Conselho da
União Europeia

Bruxelas, 22 de março de 2022
(OR. en)

7474/22

Dossiê interinstitucional:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

PROPOSTA

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	22 de março de 2022
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2022) 122 final
Assunto:	Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

Envia-se em anexo, à atenção das delegações, o documento COM(2022) 122 final.

Anexo: COM(2022) 122 final

COMISSÃO
EUROPEIA

Bruxelas, 22.3.2022
COM(2022) 122 final

2022/0085 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

{SWD(2022) 67 final} - {SWD(2022) 68 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Razões e objetivos da proposta

A presente proposta estabelece um quadro destinado a garantir regras e medidas comuns em matéria de cibersegurança nas instituições, órgãos e organismos da União. Visa reforçar a resiliência e a capacidade de resposta a incidentes de todas as entidades, estando em consonância com as prioridades da Comissão no sentido de preparar a Europa para a era digital e criar uma economia preparada para o futuro e que esteja ao serviço dos cidadãos e assegurando igualmente uma administração pública segura e resiliente enquanto pedra angular da transformação digital da sociedade no seu conjunto.

A proposta baseia-se na Estratégia da UE para a União da Segurança [COM(2020) 605 final] e na Estratégia de cibersegurança da UE para a década digital [JOIN(2020) 18 final].

A proposta moderniza o atual quadro jurídico do CERT-UE e tem em conta a evolução e intensificação da digitalização das instituições, órgãos e organismos nos últimos anos, bem como a evolução do panorama das ameaças à cibersegurança. Esses processos têm-se intensificado desde o início da crise de COVID-19, enquanto o número de incidentes continua a aumentar, com ataques cada vez mais sofisticados a serem lançados de uma grande diversidade de origens.

A proposta muda o nome das CERT-UE de «Equipas de Resposta a Emergências Informáticas» para «Centros de Cibersegurança» para as instituições, órgãos e organismos da União, em consonância com a evolução registada nos Estados-Membros e a nível mundial, onde muitas CERT passaram a designar-se Centros de Cibersegurança, mas mantém a designação abreviada «CERT-UE», devido ao reconhecimento do nome.

• Coerência com as disposições existentes da mesma política setorial

A presente proposta visa aumentar a resiliência em matéria de cibersegurança das instituições, órgãos e organismos da União, assegurando simultaneamente o alinhamento com a legislação existente:

- Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Está também em consonância com a proposta de Diretiva (UE) XXXX/XXXX relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 (proposta SIR 2).

- Regulamento (UE) 2019/881 relativo à Agência da União Europeia para a Cibersegurança e à certificação da cibersegurança das tecnologias da informação e das comunicações (Regulamento Cibersegurança).

- Proposta de Regulamento (UE) XXXX/XXXX relativo à segurança da informação nas instituições, órgãos e organismos da União.

- Recomendação da Comissão de 23 de junho de 2021 relativa à criação de uma Ciberunidade Conjunta.

- 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.

O anexo da 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, estabelece o plano de ação para a resposta coordenada a incidentes e crises de cibersegurança transfronteiriços em larga escala.

Na sua resolução de 9 de março de 2021, o Conselho da União Europeia salientou que a cibersegurança é vital para o funcionamento da administração pública, tanto a nível nacional como da UE, bem como para a sociedade e a economia no seu todo, e sublinhou a importância de instituir um quadro de segurança sólido e coerente para proteger todo o pessoal, dados, redes de comunicação e sistemas de informação da UE, bem como os respetivos processos de tomada de decisão. Tal deve ser alcançado, em especial, por meio do reforço da resiliência e da melhoria da cultura de segurança das instituições, órgãos e organismos da União, devendo ser disponibilizados recursos e capacidades suficientes para esse efeito, nomeadamente no contexto do reforço do mandato do CERT-UE.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

O presente regulamento tem por base o artigo 298.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que determina que, no desempenho das suas atribuições, as instituições, órgãos e organismos da União se apoiam numa administração europeia aberta, eficaz e independente. No respeito do Estatuto e do Regime adotados com base no artigo 336.º, o Parlamento Europeu e o Conselho, por meio de regulamentos adotados de acordo com o processo legislativo ordinário, estabelecem as disposições necessárias para o efeito.

As tecnologias da informação proporcionaram novas formas de as instituições, órgãos e organismos da União trabalharem, interagirem com os cidadãos e melhorarem as suas operações globais. O panorama das ciberameaças evolui em paralelo com a tecnologia. As instituições, órgãos e organismos da União tornaram-se alvos altamente atrativos para ciberataques sofisticados. A criação de sistemas e requisitos para garantir a cibersegurança parece estar a contribuir para a eficiência e a independência da administração europeia, permitindo que as instituições, órgãos e organismos da União consigam funcionar de forma mais eficiente, num mundo digital, na condução das suas missões.

Além disso, as disparidades existentes entre as instituições, órgãos e organismos da União em matéria de postura e abordagem no domínio da cibersegurança, como explicado na secção 3 abaixo, constituem obstáculos adicionais a uma administração europeia aberta, eficiente e independente. Sem uma abordagem comum, a postura em matéria de cibersegurança das instituições, órgãos e organismos da União continuaria a evoluir de forma divergente. Esta base jurídica é por conseguinte adequada, uma vez que o regulamento visa criar um quadro jurídico comum para a cibersegurança nas instituições, órgãos e organismos da União.

- **Subsidiariedade**

O regulamento que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União é da competência exclusiva da União.

- **Proporcionalidade**

As regras propostas no presente regulamento não excedem o necessário para atingir os objetivos específicos de forma satisfatória. As medidas previstas contribuirão para alcançar um elevado nível comum de cibersegurança sem exceder o necessário para atingir o objetivo, tendo em conta os riscos cada vez mais elevados.

- **Escolha do instrumento**

Um regulamento, que é diretamente aplicável, foi considerado como o instrumento jurídico mais adequado para definir e racionalizar as obrigações impostas às instituições, órgãos e organismos da União. Um regulamento é o instrumento jurídico mais adequado, a fim de permitir melhorias específicas.

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

- **Avaliações *ex ante***

O CERT-UE efetuou uma avaliação das principais ciberameaças a que as instituições, órgãos e organismos da União estão atualmente expostas ou poderão vir a estar expostas num futuro previsível.

A análise incidiu sobre três categorias de observações:

- Tentativas de violação da infraestrutura informática das instituições, órgãos e organismos da União (quando bem-sucedidas, são tratