas rapidamente para garantir que as plataformas de cibersegurança transfronteiriças possam tê-las em conta numa fase precoce. Deverão ter em conta as normas internacionais e as boas práticas, bem como o funcionamento de quaisquer plataformas de cibersegurança transfronteiriças estabelecidas.

(20) As plataformas de cibersegurança transfronteiriças e a rede de CSIRT deverão cooperar estreitamente para assegurar sinergias e a complementaridade das atividades. Para o efeito, deverão acordar disposições processuais em matéria de cooperação e partilha de informações pertinentes. Tal poderá incluir a partilha de informações pertinentes sobre ciberameaças e incidentes de cibersegurança significativos e a garantia de que as experiências com ferramentas de ponta, em especial, as tecnologias de inteligência artificial e de análise de dados, utilizadas no âmbito das plataformas de cibersegurança transfronteiriças, sejam partilhadas com a rede de CSIRT.

(21) A partilha do conhecimento situacional 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 incidentes de cibersegurança em grande escala. A Diretiva (UE) 2022/2555 cria a UE-CyCLONe para apoiar a gestão coordenada de crises e de 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 Diretiva (UE) 2022/2555 estabelece igualmente a rede de CSIRT para promover uma cooperação operacional célere e eficaz entre todos os Estados-Membros. Deverão prestar informações pertinentes à rede de CSIRT e informar a UE-CyCLONe, enviando um alerta rápido, a fim de assegurar o conhecimento situacional e reforçar a solidariedade, nas situações em que as plataformas de cibersegurança transfronteiriças obtenham informações relacionadas com um incidente de cibersegurança em grande escala, potencial ou em curso. Concretamente, consoante a 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. Nesse contexto, deverá ser dada a devida atenção ao princípio da necessidade de conhecer e à natureza potencialmente sensível das informações partilhadas. A Diretiva (UE) 2022/2555 reitera 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[13], e a sua responsabilidade no que se refere à apresentação de relatórios analíticos para o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (mecanismo IPCR) nos termos da Decisão de Execução (UE) 2018/1993[14].

---

13 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, 20.12.2013, p. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (JO L 320, 17.12.2018, p. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Quando as plataformas de cibersegurança transfronteiriças partilhem informações pertinentes e alertas rápidos relacionados com um incidente de cibersegurança em grande escala, potencial ou em curso, com a UE-CyCLONe e a rede de CSIRT, é imperativo que tais informações sejam partilhadas através dessas redes com as autoridades dos Estados-Membros, bem como com a Comissão. Nesse contexto, a Diretiva (UE) 2022/2555 prevê que o objetivo da UE-CyCLONe consiste em apoiar a gestão coordenada de crises e de incidentes de cibersegurança em grande escala a nível operacional e assegurar o intercâmbio regular de informações pertinentes entre os Estados-Membros e as instituições, órgãos e organismos da União. As funções da UE-CyCLONe incluem o desenvolvimento da partilha de um conhecimento situacional para tais incidentes e crises. É da maior importância que a UE-CyCLONe assegure, em consonância com esse objetivo e com as suas funções, que essas informações sejam imediatamente facultadas aos representantes dos Estados-Membros pertinentes e à Comissão. Para o efeito, é fundamental que o regulamento interno da UE-CyCLONe inclua disposições adequadas.

(22) As entidades que participam no Sistema Europeu de Alerta em matéria de Cibersegurança deverão 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. Deverão também assegurar canais de comunicação seguros, um nível mínimo de segurança da camada de aplicação, um painel de controlo de conhecimento situacional e indicadores. A adoção de uma taxonomia comum e a elaboração de um modelo de relatórios de situação para descrever as causas das ciberameaças e dos riscos detetados deverão ter em conta os trabalhos existentes realizados no contexto da aplicação da Diretiva (UE) 2022/2555.

(23) A fim de permitir o intercâmbio de dados e informações pertinentes sobre ciberameaças provenientes de várias fontes, em grande escala e num ambiente de confiança e seguro, as entidades que participam no Sistema Europeu de Alerta em matéria de Cibersegurança deverão estar equipadas com ferramentas, equipamentos e infraestruturas de ponta e altamente seguros, bem como dispor de pessoal altamente qualificado. 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.

(24) Ao recolher, analisar, partilhar e trocar dados e informações pertinentes, o Sistema Europeu de Alerta em matéria de Cibersegurança deverá reforçar a soberania tecnológica da União e a autonomia estratégica aberta no domínio da cibersegurança, da competitividade e da resiliência. A mutualização de dados selecionados de alta qualidade poderá também contribuir para o desenvolvimento de tecnologias avançadas de inteligência artificial e de análise de dados. A supervisão humana e, para o efeito, uma mão de obra qualificada continuam a ser essenciais para a mutualização eficaz de dados de alta qualidade.

(25) Embora o Sistema Europeu de Alerta em matéria de Cibersegurança seja um projeto de caráter civil, a comunidade de ciberdefesa poderá beneficiar do desenvolvimento de capacidades civis mais fortes de deteção e de conhecimento situacional para proteger as infraestruturas críticas.

(26) A partilha de informações entre os participantes no Sistema Europeu de Alerta em matéria de Cibersegurança deverá 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 deverá 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, destruir os dados assim que deixem de ser necessários para a finalidade indicada e informar a entidade que disponibiliza os dados de que os mesmos foram destruídos.

(27) A preservação da confidencialidade e da segurança da informação é da maior importância para os três pilares do presente regulamento, quer para incentivar a partilha ou o intercâmbio de informações no contexto do Sistema Europeu de Alerta em matéria de Cibersegurança, preservando os interesses das entidades que solicitam apoio ao abrigo do mecanismo de emergência em matéria de cibersegurança, quer para assegurar que os relatórios no âmbito do mecanismo europeu de análise de incidentes de cibersegurança possam produzir ensinamentos úteis, sem afetar negativamente as entidades afetadas pelos incidentes. A participação dos Estados-Membros e das entidades nesses mecanismos depende das relações de confiança entre as respetivas componentes. Caso as informações sejam confidenciais nos termos das regras nacionais ou da União, a sua partilha ou o seu intercâmbio ao abrigo do presente regulamento deverá limitar-se ao que for pertinente e proporcionado em relação ao objetivo da partilha ou do intercâmbio. A partilha ou o intercâmbio deverá igualmente preservar a confidencialidade dessas informações e proteger a segurança e os interesses comerciais de quaisquer entidades em causa. A partilha ou o intercâmbio de informações ao abrigo do presente regulamento pode realizar-se através de acordos de confidencialidade ou de orientações sobre a distribuição de informações, como o protocolo «sinalização luminosa» (TLP, na sigla em inglês). O TLP deve ser visto como um meio para prestar informações sobre eventuais limitações impostas à divulgação ulterior das informações. É utilizado em quase todas as CSIRT e em alguns ISAC. Além desses requisitos gerais, no que diz respeito ao Sistema Europeu de Alerta em matéria de Cibersegurança, os acordos de consórcios de acolhimento deverão prever regras específicas relativas às condições para a partilha de informações no âmbito da plataforma de cibersegurança transfronteiriça em causa. Esses acordos podem, em particular, exigir que as informações só sejam partilhadas em conformidade com o direito nacional e da União.

(28) No que diz respeito à implantação da Reserva de Cibersegurança da UE, são necessárias regras de confidencialidade específicas. O apoio será solicitado, avaliado e prestado num contexto de crise e no que diz respeito a entidades que operam em sectores sensíveis. Para que a Reserva de Cibersegurança da UE funcione eficazmente, é essencial que os utilizadores e as entidades possam, sem demora, partilhar e facultar o acesso a todas as informações necessárias para que cada entidade desempenhe a sua função no contexto da avaliação dos pedidos e da implantação do apoio. Por conseguinte, o presente regulamento deverá prever que todas essas informações devem ser utilizadas ou partilhadas apenas quando tal seja necessário para o funcionamento da Reserva de Cibersegurança da UE, e que as informações confidenciais ou classificadas nos termos do direito nacional e da União só devem ser utilizadas e partilhadas em conformidade com esse direito. Além disso, os utilizadores deverão poder sempre, se for caso disso, utilizar protocolos de partilha de informações, como o TLP, para especificar em maior medida as limitações. Embora os utilizadores disponham de poder discricionário a este respeito, é importante que, ao aplicarem essas limitações, tenham em conta as possíveis consequências, em especial no que diz respeito ao atraso na avaliação ou na prestação dos serviços solicitados. A fim de dispor de uma Reserva de Cibersegurança da UE eficiente, é importante que a entidade adjudicante clarifique, junto do utilizador, essas consequências antes de este apresentar um pedido. Essas salvaguardas limitam-se ao pedido e à prestação de serviços da Reserva de Cibersegurança da UE e não afetam o intercâmbio de informações noutros contextos, como na contratação pública da Reserva de Cibersegurança da UE.

(29) Tendo em conta o aumento dos riscos e do número de incidentes que afetam os Estados-Membros, é necessário criar um instrumento de apoio a situações de crise, ou seja, o mecanismo de emergência em matéria de cibersegurança, para melhorar a resiliência da União a incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala e complementar as ações dos Estados-Membros através de apoio financeiro de emergência para a preparação, resposta a incidentes e recuperação inicial de serviços essenciais. Uma vez que a recuperação total de um incidente é um processo abrangente de restabelecimento do funcionamento da entidade afetada pelo incidente para o estado anterior àquele e pode ser um processo longo, implicando custos significativos, o apoio da Reserva de Cibersegurança da UE deverá limitar-se à fase inicial do processo de recuperação, conduzindo ao restabelecimento das funcionalidades básicas dos sistemas. O mecanismo de emergência em matéria de cibersegurança deverá permitir a mobilização rápida e eficaz 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 crises e incidentes caiba aos Estados-Membros, o mecanismo de emergência em matéria de cibersegurança promove a solidariedade entre Estados-Membros, nos termos do artigo 3.º, n.º 3, do Tratado da União Europeia (TUE).

(30) O mecanismo de emergência em matéria de cibersegurança deverá prestar apoio aos Estados-Membros em complemento das suas próprias medidas e recursos, assim como de outras opções de apoio existentes para a resposta a incidentes de cibersegurança significativos e incidentes de cibersegurança em grande escala, e para a recuperação inicial dos mesmos, como os serviços prestados pela 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, e das equipas de resposta rápida a ciberataques no âmbito da cooperação estruturada permanente (CEP) prevista pela Decisão (PESC) 2017/2315 do Conselho[15]. Deverá atender à necessidade de assegurar a disponibilidade de meios especializados para apoiar a preparação e a resposta a incidentes de cibersegurança, bem como a recuperação dos mesmos, em toda a União e nos países terceiros associados ao PED.

[15] 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 (JO L 331 de 14.12.2017, p. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) O presente regulamento não prejudica os procedimentos e regimes de coordenação da resposta a situações de crise a nível da União, em especial a Diretiva (UE) 2022/2555, o Mecanismo de Proteção Civil da União Europeia, criado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho[16], o mecanismo IPCR e a Recomendação (UE) 2017/1584 da Comissão[17]. O apoio prestado no âmbito do mecanismo de emergência em matéria de cibersegurança 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, tendo em conta o caráter civil do mecanismo de emergência em matéria de cibersegurança. O apoio prestado ao abrigo do mecanismo de emergência em matéria de cibersegurança pode complementar as ações executadas no contexto do artigo 42.º, n.º 7, do TUE, incluindo a assistência prestada por um Estado-Membro a outro Estado-Membro, ou fazer parte da resposta conjunta entre a União e os Estados-Membros, ou nas situações referidas no artigo 222.º do TFUE. A aplicação deste regulamento deverá também ser coordenada com a aplicação das medidas do conjunto de instrumentos de ciberdiplomacia, se for caso disso.

---

16 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).

17 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).

(32) A assistência prestada ao abrigo do presente regulamento deverá apoiar e complementar as ações empreendidas pelos Estados-Membros a nível nacional. Para o efeito, deverá ser assegurada uma estreita cooperação e consulta entre a Comissão, a ENISA, os Estados-Membros, e, se for caso disso, o ECCC. Ao solicitar apoio ao abrigo do mecanismo de emergência em matéria de cibersegurança, os Estado-Membros deverão prestar informações pertinentes que justifiquem a necessidade de apoio.

(33) 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 sectores, subsectores e tipos de entidade 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 emergência em matéria de cibersegurança deverá 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 dos incidentes de cibersegurança em grande escala, apoiando a recuperação inicial ou restabelecer as funcionalidades básicas dos serviços prestados por entidades que operam em sectores de importância crítica ou por entidades que operam noutros sectores críticos.

(34) 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, deverá ser prestado apoio para testar e avaliar de forma coordenada a cibersegurança das entidades que operam nos sectores de importância crítica identificados nos termos da Diretiva (UE) 2022/2555, nomeadamente por meio de exercícios e ações de formação. Para o efeito, a Comissão, depois de consultar a ENISA, o grupo de cooperação SRI e a UE-CyCLONe, deverá identificar regularmente os sectores ou subsectores pertinentes que deverão ser elegíveis para receber apoio financeiro para a realização de testes coordenados de preparação a nível da União. Os sectores ou subsectores deverão ser selecionados a partir dos sectores de importância crítica enumerados no anexo I da Diretiva (UE) 2022/2555. Os testes coordenados de preparação deverão basear-se em cenários e metodologias de risco comuns.

A seleção dos sectores e o desenvolvimento de cenários de risco deverão 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, realizada pela Comissão, pelo alto representante da União para os Negócios Estrangeiros e a Política de Segurança («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 criado pelo Regulamento (UE) 2018/1971 do Parlamento Europeu e do Conselho[18], as avaliações coordenadas a nível da União dos riscos de segurança de cadeias de abastecimento críticas 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[19]. A seleção dos sectores deverá também ter em conta a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas.

---

[18] Regulamento (UE) 2018/1971 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que cria o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE) e a Agência de Apoio ao ORECE (Gabinete do ORECE), e que altera o Regulamento (UE) 2015/2120 e revoga o Regulamento (CE) n.º 1211/2009 (JO L 321 de 17.12.2018, p. 1).

[19] 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 (JO L 333 de 27.12.2022, p. 1).

(35) Além disso, o mecanismo de emergência em matéria de cibersegurança deverá prestar apoio a outras ações de preparação e apoiar a preparação noutros sectores não abrangidos pelos testes coordenados de preparação das entidades que operam em sectores de importância crítica ou das entidades que operam noutros sectores críticos. Essas ações poderão incluir vários tipos de atividades de preparação nacionais.

(36) Quando os Estados-Membros recebam subvenções para apoiar ações de preparação, as entidades que operem em sectores de importância crítica poderão participar nessas ações a título voluntário. É boa prática que, na sequência de tais ações, as entidades participantes elaborem um plano de recuperação para aplicar quaisquer recomendações de medidas específicas daí resultantes, a fim de beneficiar plenamente da ação de preparação. Embora seja importante que os Estados-Membros solicitem, no âmbito das ações, que as entidades participantes elaborem e executem esses planos de recuperação, os Estados-Membros não são obrigados nem ficam habilitados pelo presente regulamento a executar esses pedidos. Tais pedidos não prejudicam os requisitos aplicáveis às entidades nem as competências de supervisão das autoridades competentes nos termos da Diretiva (UE) 2022/2555.

(37) O mecanismo de emergência em matéria de cibersegurança deverá também prestar apoio a ações de resposta a incidentes para atenuar o impacto de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala, apoiar a recuperação inicial 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 incidentes nos cidadãos.

(38) O mecanismo de emergência em matéria de cibersegurança deverá apoiar a assistência técnica prestada por um Estado-Membro a outro Estado-Membro que é afetado por um incidente de cibersegurança significativo ou um incidente de cibersegurança em grande escala, incluindo pelas CSIRT a que se refere o artigo 11.º, n.º 3, alínea f), da Diretiva (UE) 2022/2555. Os Estados-Membros que prestam essa assistência deverão ser autorizados a apresentar pedidos para cobrir os custos relacionados com o envio de equipas de peritos no âmbito da assistência mútua. Os custos elegíveis podem incluir as despesas de viagem, alojamento e as ajudas de custo diárias dos peritos em cibersegurança.

(39) Dado o papel essencial que as empresas privadas desempenham na deteção, preparação e resposta a incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala, é importante reconhecer o valor da cooperação voluntária *pro bono* com essas empresas, através da qual oferecem serviços não remunerados em caso de crises e de incidentes de cibersegurança em grande escala e de crises e de incidentes equivalentes a um incidente de cibersegurança em grande escala. A ENISA, em cooperação com a UE-CyCLONe, pode acompanhar a evolução dessas iniciativas *pro bono* e promover a conformidade destas com os critérios aplicáveis aos prestadores de serviços de segurança geridos de confiança ao abrigo do presente regulamento, nomeadamente no que diz respeito à fiabilidade das empresas privadas, à sua experiência, bem como à capacidade destas últimas para tratar informações sensíveis de forma segura.

(40) No âmbito do mecanismo de emergência em matéria de cibersegurança, deverá ser criada progressivamente uma Reserva de Cibersegurança da UE, composta por serviços prestados por prestadores de serviços de segurança geridos de confiança, para apoiar ações de resposta e iniciar ações de recuperação em caso de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou de incidentes equivalentes a um incidente de cibersegurança em grande escala que afetam os Estados-Membros, as instituições, órgãos ou organismos da União ou os países terceiros associados ao PED. A Reserva de Cibersegurança da UE deverá assegurar a disponibilidade e prontidão dos serviços. Por conseguinte, deverá compreender serviços previamente afetados, incluindo, por exemplo, capacidades de reserva que possam ser disponibilizadas a curto prazo. Os serviços da Reserva de Cibersegurança da UE deverão servir para apoiar as autoridades nacionais na prestação de assistência às entidades afetadas que operam em sectores de importância crítica ou às entidades afetadas que operam noutros sectores críticos em complemento das suas próprias ações a nível nacional. Os serviços da Reserva de Cibersegurança da UE deverá também poder servir para apoiar as instituições, órgãos e organismos da União em condições semelhantes. A Reserva de Cibersegurança da UE pode também contribuir para reforçar a posição concorrencial da indústria e dos serviços na União em toda a economia digital, incluindo as microempresas e as pequenas e médias empresas, bem como as empresas em fase de arranque, nomeadamente incentivando o investimento na investigação e inovação. Importa ter em conta o Quadro Europeu de Competências de Cibersegurança (ECSF) ao adquirir os serviços para a Reserva de Cibersegurança da UE. Ao solicitarem o apoio da Reserva de Cibersegurança da UE, os utilizadores deverão incluir, no seu pedido, informações adequadas sobre a entidade afetada e os potenciais impactos, informações sobre o serviço solicitado à Reserva de Cibersegurança da UE e o apoio prestado à entidade afetada a nível nacional, que deverá ser tido em conta na avaliação do pedido do requerente. A fim de assegurar a complementaridade com outras formas de apoio à disposição da entidade afetada, o pedido deverá também incluir, quando disponíveis, informações sobre as disposições contratuais em vigor relativas aos serviços de resposta a incidentes e de recuperação inicial, bem como os contratos de seguro que possam abranger esse tipo de incidente.

(41) A fim de assegurar a utilização eficaz do financiamento da União, os serviços previamente afetados ao abrigo da Reserva de Cibersegurança da UE deverão ser convertidos, em conformidade com o respetivo contrato, em serviços de preparação relacionados com a prevenção e resposta a incidentes, caso esses serviços previamente afetados não sejam utilizados para a resposta a incidentes durante o período para o qual foram previamente afetados. Esses serviços deverão ser complementares e não deverão duplicar as ações de preparação que são geridas pelo ECCC.

(42) Os pedidos de apoio ao abrigo da Reserva de Cibersegurança da UE apresentados pelas autoridades de gestão de cibercrises e pelas CSIRT dos Estados-Membros, ou pelo CERT-UE, em nome das instituições, órgãos e organismos da União, deverão ser avaliados pela entidade adjudicante. Nos casos em que a ENISA seja incumbida da administração e do funcionamento da Reserva de Cibersegurança da UE, essa entidade adjudicante é a ENISA. Os pedidos de apoio de países terceiros associados ao PED deverão ser avaliados pela Comissão. Para facilitar a apresentação e a avaliação dos pedidos de apoio, a ENISA pode criar uma plataforma segura.

(43) Caso sejam recebidos múltiplos pedidos simultâneos, estes deverão ser tratados por ordem de prioridade, em conformidade com os critérios previstos no presente regulamento. À luz dos objetivos gerais do presente regulamento, esses critérios deverão incluir a gravidade e a escala do incidente, o tipo de entidade afetada, o potencial impacto do incidente nos Estados-Membros ou nos utilizadores afetados, a potencial natureza transfronteiriça do incidente e o risco de disseminação, bem como as medidas já tomadas pelo utilizador para contribuir para a resposta e a recuperação inicial. Tendo em conta esses objetivos, e uma vez que os pedidos dos utilizadores dos Estados-Membros se destinam exclusivamente a apoiar em toda a União, entidades que operam em sectores de importância crítica ou entidades que operam noutros sectores críticos, é conveniente dar maior prioridade aos pedidos dos utilizadores dos Estados-Membros sempre que esses critérios levem a que dois ou mais pedidos sejam avaliados como iguais. Tal não prejudica as obrigações que possam recair sobre os Estados-Membros ao abrigo das convenções de acolhimento pertinentes de tomar medidas para proteger e prestar assistência às instituições, órgãos e organismos da União.

(44) A Comissão deverá assumir a responsabilidade geral pela execução da Reserva de Cibersegurança da UE. Dada a vasta experiência que adquiriu com a ação de apoio à cibersegurança, a ENISA é a agência mais adequada para executar a Reserva de Cibersegurança da UE. A Comissão deverá, por conseguinte, confiar-lhe, em parte ou, se a Comissão o considerar adequado, no todo o funcionamento e a administração da Reserva de Cibersegurança da UE. Esta incumbência deverá ser cumprida em conformidade com as regras aplicáveis ao abrigo do Regulamento (UE, Euratom) 2024/2509 e, em especial, deverá estar sujeita ao cumprimento das condições aplicáveis à assinatura de um acordo de contribuição. Quaisquer aspetos do funcionamento e da administração da Reserva de Cibersegurança da UE não confiados à ENISA deverão ser geridos diretamente pela Comissão, incluindo durante a fase que antecede a assinatura do acordo de contribuição.

(45) Os Estados-Membros deverão desempenhar um papel fundamental na constituição, implantação e pós-implantação da Reserva de Cibersegurança da UE. Uma vez que o Regulamento (UE) 2021/694 é o ato de base aplicável às ações de execução da Reserva de Cibersegurança da UE, as ações no âmbito da Reserva de Cibersegurança da UE deverão estar previstas nos programas de trabalho a que se refere o artigo 24.º do Regulamento (UE) 2021/694. Em conformidade com o n.º 6 do referido artigo, esses programas de trabalho devem ser adotados pela Comissão por meio de atos de execução pelo procedimento de exame. Além disso, a Comissão, em coordenação com o grupo de cooperação SRI, deverá definir as prioridades e a evolução da Reserva de Cibersegurança da UE.

(46) Os contratos celebrados no âmbito da Reserva de Cibersegurança da UE não deverão afetar a relação entre as empresas e as obrigações existentes entre a entidade afetada ou os utilizadores e o prestador de serviços.

(47) Para efeitos da seleção de prestadores de serviços privados para a prestação de serviços no contexto da Reserva de Cibersegurança da UE, importa definir um conjunto de critérios e requisitos mínimos que deverão ser incluídos no convite à apresentação de propostas para selecionar esses prestadores, a fim de assegurar que são satisfeitas as necessidades das autoridades dos Estados-Membros, das entidades que operam em sectores de importância crítica ou das entidades que operam noutros sectores críticos. A fim de dar resposta às necessidades específicas dos Estados-Membros, ao contratar serviços para a Reserva de Cibersegurança da UE, a entidade adjudicante deverá, se for caso disso, elaborar critérios e requisitos de seleção adicionais aos previstos no presente regulamento. É importante incentivar a participação dos prestadores de serviços de menor dimensão que operam a nível regional e local.

(48) Ao selecionar os fornecedores a incluir na Reserva de Cibersegurança da UE, a entidade adjudicante deverá diligenciar para que a Reserva de Cibersegurança da UE, no seu conjunto, compreenda fornecedores capazes de satisfazer os requisitos linguísticos dos utilizadores. Para o efeito, antes de elaborar o caderno de encargos, a entidade adjudicante deverá apurar se os potenciais utilizadores da Reserva de Cibersegurança da UE têm necessidades linguísticas específicas, de modo que os serviços de apoio da Reserva de Cibersegurança da UE possam ser prestados numa das línguas oficiais das instituições da União ou dos Estados-Membros, suscetível de ser compreendida pelo utilizador ou pela entidade afetada. Caso um utilizador necessite que os serviços de apoio da Reserva de Cibersegurança da UE sejam prestados em mais do que uma língua e que esses serviços tenham sido adquiridos nessas línguas para esse utilizador, o utilizador deverá poder especificar, no pedido de apoio ao abrigo da Reserva de Cibersegurança da UE em qual dessas línguas os serviços deverão ser prestados relativamente ao incidente específico que deu origem ao pedido.

(49) A fim de apoiar a criação da Reserva de Cibersegurança da UE, é importante que a Comissão solicite à ENISA a preparação de um projeto de sistema de certificação da cibersegurança para os serviços de segurança geridos nos termos do Regulamento (UE) 2019/881 nos domínios abrangidos pelo mecanismo de emergência em matéria de cibersegurança.

(50) A fim de apoiar os objetivos do presente regulamento de promover a partilha do conhecimento situacional, reforçar a resiliência da União e permitir uma resposta eficaz a incidentes de cibersegurança significativos e a incidentes de cibersegurança em grande escala, a Comissão ou a UE-CyCLONe deverão poder solicitar à ENISA, com o apoio da rede de CSIRT e com a aprovação dos Estados-Membros afetados, a análise e avaliação de ciberameaças, vulnerabilidades conhecidas que possam ser exploradas e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou um incidente de cibersegurança em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA deverá elaborar um relatório de análise de incidentes em colaboração com os Estados-Membros afetados e as partes interessadas pertinentes, incluindo representantes do sector privado, da Comissão e de outras instituições, órgãos e organismos competentes da União. Com base na colaboração com as partes interessadas, incluindo o sector privado, o relatório de análise de incidentes específicos deverá ter por objetivo avaliar as causas, os impactos e as medidas de atenuação de um incidente após a sua ocorrência. Deverá 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 deverá ser apresentado à UE-CyCLONe, à rede de CSIRT e à Comissão e deverá contribuir para o seu trabalho, bem como o da ENISA. Se o incidente disser respeito a um país terceiro associado ao PED, a Comissão deverá também apresentar o relatório ao alto representante.

(51) Tendo em conta a natureza imprevisível dos ciberataques 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 e a incidentes equivalentes a um incidente de cibersegurança em grande escala contribui para a proteção da União no seu conjunto, em particular do seu mercado interno e da sua indústria. Essas atividades podem contribuir ainda mais para a ciberdiplomacia da União. Por conseguinte, os países terceiros associados ao PED deverão poder solicitar apoio da Reserva de Cibersegurança da UE em todo o seu território ou parte dele sempre que tal esteja previsto no acordo através do qual o país terceiro está associado ao PED. O financiamento dos países terceiros associados ao PED deverá ser apoiado pela União no âmbito de parcerias e instrumentos de financiamento pertinentes para esses países. O apoio deverá abranger serviços no domínio da resposta a incidentes de cibersegurança significativos ou a incidentes equivalentes a um incidente de cibersegurança em grande escala e da recuperação inicial dos mesmos.

(52) Aquando da prestação de apoio aos países terceiros associados ao PED, deverão aplicar-se as condições previstas no presente regulamento relativamente à Reserva de Cibersegurança da UE e aos prestadores de serviços de segurança geridos de confiança. Os países terceiros associados ao PED deverão poder solicitar o apoio da Reserva de Cibersegurança da UE nos casos em que as entidades visadas, para as quais solicitam o apoio da Reserva de Cibersegurança da UE, sejam entidades que operam em sectores de importância crítica ou entidades que operam noutros sectores críticos e nos casos em que os incidentes detetados conduzam a perturbações operacionais significativas ou sejam suscetíveis de ter efeitos colaterais na União. Os países terceiros associados ao PED só deverão ser elegíveis para receber apoio se o acordo mediante o qual estão associados ao PED previr especificamente esse apoio. Além disso, esses países terceiros só deverão manter-se elegíveis enquanto estiverem preenchidos três critérios. Em primeiro lugar, o país terceiro deverá cumprir plenamente as condições pertinentes desse acordo. Em segundo lugar, dada a natureza complementar da Reserva de Cibersegurança da UE, o país terceiro deverá ter tomado medidas adequadas para se preparar para incidentes de cibersegurança significativos ou incidentes equivalentes a um incidente de cibersegurança em grande escala. Em terceiro lugar, a prestação de apoio ao abrigo da Reserva de Cibersegurança da UE deverá ser consonante com a política e as relações globais da União com esse país e com outras políticas da União no domínio da segurança. No contexto da sua avaliação do cumprimento desse terceiro critério, a Comissão deverá consultar o alto representante para alinhar a concessão desse apoio pela política externa e de segurança comum.

(53) A prestação de apoio aos países terceiros associados ao PED pode afetar as relações com países terceiros e a política de segurança da União, nomeadamente no contexto da política externa e de segurança comum e da política comum de segurança e defesa. Por conseguinte, é conveniente que sejam atribuídas ao Conselho competências de execução para autorizar e especificar o período durante o qual pode ser prestado esse apoio. O Conselho deverá deliberar com base numa proposta da Comissão, tendo devidamente em conta a avaliação dos três critérios, efetuada pela Comissão. O mesmo se deverá aplicar às renovações e às propostas de alteração ou revogação desses atos. Se, em circunstâncias excecionais, o Conselho considerar que houve uma alteração significativa das circunstâncias no que diz respeito ao terceiro critério, deverá poder deliberar por sua própria iniciativa para alterar ou revogar um ato de execução, sem aguardar uma proposta da Comissão. Tais alterações significativas são suscetíveis de exigir uma ação urgente, de ter implicações particularmente importantes para as relações com países terceiros e de não necessitarem de uma avaliação pormenorizada prévia da Comissão. Além disso, a Comissão deverá cooperar com o alto representante no que diz respeito aos pedidos de apoio dos países terceiros associados ao PED e à execução do apoio concedido a esses países terceiros. A Comissão deverá igualmente ter em conta os pontos de vista da ENISA relativamente a esses pedidos e apoio. A Comissão deverá informar o Conselho sobre o resultado da avaliação dos pedidos, incluindo as considerações pertinentes formuladas a esse respeito, e sobre os serviços disponibilizados.

(54) A Comunicação da Comissão de 18 de abril de 2023, sobre a Academia de Competências de Cibersegurança, reconheceu a escassez de profissionais qualificados. Essas competências são necessárias para cumprir os objetivos do presente regulamento. A União necessita urgentemente de profissionais com aptidões e competências para prevenir, detetar e dissuadir os ciberataques e defender a União, incluindo as suas infraestruturas mais críticas, contra esses ataques e assegurar a sua resiliência. Para o efeito, é importante incentivar a cooperação entre as partes interessadas, incluindo o sector privado, o meio académico e o sector público. É igualmente importante criar sinergias, em todos os territórios da União, por forma a permitir que o investimento na educação e na formação promova a criação de salvaguardas para evitar a fuga de cérebros e o agravamento do défice de competências em algumas regiões mais do que noutras. É urgente colmatar o défice de competências em matéria de cibersegurança, especialmente para reduzir as disparidades de género na mão de obra no domínio da cibersegurança, a fim de promover a presença e a participação das mulheres na conceção da governação digital.

(55) A fim de impulsionar a inovação no mercado único digital, é importante reforçar a investigação e a inovação no domínio da cibersegurança, com vista a contribuir para aumentar a resiliência dos Estados-Membros e a autonomia estratégica aberta da União, que são ambos objetivos do presente regulamento. As sinergias são essenciais para reforçar a cooperação e coordenação entre as diferentes partes interessadas, incluindo o sector privado, a sociedade civil e o meio académico.

(56) O presente regulamento deverá ter em conta o compromisso assumido na Declaração conjunta de 26 de janeiro de 2022 do Parlamento Europeu, o Conselho e a Comissão, intitulada «Declaração Europeia sobre os Direitos e Princípios Digitais para a Década Digital», de proteger os interesses das democracias, das pessoas, das empresas e das instituições públicas da União contra os riscos de cibersegurança e a cibercriminalidade, incluindo violações de dados e a usurpação ou manipulação da identidade.

(57) A fim de completar certos elementos não essenciais do presente regulamento, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão para especificar os tipos e o número de serviços de resposta necessários para a Reserva de Cibersegurança da UE. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[20]. Em especial, e a fim de assegurar a igualdade de participação na elaboração dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão incumbidos da elaboração dos atos delegados.

[20] JO L 123 de 12.5.2016, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(58) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão para especificar mais pormenorizadamente as modalidades processuais da atribuição dos serviços de apoio da Reserva de Cibersegurança da UE. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[21].

(59) Sem prejuízo das regras relativas ao orçamento anual da União ao abrigo dos Tratados, a Comissão deverá ter em conta as obrigações decorrentes do presente regulamento ao avaliar as necessidades orçamentais e de pessoal da ENISA.

(60) A Comissão deverá proceder regularmente a uma avaliação das medidas previstas no presente regulamento. A primeira avaliação deverá ser realizada nos primeiros dois anos após a data de entrada em vigor do presente regulamento e, posteriormente, pelo menos de quatro em quatro anos, tendo em conta o calendário da revisão do quadro financeiro plurianual fixado nos termos do artigo 312.º do TFUE. A Comissão deverá apresentar ao Parlamento Europeu e ao Conselho um relatório sobre os progressos realizados neste contexto. A fim de avaliar os diferentes elementos necessários, incluindo a extensão das informações partilhadas no âmbito do Sistema Europeu de Alerta em matéria de Cibersegurança, a Comissão deverá basear-se exclusivamente em informações facilmente acessíveis ou prestadas voluntariamente. Tendo em conta a evolução geopolítica e a fim de assegurar a continuidade e o desenvolvimento das medidas previstas no presente regulamento para além de 2027, é importante que a Comissão avalie a necessidade de afetar um orçamento adequado no quadro financeiro plurianual para 2028 a 2034.

---

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

(61) Atendendo a que os objetivos do presente regulamento, a saber, o reforço da posição concorrencial dos sectores da indústria e dos serviços na União em toda a economia digital e a contribuição para a soberania tecnológica e a autonomia estratégica aberta da União no domínio da cibersegurança, não podem ser suficientemente alcançados pelos Estados-Membros, mas podem, devido à dimensão ou aos efeitos da ação, ser mais bem alcançados ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrados no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir esses objetivos,

ADOTARAM O PRESENTE REGULAMENTO:

Capítulo I
Disposições gerais

Artigo 1.º

Objeto e objetivos

1. O presente regulamento prevê medidas para reforçar as capacidades da União em matéria de deteção, preparação e resposta a ciberameaças e incidentes de cibersegurança, principalmente através de:

   a) Uma rede pan-europeia de plataformas de cibersegurança (Sistema Europeu de Alerta em matéria de Cibersegurança) a fim de criar e reforçar as capacidades de deteção coordenada e de conhecimento situacional comum;

   b) Um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros na preparação, resposta, atenuação do impacto e início da recuperação de incidentes de cibersegurança significativos e de incidentes de cibersegurança em grande escala e para apoiar outros utilizadores na resposta a incidentes de cibersegurança significativos e incidentes equivalentes a um incidente de cibersegurança em grande escala;

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

2. O presente regulamento visa os objetivos gerais de reforçar a posição concorrencial da indústria e dos serviços na União na economia digital, incluindo as microempresas e as pequenas e médias empresas, bem como as empresas em fase de arranque, e de contribuir para a soberania tecnológica e a autonomia estratégica aberta da União no domínio da cibersegurança, nomeadamente através da promoção da inovação no mercado único digital. Prossegue esses objetivos através do reforço da solidariedade à escala da União, da consolidação do ecossistema de cibersegurança, do aumento da ciber-resiliência dos Estados-Membros e do desenvolvimento das aptidões, conhecimentos, capacidades e competências da mão de obra em matéria de cibersegurança.

3. Os objetivos gerais referidos no n.º 2 são atingidos através da realização dos seguintes objetivos específicos:

a) Reforçar as capacidades de deteção coordenada a nível da União e o conhecimento situacional comum relativamente a ciberameaças e incidentes de cibersegurança;

b) Aumentar o grau de preparação das entidades que operam em sectores de importância crítica ou das entidades que operam noutros sectores críticos na União e reforçar a solidariedade através do desenvolvimento de testes coordenados de preparação e de capacidades otimizadas de resposta e recuperação para fazer face a incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou incidentes equivalentes a um incidente de cibersegurança em grande escala, nomeadamente a possibilidade de disponibilizar apoio da União para resposta a incidentes de cibersegurança a países terceiros associados ao PED;

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

4. As ações no âmbito do presente regulamento são realizadas no devido respeito pelas competências dos Estados-Membros e complementam as atividades levadas a cabo pela rede de CSIRT, pela UE-CyCLONe e pelo grupo de cooperação SRI.

5. O presente regulamento não prejudica as funções do Estado essenciais dos Estados-Membros, incluindo a garantia da integridade territorial do Estado, a manutenção da ordem pública e a salvaguarda da segurança nacional. Em especial, a segurança nacional continua a ser da exclusiva responsabilidade de cada Estado-Membro.

6. A partilha ou intercâmbio de informações ao abrigo do presente regulamento que são classificadas como confidenciais nos termos das regras nacionais ou da União limita-se ao que for pertinente e proporcionado em relação ao objetivo dessa partilha ou desse intercâmbio. A referida partilha ou intercâmbio de informações deve preservar a confidencialidade das informações e salvaguardar a segurança e os interesses comerciais das entidades em causa. Não implica a prestação de informações cuja divulgação seria contrária aos interesses essenciais dos Estados-Membros em matéria de segurança nacional, segurança pública ou defesa.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Plataforma de cibersegurança transfronteiriça», uma plataforma plurinacional, criada através de um acordo de consórcio por escrito, que reúne, numa estrutura de rede coordenada, plataformas de cibersegurança nacionais de, pelo menos, três Estados-Membros, e que é concebida para otimizar a monitorização, deteção e análise de ciberameaças, prevenir incidentes e apoiar a produção de informações sobre ciberameaças, sobretudo através do intercâmbio de dados e informações pertinentes, anonimizados se for caso disso, bem como através da partilha de ferramentas de ponta e do desenvolvimento conjunto de capacidades de deteção, análise, prevenção e proteção no domínio da cibersegurança num ambiente de confiança;

2) «Consórcio de acolhimento», um consórcio composto por Estados-Membros participantes, que acordaram em criar uma plataforma de cibersegurança transfronteiriça e em contribuir para a aquisição de ferramentas, infraestruturas ou serviços, e para o funcionamento dessa plataforma;

3) «CSIRT», um CSIRT designado ou criado nos termos do artigo 10.º da Diretiva (UE) 2022/2555;

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

5) «Entidades que operam em sectores de importância crítica», os tipos de entidades enumerados no anexo I da Diretiva (UE) 2022/2555;

6) «Entidades que operam noutros sectores críticos», os tipos de entidades enumerados no anexo II da Diretiva (UE) 2022/2555;

7) «Risco», um risco na aceção do artigo 6.º, ponto 9, da Diretiva (UE) 2022/2555;

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

9) «Incidente», um incidente na aceção do artigo 6.º, ponto 6, da Diretiva (UE) 2022/2555;

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

11) «Incidente grave», um incidente grave na aceção do artigo 3.º, ponto 8, do Regulamento (UE, Euratom) 2023/2841 do Parlamento Europeu e do Conselho[22];

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

---

[22] Regulamento (UE, Euratom) 2023/2841 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União (JO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) «Incidente equivalente a um incidente de cibersegurança em grande escala», no caso das instituições, órgãos e organismos da União, um incidente grave e, no caso de países terceiros associados ao PED, um incidente que cause um nível de perturbação que excede a capacidade de resposta do país terceiro associado ao PED em causa;

14) «País terceiro associado ao PED», um país terceiro que é parte num acordo com a União que permite a sua participação no Programa Europa Digital nos termos do artigo 10.º do Regulamento (UE) 2021/694;

15) «Entidade adjudicante», a Comissão ou, na medida em que o funcionamento e a administração da Reserva de Cibersegurança da UE tenham sido confiados à ENISA nos termos do artigo 14.º, n.º 5, a ENISA;

16) «Prestador de serviços de segurança geridos», um prestador de serviços de segurança geridos na aceção do artigo 6.º, ponto 40, da Diretiva (UE) 2022/2555;

17) «Prestadores de serviços de segurança geridos de confiança», os prestadores de serviços de segurança geridos selecionados para serem incluídos na Reserva de Cibersegurança da UE em conformidade com o artigo 17.º do presente regulamento.

Capítulo II
Sistema Europeu de Alerta em matéria de Cibersegurança

Artigo 3.º

Criação do Sistema Europeu de Alerta em matéria de Cibersegurança

1. Deve ser criada uma rede pan-europeia de infraestruturas, composta por plataformas de cibersegurança nacionais e plataformas de cibersegurança transfronteiriças que adiram voluntariamente ao Sistema Europeu de Alerta em matéria de Cibersegurança a fim de apoiar o desenvolvimento de capacidades avançadas, de molde a permitir à União reforçar as capacidades de deteção, análise e tratamento de dados relacionadas com ciberameaças e a prevenção de incidentes no seu território.

2. O Sistema Europeu de Alerta em matéria de Cibersegurança deve:

   a) Contribuir para uma melhor proteção e resposta às ciberameaças, apoiando e cooperando com as entidades pertinentes e reforçando as suas capacidades, em especial as CSIRT, a rede de CSIRT, a UE-CyCLONe e as autoridades competentes designadas ou criadas nos termos do artigo 8.º, n.º 1, da Diretiva (UE) 2022/2555;

   b) Mutualizar dados e informações pertinentes sobre ciberameaças e incidentes de cibersegurança provenientes de várias fontes no âmbito das plataformas de cibersegurança transfronteiriças e partilhar informações analisadas ou agregadas através de plataformas de cibersegurança transfronteiriças, se for caso disso com a rede de CSIRT;

c) Recolher e apoiar a produção de informações de alta qualidade e utilizáveis e de informações sobre ciberameaças através da utilização de ferramentas de ponta e de tecnologias avançadas, e partilhar essas informações;

d) Contribuir para o reforço da deteção coordenada das ciberameaças e para o conhecimento situacional comum na União, bem como para a emissão de alertas, nomeadamente, se for caso disso, apresentando recomendações concretas às entidades;

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

3. As ações de execução do Sistema Europeu de Alerta em matéria de Cibersegurança são apoiadas por financiamento do Programa Europa Digital (PED) e executadas nos termos do Regulamento (UE) 2021/694, em especial, com o objetivo específico n.º 3 do mesmo regulamento.

Artigo 4.º

Plataformas de cibersegurança nacionais

1. Caso um Estado-Membro decida participar no Sistema Europeu de Alerta em matéria de Cibersegurança, deve designar ou, se for caso disso, criar uma plataforma de cibersegurança nacional para efeitos do presente regulamento.

2. A plataforma de cibersegurança nacional é uma entidade única que atua sob a autoridade de um Estado-Membro. Pode ser uma CSIRT ou, se for caso disso, uma autoridade nacional de gestão de cibercrises ou outra autoridade competente designada ou criada nos termos do artigo 8.º, n.º 1, da Diretiva (UE) 2022/2555, ou outra entidade. A plataforma de cibersegurança nacional deve:

   a) Ter 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 ciberameaças e incidentes de cibersegurança e contribuir para a plataforma de cibersegurança transfronteiriça a que se refere o artigo 5.º; e

   b) Ser capaz de detetar, agregar e analisar dados e informações relevantes em matéria de ciberameaças e incidentes de cibersegurança, como a informação sobre ciberameaças, utilizando, em especial, tecnologias de ponta e visando prevenir incidentes.

3. No âmbito das funções referidas no n.º 2 do presente artigo, as plataformas de cibersegurança nacionais podem cooperar com entidades do sector privado no intercâmbio de dados e informações pertinentes para efeitos de deteção e prevenção de ciberameaças e incidentes de cibersegurança, incluindo com comunidades sectoriais e intersectoriais de entidades essenciais e importantes como referido no artigo 3.º da Diretiva (UE) 2022/2555. Se for caso disso, e em conformidade com o direito nacional e da União, as informações solicitadas ou recebidas pelas plataformas de cibersegurança nacionais podem incluir dados de telemetria, sensores e registos.

4. Um Estado-Membro selecionado nos termos do artigo 9.º, n.º 1, deve comprometer-se a candidatar-se para que a sua plataforma de cibersegurança nacional participe numa plataforma de cibersegurança transfronteiriça.

Artigo 5.º

Plataformas de cibersegurança transfronteiriças

1. Se, pelo menos, três Estados-Membros estiverem empenhados em assegurar que as suas plataformas de cibersegurança nacionais trabalhem em conjunto para coordenar as respetivas atividades de ciberdeteção e monitorização de ameaças, tais Estados-Membros podem criar um consórcio de acolhimento para efeitos do presente regulamento.

2. Um consórcio de acolhimento é composto por, pelo menos, três Estados-Membros participantes que tenham acordado em criar e contribuir para a aquisição de ferramentas, infraestruturas ou serviços para uma plataforma de cibersegurança transfronteiriça, e para o seu funcionamento nos termos do n.º 4.

3. Caso um consórcio de acolhimento seja selecionado em conformidade com o artigo 9.º, n.º 3, os seus membros devem celebrar, por escrito, um acordo de consórcio que:

   a) Defina as disposições internas para a execução da convenção de acolhimento e utilização a que se refere o artigo 9.º, n.º 3;

   b) Crie a plataforma de cibersegurança transfronteiriça do consórcio de acolhimento; e

   c) Inclua as cláusulas específicas exigidas nos termos do artigo 6.º, n.ºs 1 e 2.

4. Uma plataforma de cibersegurança transfronteiriça é uma plataforma plurinacional criada por um acordo de consórcio por escrito, tal como referido no n.º 3. Reúne, numa estrutura de rede coordenada, as plataformas de cibersegurança nacionais dos Estados-Membros do consórcio de acolhimento. É concebida para otimizar a monitorização, a deteção e a análise de ciberameaças, prevenir incidentes e apoiar a produção de informações em matéria de ciberameaças, designadamente através do intercâmbio de dados e informações pertinentes, anonimizados se for caso disso, bem como da partilha de ferramentas de ponta e do desenvolvimento conjunto de capacidades de deteção, análise, prevenção e proteção no domínio da cibersegurança num ambiente de confiança.

5. Para efeitos jurídicos, uma plataforma de cibersegurança transfronteiriça é representada por um membro do consórcio de acolhimento correspondente que atue como coordenador ou pelo consórcio de acolhimento, se este último tiver personalidade jurídica. A responsabilidade pela conformidade da plataforma de cibersegurança transfronteiriça com o presente regulamento e a convenção de acolhimento e utilização é atribuída no acordo de consórcio por escrito a que se refere o n.º 3.

6. Um Estado-Membro pode aderir a um consórcio de acolhimento existente com o acordo dos membros desse consórcio de acolhimento. O acordo de consórcio por escrito referido no n.º 3 e a convenção de acolhimento e utilização devem ser alterados em conformidade. Tal não afeta os direitos de propriedade do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC, na sigla em inglês) sobre as ferramentas, infraestruturas ou serviços já adquiridos em conjunto com esse consórcio de acolhimento.

Artigo 6.º

Cooperação e partilha de informações entre as plataformas de cibersegurança transfronteiriças e no âmbito das mesmas

1. Os membros de um consórcio de acolhimento asseguram que, em conformidade com o acordo de consórcio escrito a que se refere o artigo 5.º, n.º 3, as suas plataformas de cibersegurança nacionais partilham entre si, no âmbito da plataforma de cibersegurança transfronteiriça, informações pertinentes, anonimizados se for caso disso, como por exemplo 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) Promova e otimize a deteção de ciberameaças e reforce as capacidades da rede de CSIRT para evitar e responder a incidentes ou atenuar o seu impacto;

   b) Reforce o nível de cibersegurança, por exemplo 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, 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, determina:

a) O compromisso de partilhar entre os membros do consórcio de acolhimento as informações referidas no n.º 1, bem como as condições em que esses dados e essas informações devem ser partilhadas.

b) Um modelo de governação que clarifique e incentive a partilha por todos os participantes de informações pertinentes, anonimizados se for caso disso, a que se refere o n.º 1;

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

O acordo de consórcio por escrito pode especificar que as informações referidas no n.º 1 devem ser partilhadas em conformidade com o direito nacional e da União.

3. As plataformas de cibersegurança transfronteiriças celebram acordos de cooperação entre si, especificando os princípios de partilha de informações e a interoperabilidade entre as plataformas de cibersegurança transfronteiriças. As plataformas de cibersegurança transfronteiriças informam a Comissão sobre os acordos de cooperação celebrados.

4. A partilha de informações a que se refere o n.º 1 entre as plataformas de cibersegurança transfronteiriças é assegurada por um elevado nível de interoperabilidade. Por forma a apoiar essa interoperabilidade, a ENISA, em estreita consulta com a Comissão, emite, sem demora injustificada e o mais tardar em … [12 meses após a data de entrada em vigor do presente regulamento], orientações em matéria de interoperabilidade que especifiquem, em especial, os formatos e protocolos de partilha de informações, tendo em conta as normas internacionais e as boas práticas, bem como o funcionamento das plataformas de cibersegurança transfronteiriças estabelecidas. Os requisitos de interoperabilidade previstos nos acordos de cooperação das plataformas de cibersegurança transfronteiriças devem basear-se nas orientações emitidas pela ENISA.

Artigo 7.º

Cooperação e partilha de informações com redes à escala da União

1. As plataformas de cibersegurança transfronteiriças e a rede de CSIRT cooperam estreitamente, em especial com o objetivo de partilhar informações. Para o efeito, acordam disposições processuais em matéria de cooperação e partilha de informações pertinentes e, sem prejuízo do disposto no n.º 2, os tipos de informações a partilhar.

2. Caso obtenham informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, as plataformas de cibersegurança transfronteiriças devem assegurar, sem demora injustificada, para efeitos de conhecimento situacional comum, que são prestadas informações pertinentes, bem como alertas precoces, às autoridades dos Estados-Membros e à Comissão através da UE-CyCLONe e da rede de CSIRT.

Artigo 8.º

Segurança

1. Os Estados-Membros que participam no Sistema Europeu de Alerta em matéria de Cibersegurança devem assegurar um elevado nível de cibersegurança, nomeadamente confidencialidade e segurança dos dados, bem como de segurança física da infraestrutura do Sistema Europeu de Alerta em matéria de Cibersegurança, e assegurar que a rede 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 e das informações partilhados através da rede.

2. Os Estados-Membros que participam no Sistema Europeu de Alerta em matéria de Cibersegurança devem assegurar que a partilha de informações a que se refere o artigo 6.º, n.º 1, no âmbito do Sistema Europeu de Alerta em matéria de Cibersegurança com qualquer entidade que não seja uma autoridade ou organismo público de um Estado-Membro, não afeta negativamente os interesses de segurança da União ou dos Estados-Membros.

Artigo 9.º

Financiamento do Sistema Europeu de Alerta em matéria de Cibersegurança

1. Na sequência de um convite à manifestação de interesse dos Estados-Membros que pretendam participar no Sistema Europeu de Alerta em matéria de Cibersegurança, o ECCC seleciona os Estados-Membros que com ele participam na contratação pública conjunta de ferramentas, infraestruturas ou serviços, com o objetivo de criar, ou reforçar, as capacidades das plataformas de cibersegurança nacionais designadas ou criadas nos termos do artigo 4.º, n.º 1. O ECCC pode conceder aos Estados-Membros selecionados subvenções para financiar o funcionamento dessas ferramentas, infraestruturas ou serviços. A contribuição financeira da União cobre até 50 % dos custos de aquisição das ferramentas, infraestruturas ou serviços, e até 50 % dos custos operacionais. Os Estados-Membros selecionados cobrem os restantes custos. Antes de lançar o procedimento de aquisição das ferramentas, infraestruturas ou serviços, o ECCC e os Estados-Membros selecionados devem celebrar uma convenção de acolhimento e utilização que regule a utilização das ferramentas, infraestruturas ou serviços.

2. Se a plataforma de cibersegurança nacional de um Estado-Membro não participar numa plataforma de cibersegurança transfronteiriça no prazo de dois anos a contar da data de aquisição das ferramentas, infraestruturas ou serviços ou da data em que recebeu financiamento através de subvenções, consoante o que ocorrer primeiro, não é elegível para apoio adicional da União ao abrigo do presente capítulo até se juntar a uma plataforma de cibersegurança transfronteiriça.

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

4. O ECCC prepara, pelo menos de dois em dois anos, um levantamento das ferramentas, infraestruturas ou serviços necessários e de qualidade adequada para criar ou reforçar as capacidades das plataformas de cibersegurança nacionais e das plataformas de cibersegurança transfronteiriças, bem como a sua disponibilidade, nomeadamente de entidades jurídicas estabelecidas ou consideradas estabelecidas nos Estados-Membros e controladas pelos Estados-Membros ou por nacionais dos Estados-Membros. Ao preparar o levantamento, o ECCC consulta a rede de CSIRT, as plataformas de cibersegurança transfronteiriças existentes, a ENISA e a Comissão.

Capítulo III

Mecanismo de emergência em matéria de cibersegurança

Artigo 10.º

Criação do mecanismo de emergência em matéria de cibersegurança

1. É criado um mecanismo de emergência em matéria de cibersegurança para apoiar a melhoria da resiliência da União a ciberameaças e para preparar e atenuar, num espírito de solidariedade, o impacto a curto prazo de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala.

2. No caso dos Estados-Membros, as ações no âmbito do mecanismo de emergência em matéria de cibersegurança são realizadas mediante pedido e complementam os esforços e medidas dos Estados-Membros para preparar, responder e recuperar de incidentes.

3. As ações de execução do mecanismo de emergência em matéria de cibersegurança são apoiadas por financiamento do PED e executadas em conformidade com o Regulamento (UE) 2021/694, em especial, com o objetivo específico n.º 3 do mesmo regulamento.

4. As ações no âmbito do mecanismo de emergência em matéria de cibersegurança são executadas principalmente através do ECCC, nos termos do Regulamento (UE) 2021/887. No entanto, as medidas que executam a Reserva de Cibersegurança da UE a que se refere o artigo 11.º, alínea b), do presente regulamento são executadas pela Comissão e pela ENISA.

Artigo 11.º

Tipos de ações

O mecanismo de emergência em matéria de cibersegurança apoia os seguintes tipos de ações:

a) Ações de preparação, a saber:

i) testes coordenados de preparação das entidades que operam em sectores de importância crítica em toda a União, tal como especificado no artigo 12.º,

ii) outras ações de preparação para entidades que operam em sectores de importância crítica ou entidades que operam noutros sectores críticos, tal como especificado no artigo 13.º;

b) Ações de apoio à resposta e para iniciar a recuperação de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala e incidentes equivalentes a um incidente de cibersegurança em grande escala, a concretizar por prestadores de serviços de segurança geridos de confiança que participem na Reserva de Cibersegurança da UE criada nos termos do artigo 14.º;

c) Ações de apoio à assistência mútua, como referido no artigo 18.º.

Artigo 12.º

Testes coordenados de preparação das entidades

1. O mecanismo de emergência em matéria de cibersegurança apoia os testes voluntários e coordenados de preparação das entidades que operam em sectores de importância crítica.

2. Os testes coordenados de preparação podem consistir em atividades de preparação, como testes de penetração e a avaliação da ameaça.

3. O apoio às ações de preparação no âmbito do presente artigo é prestado aos Estados-Membros principalmente sob a forma de subvenções e sujeito às condições previstas nos programas de trabalho pertinentes referidos no artigo 24.º do Regulamento (UE) 2021/694.

4. A fim de apoiar os testes coordenados de preparação das entidades a que se refere o artigo 11.º, alínea a), subalínea i), do presente regulamento na União, a Comissão, após consulta ao grupo de cooperação SRI, a UE-CyCLONe e a ENISA, identifica os sectores ou subsectores em causa com base nos sectores de importância crítica enumerados no anexo I da Diretiva (UE) 2022/2555, para os quais pode ser lançado um convite à apresentação de propostas. A participação dos Estados-Membros nesses convites à apresentação de propostas é voluntária.

5. Ao identificar os sectores ou subsectores referidos no n.º 4, a Comissão tem em conta as avaliações coordenadas dos riscos e os testes de resiliência à escala da União, bem como os respetivos resultados.

6. O grupo de cooperação SRI, em cooperação com a Comissão, o alto representante da União para os Negócios Estrangeiros e a Política de Segurança («alto representante») e a ENISA, e, no âmbito do seu mandato, a UE-CyCLONe, devem desenvolver cenários e metodologias de risco comuns para os exercícios de teste coordenados de preparação a que se refere o 11.º, alínea a), subalínea i), e, se for caso disso, para outras ações de preparação referidas na alínea a), subalínea ii) desse artigo.

7. Caso uma entidade que opera num sector de importância crítica participe voluntariamente em testes coordenados de preparação e desses testes resultarem recomendações de medidas específicas que a entidade participante possa integrar num plano de recuperação, a autoridade do Estado-Membro responsável pelos testes coordenados de preparação deve, se for caso disso, rever o seguimento dado a essas medidas pelas entidades participantes, com vista a reforçar o grau de preparação.

Artigo 13.º

Outras ações de preparação

1. O mecanismo de emergência em matéria de cibersegurança apoia ações de preparação não abrangidas pelo artigo 12.º. Essas ações devem incluir ações de preparação das entidades em sectores não identificados para testes coordenados de preparação nos termos do artigo 12.º. Essas ações podem apoiar a monitorização das vulnerabilidades, a monitorização dos riscos, exercícios e ações de formação.

2. O apoio às ações de preparação no âmbito do presente artigo é prestado aos Estados-Membros mediante pedido e principalmente sob a forma de subvenções e sujeito às condições previstas nos programas de trabalho pertinentes referidos no artigo 24.º do Regulamento (UE) 2021/694.

Artigo 14.º

Criação da Reserva de Cibersegurança da UE

1. É criada uma Reserva de Cibersegurança da UE, a fim de, mediante pedido, ajudar os utilizadores a que se refere o n.º 3 a responder ou a prestar apoio para responder a incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou incidentes equivalentes a um incidente de cibersegurança em grande escala e para iniciar a recuperação desses mesmos incidentes.

2. A Reserva de Cibersegurança da UE é constituída por serviços de resposta de prestadores de serviços de segurança geridos de confiança selecionados de acordo com os critérios previstos no artigo 17.º, n.º 2. A Reserva de Cibersegurança da UE pode incluir serviços previamente afetados. Os serviços previamente afetados de um prestador de serviços de segurança geridos de confiança devem ser convertíveis em serviços de preparação relacionados com a prevenção e resposta a incidentes, quando esses serviços não sejam utilizados para a resposta a incidentes durante o período em que estão previamente afetados. A Reserva de Cibersegurança da UE pode ser disponibilizada, mediante pedido, em todos os Estados-Membros, instituições, órgãos e organismos da União e nos países terceiros associados ao PED a que se refere o artigo 19.º, n.º 1.

3. Os utilizadores dos serviços da Reserva de Cibersegurança da UE consistem no seguinte:

a) As 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) O CERT-UE, nos termos do artigo 13.º do Regulamento (UE, Euratom) 2023/2841;

c) Autoridades competentes, tais como as equipas de resposta a incidentes de segurança informática e autoridades de gestão de cibercrises de países terceiros associados ao PED, nos termos do artigo 19.º, n.º 8.

4. 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 articulação com o grupo de cooperação SRI e, 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 no âmbito do presente regulamento, bem como com outras ações e programas da União. Essas prioridades são reexaminadas e, se aplicável, revistas de dois em dois anos. A Comissão informa o Parlamento Europeu e o Conselho sobre essas prioridades e as respetivas revisões.

5. Sem prejuízo da responsabilidade global da Comissão pela execução da Reserva de Cibersegurança da UE a que se refere o n.º 4 do presente artigo e sob reserva de um acordo de contribuição, na aceção do artigo 2.º, ponto 19, do Regulamento (UE, Euratom) 2024/2509, a Comissão confia o funcionamento e a administração da Reserva de Cibersegurança da UE, no todo ou em parte, à ENISA. Os aspetos não confiados à ENISA continuam a ser objeto de gestão direta pela Comissão.

6. A ENISA prepara, pelo menos de dois em dois anos, um levantamento dos serviços necessários aos utilizadores a que se refere o n.º 3, alíneas a) e b), do presente artigo. O levantamento inclui também a disponibilidade desses serviços, nomeadamente de entidades jurídicas estabelecidas ou consideradas como estando estabelecidas nos Estados-Membros e controladas pelos Estados-Membros ou por nacionais dos Estados-Membros. Ao proceder ao levantamento dessa disponibilidade, a ENISA avalia as competências e a capacidade da mão de obra da União no domínio da cibersegurança que sejam pertinentes para os objetivos da Reserva de Cibersegurança da UE. Ao preparar o levantamento, a ENISA consulta o grupo de cooperação SRI, a UE-CyCLONe, a Comissão e, se aplicável, o Conselho Interinstitucional para a Cibersegurança criado pelo artigo 10.º do Regulamento (UE, Euratom) 2023/2841 (IICB, do inglês *Interinstitutional Cybersecurity Board*). Ao proceder ao levantamento da disponibilidade de serviços, a ENISA consulta também as partes interessadas pertinentes do sector da cibersegurança, incluindo os prestadores de serviços de segurança geridos. A ENISA prepara um levantamento semelhante, após informar o Conselho e consultar a UE-CyCLONe, a Comissão e, se for caso disso, o alto representante, a fim de identificar as necessidades dos utilizadores a que se refere o n.º 3, alínea c), do presente artigo.

7. A Comissão fica habilitada a adotar atos delegados, nos termos do artigo 23.º, para completar o presente regulamento, especificando os tipos e o número de serviços de resposta necessários para a Reserva de Cibersegurança da UE. Ao preparar esses atos delegados, a Comissão tem em conta o levantamento a que se refere o n.º 6 do presente artigo e pode proceder ao intercâmbio de aconselhamentos e cooperar com o grupo de cooperação SRI e a ENISA.

Artigo 15.º

Pedidos de apoio ao abrigo da Reserva de Cibersegurança da UE

1. Os utilizadores a que se refere o artigo 14.º, n.º 3, podem solicitar serviços à Reserva de Cibersegurança da UE para apoiar a resposta e iniciar a recuperação de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou incidentes equivalentes a um incidente de cibersegurança em grande escala.

2. Para receberem apoio da Reserva de Cibersegurança da UE, os utilizadores a que se refere o artigo 14.º, n.º 3, devem tomar todas as medidas adequadas para atenuar os efeitos do incidente para o qual o apoio é solicitado, incluindo, se for caso disso, a prestação de assistência técnica direta e outros recursos para apoiar a resposta ao incidente e os esforços de recuperação.

3. Os pedidos de apoio são transmitidos à entidade adjudicante da seguinte forma:

   a) No caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea a), do presente regulamento, através do ponto de contacto único designado ou criado pelo Estado-Membro nos termos do artigo 8.º, n.º 3, da Diretiva (UE) 2022/2555;

b) No caso do utilizador a que se refere o artigo 14.º, n.º 3, alínea b) por esse utilizador;

c) No caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea c), através do ponto de contacto único a que se refere o artigo 19.º, n.º 9.

4. No caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea a), os Estados-Membros informam a rede de CSIRT e, se for caso disso, a UE-CyCLONe sobre os pedidos dos seus utilizadores de apoio para resposta a incidentes e início da recuperação nos termos do presente artigo.

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

a) Informações adequadas sobre a entidade afetada e potenciais impactos do incidente nas seguintes entidades:

i) no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea a), os Estados-Membros e os utilizadores afetados, incluindo o risco de disseminação para outro Estado-Membro,

ii) no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea b), as instituições, órgãos ou organismos da União afetados,

iii) no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea c), os países terceiros associados ao PED afetados;

b) Informações sobre o serviço solicitado, juntamente com a utilização prevista do apoio solicitado, nomeadamente uma indicação das necessidades estimadas;

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

d) Se pertinente, informações disponíveis sobre outras formas de apoio à disposição da entidade afetada.

6. A ENISA, em colaboração com a Comissão e a UE-CyCLONe, 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 processuais relativas à forma como os serviços de apoio da Reserva de Cibersegurança da UE são solicitados e à forma como esses pedidos devem ser respondidos nos termos do presente artigo, do artigo 16.º, n.º 1, e do artigo 19.º, n.º 10, incluindo as modalidades de apresentação desses pedidos e de apresentação das respostas e dos modelos para os relatórios a que se refere o artigo 16.º, n.º 9. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 24.º, n.º 2.

Artigo 16.º

Execução do apoio da Reserva de Cibersegurança da UE

1. No caso dos pedidos dos utilizadores a que se refere o artigo 14.º, n.º 3, alíneas a) e b), os pedidos de apoio da Reserva de Cibersegurança da UE são avaliados pela entidade adjudicante. Deve ser transmitida uma resposta aos utilizadores a que se refere o artigo 14.º, n.º 3, alíneas a) e b), sem demora e, em qualquer caso, no prazo máximo de 48 horas a contar da apresentação do pedido, a fim de assegurar a efetividade de apoio. A entidade adjudicante informa o Conselho e a Comissão dos resultados do processo.

2. No que diz respeito às informações partilhadas durante o pedido e a prestação dos serviços da Reserva de Cibersegurança da UE, todas as partes envolvidas na aplicação do presente regulamento devem:

   a) Limitar a utilização e a partilha dessas informações ao necessário para o cumprimento das suas obrigações ou funções nos termos do presente regulamento;

   b) Utilizar e partilhar quaisquer informações confidenciais ou classificadas nos termos do direito nacional ou da União apenas em conformidade com esse direito; e

   c) Assegurar um intercâmbio de informações eficaz, eficiente e seguro, utilizando e respeitando, se for caso disso, os protocolos de partilha de informações pertinentes, designadamente o protocolo «sinalização luminosa» (TLP, na sigla em inglês).

3. Ao avaliar os pedidos individuais nos termos do artigo 16.º, n.º 1, e do artigo 19.º, n.º 10, a entidade adjudicante ou a Comissão, consoante o caso, avalia, em primeiro lugar, se estão preenchidos os critérios referidos no artigo 15.º, n.os 1 e 2. Se for esse o caso, deve avaliar a duração e a natureza do apoio adequado, tendo em conta o objetivo referido no artigo 1.º, n.º 3, alínea b), e, se for caso disso, os seguintes critérios:

a) A escala e a gravidade do incidente;

b) O tipo de entidade afetada, dando maior prioridade aos incidentes que afetem entidades essenciais como referido no artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555;

c) O potencial impacto do incidente nos Estados-Membros, nas instituições, órgãos ou organismos da União, ou nos países terceiros associados ao PED afetados;

d) A potencial natureza transfronteiriça do incidente e o risco de disseminação para outros Estados-Membros, instituições, órgãos ou organismos da União ou países terceiros associados ao PED;

e) As medidas tomadas pelo utilizador para apoiar a resposta e os esforços para iniciar a recuperação, conforme referido no artigo 15.º, n.º 2.

4. Para determinar a prioridade dos pedidos, no caso de pedidos concorrentes dos utilizadores a que se refere o artigo 14.º, n.º 3, os critérios a que se refere o n.º 3 do presente artigo devem ser tidos em conta, se for caso disso, sem prejuízo do princípio da cooperação leal entre os Estados-Membros e as instituições, órgãos e organismos da União. Se dois ou mais pedidos forem avaliados como iguais nos termos desses critérios, deve ser dada maior prioridade aos pedidos dos utilizadores dos Estados-Membros. Caso o funcionamento e a administração da Reserva de Cibersegurança da UE tenham sido confiados, no todo ou em parte, à ENISA nos termos do artigo 14.º, n.º 5, a ENISA e a Comissão cooperam estreitamente para determinar a prioridade dos pedidos em conformidade com o presente número.

5. Os serviços da Reserva de Cibersegurança da UE são prestados em conformidade com acordos específicos entre o prestador de serviços de segurança geridos de confiança e o utilizador ao qual é prestado apoio ao abrigo da Reserva de Cibersegurança da UE. Esses serviços podem ser prestados em conformidade com acordos específicos entre o prestador de serviços de segurança geridos de confiança, o utilizador e a entidade afetados. Todos os acordos referidos no presente número incluem, nomeadamente, condições de responsabilidade.

6. Os acordos a que se refere o n.º 5 baseiam-se em modelos elaborados pela ENISA, após consulta aos Estados-Membros e, se adequado, a outros utilizadores da Reserva de Cibersegurança da UE.

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

8. Os utilizadores só podem utilizar os serviços da Reserva de Cibersegurança da UE prestados em resposta a um pedido nos termos do artigo 15.º, n.º 1, para apoiar a resposta e iniciar a recuperação de incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou incidentes equivalentes a um incidente de cibersegurança em grande escala. Só podem utilizar esses serviços em relação a:

   a) Entidades que operam em sectores de importância crítica ou entidades que operam noutros sectores críticos, no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea a), e entidades equivalentes no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea c); e

   b) Instituições, órgãos e organismos da União, no caso do utilizador a que se refere o artigo 14.º, n.º 3, alínea b).

9. No prazo de dois meses a contar do termo de um apoio, os utilizadores que tenham recebido apoio apresentam um relatório de síntese sobre o serviço prestado, os resultados obtidos e os ensinamentos retirados:

   a) À Comissão, à ENISA, à rede de CSIRT e à UE-CyCLONe no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea a);

   b) À Comissão, à ENISA e ao Conselho Interinstitucional para a Cibersegurança no caso do utilizador a que se refere o artigo 14.º, n.º 3, alínea b);

c) À Comissão no caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea c).

A Comissão transmite ao Conselho e ao alto representante todos os relatórios de síntese recebidos dos utilizadores a que se refere o artigo 14.º, n.º 3, nos termos do primeiro parágrafo, alínea c), do presente número.

10. Caso o funcionamento e a administração da Reserva de Cibersegurança da UE tenham sido confiados, no todo ou em parte, à ENISA nos termos do artigo 14.º, n.º 5, do presente regulamento, a ENISA informa e consulta a Comissão regularmente a esse respeito. Nesse contexto, a ENISA envia imediatamente à Comissão quaisquer pedidos que receba dos utilizadores referidos no artigo 14.º, n.º 3, alínea c), do presente regulamento, e, se necessário para efeitos de determinação de prioridades ao abrigo do presente artigo, quaisquer pedidos que tenha recebido dos utilizadores referidos no artigo 14.º, n.º 3, alínea a) ou alínea b), do presente regulamento. As obrigações previstas no presente número não prejudicam o disposto no artigo 14.º do Regulamento (UE) 2019/881.

11. No caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alíneas a) e b), a entidade adjudicante informa o grupo de cooperação SRI regularmente e, pelo menos, duas vezes por ano sobre a utilização e os resultados do apoio.

12. No caso dos utilizadores a que se refere o artigo 14.º, n.º 3, alínea c), a Comissão apresenta um relatório ao Conselho e informa o alto representante regularmente e, pelo menos, duas vezes por ano sobre a utilização e os resultados do apoio.

Artigo 17.º

Prestadores de serviços de segurança geridos de confiança

1. Nos procedimentos de contratação pública para efeitos da criação da Reserva de Cibersegurança da UE, a entidade adjudicante age de acordo com os princípios previstos no Regulamento (UE, Euratom) 2024/2509 e com os seguintes princípios:

   a) Assegurar que os serviços incluídos na Reserva de Cibersegurança da UE, no seu conjunto, sejam de molde a permitir que a Reserva de Cibersegurança da UE inclua serviços que podem ser disponibilizados em todos os Estados-Membros, tendo em conta, em especial, os requisitos nacionais para a prestação desses serviços, incluindo os relativos às línguas, à certificação ou à 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 à União valor acrescentado, contribuindo para a consecução dos objetivos determinados no artigo 3.º do Regulamento (UE) 2021/694, incluindo a promoção do desenvolvimento de competências em matéria de cibersegurança na União.

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

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 e continuidade dos conhecimentos especializados, bem como os recursos técnicos necessários;

b) O prestador e quaisquer filiais e subcontratantes relevantes devem cumprir as regras aplicáveis em matéria de proteção das informações classificadas e devem dispor de medidas adequadas, incluindo, se for caso disso, acordos entre si, para proteger as informações confidenciais relacionadas com o serviço e, em especial, elementos de prova, conclusões e relatórios;

c) O prestador deve apresentar 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, quando tal seja exigido pelo Estado-Membro;

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

f) O prestador deve estar equipado com o *hardware* e o *software* necessários para apoiar o serviço solicitado, que não devem conter vulnerabilidades conhecidas que possam ser exploradas, devem ter as últimas atualizações de segurança e, em qualquer caso, devem cumprir todas as disposições aplicáveis do Regulamento (UE) 2024/… do Parlamento Europeu e do Conselho[23+];

g) O prestador deve ser capaz de demonstrar que possui experiência na prestação de serviços semelhantes às autoridades nacionais competentes, às entidades que operam em sectores de importância crítica ou às entidades que operam noutros sectores críticos;

h) O prestador deve ser capaz de prestar o serviço num curto espaço de tempo nos Estados-Membros onde pode prestar o serviço;

i) O prestador deve poder prestar o serviço numa ou mais línguas oficiais das instituições da União ou de um Estado-Membro, conforme exigido, se for caso disso, pelos Estados-Membros ou pelos utilizadores referidos no artigo 14.º, n.º 3, alíneas b) e c), onde o prestador pode prestar o serviço;

j) Quando estiver em vigor um sistema europeu de certificação da cibersegurança para os serviços de segurança geridos nos termos do Regulamento (UE) 2019/881, o prestador deve obter certificação em conformidade com esse sistema, no prazo de dois anos a contar da entrada de aplicação do sistema;

---

[23] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho, de ..., relativo ... (JO L, …, ELI: …).

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 100/23 (2022/0272(COD)) e inserir na nota de rodapé o número, a data, o título, a referência do JO e a referência ELI desse regulamento.

k) O prestador de serviços deve incluir no concurso as condições de conversão para qualquer serviço de resposta a incidentes não utilizado que possa ser convertido em serviços de preparação estreitamente relacionados com a resposta a incidentes, como exercícios ou ações de formação.

3. Para efeitos de contratação de serviços para a Reserva de Cibersegurança da UE, a entidade adjudicante pode, se for caso disso, desenvolver critérios e requisitos além dos referidos no n.º 2, em estreita cooperação com os Estados-Membros.

Artigo 18.º

Ações de apoio à assistência mútua

1. O mecanismo de emergência em matéria de cibersegurança deve apoiar a assistência técnica prestada por um Estado-Membro a outro Estado-Membro afetado por um incidente de cibersegurança significativo ou um incidente de cibersegurança em grande escala, incluindo nos casos a que se refere o artigo 11.º, n.º 3, alínea f), da Diretiva (UE) 2022/2555.

2. O apoio à assistência técnica mútua referido no n.º 1 do presente artigo é prestado sob a forma de subvenções e sujeito às condições previstas nos programas de trabalho pertinentes referidos no artigo 24.º do Regulamento (UE) 2021/694.

Artigo 19.º

Apoio a países terceiros associados ao PED

1. Um país terceiro associado ao PED pode solicitar apoio da Reserva de Cibersegurança da UE sempre que o acordo, através do qual está associado ao PED, preveja a participação na Reserva de Cibersegurança da UE. Esse acordo deve incluir disposições que exijam que o país terceiro associado ao PED em causa cumpra as obrigações previstas nos n.ºs 2 e 9 do presente artigo. Para efeitos da participação de um país terceiro na Reserva de Cibersegurança da UE, a associação parcial de um país terceiro ao PED pode incluir uma associação limitada ao objetivo operacional a que se refere o artigo 6.º, n.º 1, alínea g), do Regulamento (UE) 2021/694.

2. No prazo de três meses a contar da data de celebração do acordo a que se refere o n.º 1 e, em todo o caso, antes de receberem qualquer apoio da Reserva de Cibersegurança da UE, o país terceiro associado ao PED deve facultar à Comissão informações sobre a sua ciber-resiliência e a sua capacidade de gestão de riscos, incluindo, pelo menos, informações sobre as medidas nacionais tomadas para se preparar para incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou incidentes equivalentes a um incidente de cibersegurança em grande escala, bem como informações sobre as entidades nacionais responsáveis, incluindo as equipas de resposta a incidentes de segurança informática ou entidades equivalentes, a suas capacidades e os recursos que lhes são afetados. O país terceiro associado ao PED deve disponibilizar atualizações dessas informações regularmente e, pelo menos, uma vez por ano. A Comissão disponibiliza essas informações ao alto representante e à ENISA, a fim de facilitar a aplicação do n.º 11.

3. A Comissão avalia regularmente e, pelo menos, uma vez por ano os seguintes critérios relativamente a cada país terceiro associado ao PED a que se refere o n.º 1:

a) Se esse país cumpre os termos do acordo a que se refere o n.º 1, na medida em que esses termos digam respeito à participação na Reserva de Cibersegurança da UE;

b) Se esse país tomou medidas adequadas para se preparar para incidentes de cibersegurança significativos ou incidentes equivalentes a um incidente de cibersegurança em grande escala, com base nas informações a que se refere o n.º 2; e

c) Se a prestação de apoio é consonante com a política e as relações globais da União com esse país e se é consonante com outras políticas da União no domínio da segurança.

Ao proceder a essa avaliação referida no primeiro parágrafo, a Comissão consulta o alto representante no que diz respeito ao critério referido na alínea c) desse parágrafo.

Se concluir que um país terceiro associado ao PED preenche todas as condições referidas no primeiro parágrafo, a Comissão apresenta ao Conselho uma proposta de adoção de um ato de execução nos termos do n.º 4 que autorize a prestação de apoio da Reserva de Cibersegurança da UE a esse país.

4. O Conselho pode adotar os atos de execução a que se refere o n.º 3. Esses atos de execução são aplicáveis por um período máximo de um ano. Podem ser renovados. Podem incluir um limite não inferior a 75 dias para o número de dias em que o apoio pode ser prestado em resposta a um único pedido.

Para efeitos do presente artigo, o Conselho delibera de forma expedita e, por norma, adota os atos de execução a que se refere o presente número no prazo de oito semanas a contar da adoção da correspondente proposta da Comissão nos termos do n.º 3, terceiro parágrafo.

5. O Conselho pode alterar ou revogar um ato de execução adotado nos termos do n.º 4 em qualquer momento, sob proposta da Comissão.

Caso considere que houve uma alteração significativa do critério referido no n.º 3, primeiro parágrafo, alínea c), o Conselho pode alterar ou revogar o ato de execução a que se refere o n.º 4, deliberando por iniciativa devidamente fundamentada de um ou mais Estados-Membros.

6. No exercício das suas competências de execução nos termos do presente artigo, o Conselho aplica os critérios referidos no n.º 3, primeiro parágrafo, e explica a sua avaliação desses critérios. Em especial, se agir por iniciativa própria nos termos do n.º 5, segundo parágrafo, o Conselho explica a alteração significativa a que se refere esse parágrafo.

7. O apoio da Reserva de Cibersegurança da UE a um país terceiro associado ao PED deve cumprir quaisquer condições específicas previstas no acordo a que se refere o n.º 1.

8. Os utilizadores de países terceiros associados ao PED elegíveis para beneficiar de serviços da Reserva de Cibersegurança da UE incluem autoridades competentes como as equipas de resposta a incidentes de segurança informática ou entidades equivalentes e as autoridades de gestão de cibercrises.

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

10. Os pedidos de apoio da Reserva de Cibersegurança da UE ao abrigo do presente artigo devem ser avaliados pela Comissão. A entidade adjudicante só pode prestar apoio a um país terceiro se e enquanto estiver em vigor um ato de execução do Conselho que autorize esse apoio em relação a esse país, adotado nos termos do n.º 4 do presente artigo. Deve ser transmitida uma resposta aos utilizadores a que se refere o artigo 14.º, n.º 3, alínea c), sem demora injustificada.

11. Após receção de um pedido de apoio ao abrigo do presente artigo, a Comissão informa imediatamente o Conselho. A Comissão mantém o Conselho informado da avaliação do pedido. A Comissão também coopera com o alto representante em matéria dos pedidos recebidos e da execução do apoio concedido a países terceiros associados ao PED ao abrigo da Reserva de Cibersegurança da UE. Além disso, a Comissão tem igualmente em conta os pontos de vista da ENISA relativamente a esses pedidos.

Artigo 20.º

Coordenação com mecanismos de gestão de crises da União

1. Sempre que incidentes de cibersegurança significativos, incidentes de cibersegurança em grande escala ou incidentes equivalentes a um incidente de cibersegurança em grande escala tenham origem ou resultem em catástrofes, na aceção do artigo 4.º, ponto 1, da Decisão n.º 1313/2013/UE, o apoio prestado ao abrigo do presente regulamento para dar resposta a tais incidentes complementa as ações no âmbito dessa decisão sem prejuízo da mesma.

2. Em caso de incidentes de cibersegurança em grande escala ou de incidentes equivalentes a um incidente de cibersegurança em grande escala em que seja acionado o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (mecanismo IPCR) ao abrigo da Decisão de Execução (UE) 2018/1993, o apoio prestado ao abrigo do presente regulamento para dar resposta a esses incidentes deve ser tratado em conformidade com os protocolos e procedimentos aplicáveis previstos pelo mecanismo IPCR.

Capítulo IV

Mecanismo europeu de análise de incidentes de cibersegurança

Artigo 21.º

Mecanismo europeu de análise de incidentes de cibersegurança

1. A pedido da Comissão ou da UE-CyCLONe, a ENISA analisa e avalia, com o apoio da rede de CSIRT e a aprovação dos Estados-Membros afetados, as ciberameaças, as vulnerabilidades conhecidas que possam ser exploradas e as medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou um incidente de cibersegurança em grande escala específico. Após a conclusão da análise e avaliação de um incidente e com o intuito de retirar ensinamentos e de prevenir ou mitigar futuros incidentes, a ENISA apresenta um relatório de análise de incidentes à UE-CyCLONe, à rede de CSIRT, aos Estados-Membros em causa e à Comissão, a fim de os apoiar no desempenho das suas funções, em especial tendo em conta as funções enunciadas nos artigos 15.º e 16.º da Diretiva (UE) 2022/2555. Sempre que um incidente tenha um impacto num país terceiro associado ao PED, a ENISA deve disponibilizar o relatório ao Conselho. Nesses casos, a Comissão disponibiliza o relatório ao alto representante.

2. Para elaborar o relatório de análise de incidentes referido no n.º 1 do presente artigo, a ENISA coopera com todas as partes interessadas pertinentes, incluindo representantes dos Estados-Membros, a Comissão, outras instituições, órgãos e organismos competentes da União, a indústria, nomeadamente os prestadores de serviços de segurança geridos e utilizadores de serviços de cibersegurança, e recolhe as reações das referidas partes interessadas. Se for caso disso, a ENISA, em articulação com as CSIRT e, sempre que pertinente, com as autoridades competentes designadas ou criadas nos termos do artigo 8.º, n.º 1 da Diretiva (UE) 2022/2555, coopera também com as entidades afetadas por incidentes de cibersegurança significativos ou incidentes de cibersegurança em grande escala. Os representantes consultados devem divulgar qualquer potencial conflito de interesses.

3. O relatório de análise de incidentes a que se refere o n.º 1 do presente artigo inclui uma revisão e análise do incidente de cibersegurança significativo ou do incidente de cibersegurança em grande escala específico, incluindo as principais causas, vulnerabilidades conhecidas que possam ser exploradas e ensinamentos retirados. A ENISA assegura a conformidade do relatório com o direito da União ou o direito nacional relativo à proteção de informações sensíveis ou classificadas. Se os Estados-Membros afetados ou outros utilizadores referidos no artigo 14.º, n.º 3, afetados pelo incidente o solicitarem, os dados e informações que o relatório contém são anonimizados. Não pode incluir quaisquer pormenores sobre vulnerabilidades ativamente exploradas que permaneçam sem correção.

4. Se for caso disso, o relatório de análise de incidentes formula recomendações para melhorar a postura da União no ciberespaço e pode incluir boas práticas das partes interessadas pertinentes e os ensinamentos retirados por elas.

5. A ENISA pode disponibilizar ao público uma versão do relatório de análise de incidentes. Essa versão do relatório deve conter apenas informações públicas fiáveis, ou outras informações fiáveis que tenham sido incluídas com o consentimento dos Estados-Membros em causa e, sempre que se trate de informação relativa a um utilizador a que se refere o artigo 14.º, n.º 3, alínea b) ou alínea c), com o consentimento do utilizador em causa.

Capítulo V

Disposições finais

Artigo 22.º

Alteração 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:

i) é inserida a seguinte alínea:

«a-A) Apoiar o desenvolvimento de um Sistema Europeu de Alerta em matéria de Cibersegurança criado pelo artigo 3.º do Regulamento (UE) 2024/… do Parlamento Europeu e do Conselho[*+], incluindo o desenvolvimento, a implantação e o funcionamento de plataformas de cibersegurança nacionais e transfronteiriças que contribuam para o conhecimento situacional na União e para o reforço das capacidades da União em matéria de informações sobre ciberameaças;

---

[*] Regulamento (UE) 2024/… do Parlamento Europeu e do Conselho, de …, que cria medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ciberameaças e incidentes de cibersegurança e que altera o Regulamento (UE) 2021/694 (Regulamento de Cibersolidariedade) (JO L, …, ELI: …).»,

---

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)) e inserir na nota de rodapé o número, a data, a referência do JO e a referência ELI desse regulamento.

ii) é aditada a seguinte alínea:

«g) Criar e operar o mecanismo de emergência em matéria de cibersegurança, criado pelo artigo 10.º do Regulamento (UE) …/…[+], incluindo a Reserva de Cibersegurança da UE, criada pelo artigo 14.º do mesmo regulamento ("Reserva de Cibersegurança da UE"), para apoiar os Estados-Membros na preparação e resposta a incidentes de cibersegurança significativos e incidentes de cibersegurança em grande escala em complemento dos recursos e capacidades nacionais e de outras formas de apoio disponíveis a nível da União, e para apoiar outros utilizadores na resposta a incidentes de cibersegurança significativos e incidentes de cibersegurança em grande escala;»;

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

«2. As ações 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, na sigla em inglês) e da Rede de Centros Nacionais de Coordenação nos termos do Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho[*]. No entanto, a Reserva de Cibersegurança da UE é executada pela Comissão e, em conformidade com o artigo 14.º, n.º 6, do Regulamento (UE) …/…[+], pela ENISA.

---

[*] 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).»;

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

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) 1 760 806 000 EUR para o objetivo específico n.º 2, Inteligência artificial;

c) 1 372 020 000 EUR para o objetivo específico n.º 3, Cibersegurança e confiança;

d) 482 640 000 EUR para o objetivo específico n.º 4, Competências digitais avançadas;»;

b) É aditado o seguinte número:

«8. Em derrogação do artigo 12.º, n.º 1, do Regulamento Financeiro, as dotações de autorização e de pagamento não utilizadas para as ações realizadas no âmbito da execução da Reserva de Cibersegurança da UE e as ações de apoio à assistência mútua nos termos do Regulamento (UE) …/…[+], que visem a consecução dos objetivos previstos 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. O Parlamento Europeu e o Conselho devem ser informados das dotações transitadas nos termos do artigo 12.º, n.º 6, do Regulamento Financeiro.»;

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

3) O artigo 12.º é alterado do seguinte modo:

a) São inseridos os seguintes números:

«5-A. O n.º 5 não se aplica às ações de execução do Sistema Europeu de Alerta em matéria de Cibersegurança, no que diz respeita às entidades jurídicas estabelecidas na União, mas controladas a partir de países terceiros, se se verificarem cumulativamente ambas as seguintes condições no que diz respeito à ação em causa:

a) Verifica-se, à luz dos resultados do levantamento realizado nos termos do artigo 9.º, n.º 4, do Regulamento (UE) …/…[+], um risco real de as ferramentas, infraestruturas ou serviços necessários e suficientes para que essa ação contribua adequadamente para o objetivo do Sistema Europeu de Alerta em matéria de Cibersegurança não poderem vir a ser disponibilizados por entidades jurídicas estabelecidas ou consideradas como estando estabelecidas nos Estados-Membros e controladas pelos Estados-Membros ou por nacionais dos Estados-Membros;

b) O risco para a segurança associado à aquisição junto de tais entidades jurídicas no âmbito do Sistema Europeu de Alerta em matéria de Cibersegurança é proporcionado tendo em conta os benefícios e não compromete os interesses essenciais de segurança da União e dos seus Estados-Membros.

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

5-B. O n.º 5 não se aplica às ações de execução da Reserva de Cibersegurança da UE, no que diz respeito às entidades jurídicas estabelecidas na União, mas controladas a partir de países terceiros, se se verificarem cumulativamente as seguintes condições no que diz respeito à ação em causa:

a) Verifica-se, à luz dos resultados do levantamento realizado nos termos do artigo 14.º, n.º 6, do Regulamento (UE) …/…[+], um risco real de a tecnologia, os conhecimentos especializados ou a capacidade necessários e suficientes para que a Reserva de Cibersegurança da UE desempenhe adequadamente as suas funções não poderem vir a ser disponibilizados pelas entidades jurídicas estabelecidas ou consideradas como estando estabelecidas nos Estados-Membros e controladas pelos Estados-Membros ou por nacionais dos Estados-Membros;

b) O risco para a segurança associado à integração dessas entidades jurídicas na Reserva de Cibersegurança da UE é proporcionado tendo em conta os benefícios e não compromete os interesses essenciais de segurança da União e dos seus Estados-Membros.»;

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

b) O n.º 6 passa a ter a seguinte redação:

«6. Se devidamente justificado por razões de segurança, o programa de trabalho pode igualmente prever que as entidades jurídicas estabelecidas em países associados e as entidades jurídicas estabelecidas na União, mas controladas a partir de países terceiros sejam elegíveis para participação em todas ou em algumas das ações no âmbito dos objetivos específicos n.ºs 1 e 2, mas apenas se cumprirem os requisitos aplicáveis a essas entidades jurídicas a fim de garantir a proteção dos interesses essenciais de segurança da União e dos Estados-Membros e de garantir a proteção de informações classificadas. Esses requisitos devem constar do programa de trabalho.

O primeiro parágrafo aplica-se igualmente, no que diz respeito às entidades jurídicas estabelecidas na União, mas controladas a partir de países terceiros, às ações no âmbito do objetivo específico n.º 3:

a) Destinadas a executar o Sistema Europeu de Alerta em matéria de Cibersegurança, se for aplicável o n.º 5-A; e

b) Destinadas a executar a Reserva de Cibersegurança da UE, se for aplicável o n.º 5-B.»;

4) 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* e 2014/25/UE** 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 determinar 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, a 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 do presente regulamento. 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 168.º, n.º 3, do Regulamento (UE, Euratom) 2024/2509 do Parlamento Europeu e do Conselho[***], o pedido de um único país terceiro é suficiente para mandatar a Comissão ou a ENISA para agir.

Ao executarem os procedimentos de contratação pública relativos à Reserva de Cibersegurança da UE, 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 168.º, n.º 3, do Regulamento (UE, Euratom) 2024/2509, 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.

---

* 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 28/03/2014, p. 65).

** Diretiva 2014/25/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos celebrados pelas entidades que operam nos setores da água, da energia, dos transportes e dos serviços postais e que revoga a Diretiva 2004/17/CE (JO L 94 de 28.3.2014, p. 243).

*** Regulamento (UE, Euratom) 2024/2509 do Parlamento Europeu e do Conselho, de 23 de setembro de 2024, relativo às regras financeiras aplicáveis ao orçamento geral da União (JO L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).»;

5) É inserido o seguinte artigo:

«*Artigo 16.º-A*

Conflitos de regras

No caso das ações de execução do Sistema Europeu de Alerta em matéria de Cibersegurança, as regras aplicáveis são as previstas nos artigos 4.º, 5.º e 9.º do Regulamento (UE) …/…[+]. Em caso de conflito entre as disposições do presente regulamento e as dos artigos 4.º, 5.º e 9.º do Regulamento (UE) …/…[+], estas últimas prevalecem, aplicando-se a essas ações específicas.

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

No caso da Reserva de Cibersegurança da UE, o artigo 17.º do Regulamento (UE) …/…[+] prevê as regras específicas relativas à participação de países terceiros associados ao Programa. Em caso de conflito entre as disposições do presente regulamento e as do artigo 19.º do Regulamento (UE) …/…[+], estas últimas prevalecem, aplicando-se a essas ações específicas.»;

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

«*Artigo 19.º*
Subvenções

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 disposto 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 Estados-Membros selecionados nos termos do artigo 9.º do Regulamento (UE) …/…[+] e ao consórcio de acolhimento a que se refere o artigo 5.º do Regulamento (UE) …/…[+] em conformidade com o artigo 195.º, n.º 1, alínea d), do Regulamento Financeiro.

O mecanismo de emergência em matéria de cibersegurança pode conceder apoio 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.

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

No que respeita às ações de apoio à assistência mútua previstas no artigo 18.º do Regulamento (UE) …/…[+], 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.

No que respeita às ações de apoio à assistência mútua previstas no artigo 18.º do Regulamento (UE) …/…[+], e em conformidade com o artigo 193.º, n.º 2, segundo parágrafo, alínea a), do Regulamento Financeiro, os custos podem, em casos devidamente justificados, ser considerados elegíveis ainda que tenham sido incorridos antes da apresentação do pedido de subvenção.»;

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

Artigo 23.º

Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 14.º, n.º 7, é conferido à Comissão por um prazo de cinco anos, a partir de … [data de entrada em vigor do presente regulamento]. A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 94/24 (2023/0109(COD)).

3. A delegação de poderes referida no artigo 14º, n.º 7, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. Não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor.

5. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados nos termos do artigo 14.º, n.º 7, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 24.º

Procedimento de comité

1. A Comissão é assistida pelo Comité de Coordenação do Programa Europa Digital a que se refere o artigo 31.º, n.º 1, do Regulamento (UE) 2021/694. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

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

Artigo 25.º

Avaliação e reexame

1. Até … [dois anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, pelo menos de quatro em quatro anos, a Comissão avalia o funcionamento das medidas previstas no presente regulamento e apresenta um relatório ao Parlamento Europeu e ao Conselho.

2. A avaliação a que se refere o n.º 1 incide, em especial, nos seguintes aspetos:

a) O número de plataformas de cibersegurança nacionais e transfronteiriças, a extensão das informações partilhadas, nomeadamente, se possível, o impacto no trabalho da rede de CSIRT, e em que medida contribuíram para reforçar a deteção e o conhecimento situacional comum da União em matéria de ciberameaças e incidentes de cibersegurança, bem como para desenvolver tecnologias de ponta; a utilização dos fundos do PED para a aquisição conjunta de infraestruturas, ferramentas ou serviços de cibersegurança; e, se esta informação estiver disponível, o grau de cooperação entre as plataformas de cibersegurança nacionais e as comunidades sectoriais e transectoriais de entidades essenciais e importantes a que se refere o artigo 3.º da Diretiva (UE) 2022/2555;

b) A mobilização e eficácia das ações no âmbito do mecanismo de emergência em matéria de cibersegurança no apoio à preparação, nomeadamente ações de formação, a resposta e a recuperação inicial aos incidentes de cibersegurança significativos, aos incidentes de cibersegurança em grande escala e aos incidentes equivalentes a um incidente de cibersegurança em grande escala, incluindo a utilização dos fundos do PED, bem como os ensinamentos retirados da execução do mecanismo de emergência em matéria de cibersegurança e as recomendações daí decorrentes;

c) O uso e eficácia da Reserva de Cibersegurança da UE em relação ao tipo de utilizadores, nomeadamente o recurso aos fundos do PED, a adesão aos serviços, incluindo o seu tipo, o tempo médio de resposta aos pedidos e de mobilização da Reserva de Cibersegurança da UE, a percentagem de serviços convertidos em serviços de preparação relacionados com a prevenção e a resposta a incidentes, bem como os ensinamentos retirados da execução da Reserva de Cibersegurança da UE e as recomendações daí decorrentes;

d) O contributo do presente regulamento para o reforço da posição concorrencial da indústria e dos serviços na União em toda a economia digital, incluindo as microempresas e as pequenas e médias empresas, bem como as empresas em fase de arranque, e o contributo para a realização do objetivo geral de reforçar as competências e capacidades da mão de obra no domínio da cibersegurança.

3. Com base nos relatórios a que se refere o n.º 1, a Comissão apresenta, se for caso disso, uma proposta legislativa ao Parlamento Europeu e ao Conselho para alterar o presente regulamento.

Artigo 26.º

Entrada em vigor

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

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

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente / A Presidente*

ANEXO

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

1) No anexo I, a secção «Objetivo específico n.º 3 — Cibersegurança e confiança» passa a ter a seguinte redação:

«Objetivo específico n.º 3 — Cibersegurança e confiança

O Programa deve estimular o reforço, a criação e a aquisição de capacidades essenciais para proteger a economia digital, a sociedade e a democracia da União através do reforço do potencial e da competitividade da indústria de cibersegurança da União, bem como a melhoria das capacidades dos sectores público e privado para protegerem as empresas e os cidadãos contra as ciberameaças, incluindo o apoio à aplicação da Diretiva (UE) 2016/1148.

As ações iniciais e, se for caso disso, posteriores, no âmbito do presente objetivo incluem:

1. O coinvestimento com os Estados-Membros em equipamento, infraestruturas e conhecimentos avançados de cibersegurança, essenciais para proteger as infraestruturas críticas e o Mercado Único Digital em geral. Tal coinvestimento poderá incluir investimentos em instalações de tecnologias quânticas e recursos de dados para a cibersegurança e o conhecimento situacional em matéria de ciberespaço, incluindo as plataformas de cibersegurança nacionais e transfronteiriças que constituem o Sistema Europeu de Alerta em matéria de Cibersegurança, bem como outras ferramentas à disposição dos sectores público e privado em toda a Europa.

2. A expansão das capacidades tecnológicas existentes e a criação de redes entre os centros de competências nos Estados-Membros e a garantia de que estas capacidades possam dar resposta às necessidades do sector público e da indústria, nomeadamente em termos de produtos e serviços que reforcem a cibersegurança e a confiança dentro do Mercado Único Digital.

3. A garantia de uma implantação de soluções eficazes e de ponta em matéria de cibersegurança e confiança em todos os Estados-Membros. Essa implantação inclui o reforço da segurança e proteção dos produtos, desde a conceção à sua comercialização.

4. O apoio para colmatar o défice de competências em matéria de cibersegurança, tendo em conta o equilíbrio entre homens e mulheres, por exemplo alinhando e adaptando os programas de formação no domínio da cibersegurança às necessidades específicas de cada sector e facilitando o acesso a cursos específicos de formação especializada.

5. A promoção da solidariedade entre os Estados-Membros na preparação e resposta a incidentes de cibersegurança significativos e incidentes de cibersegurança em grande escala através da disponibilização de serviços de cibersegurança além-fronteiras, incluindo apoio à assistência mútua entre autoridades públicas e a criação de uma reserva de prestadores de serviços de segurança geridos de confiança a nível da União.»;

2) No anexo II, a secção «Objetivo específico n.º 3 — Cibersegurança e confiança» passa a ter a seguinte redação:

«Objetivo específico n.º 3 — Cibersegurança e confiança

3.1. O número de infraestruturas ou ferramentas de cibersegurança, ou ambas, adquiridas conjuntamente, incluindo no âmbito do Sistema Europeu de Alerta em matéria de Cibersegurança

3.2. O número de utilizadores e comunidades de utilizadores que obtêm acesso a instalações europeias de cibersegurança

3.3 O número de ações de apoio à preparação e resposta a incidentes de cibersegurança no âmbito do mecanismo de emergência em matéria de cibersegurança».

Foi feita uma declaração sobre este ato, que pode ser consultada em [Serviço do JO: JO C XXX, XX.XX.2024, p. XX] e na seguinte hiperligação: [JO: Inserir no texto a hiperligação para a declaração].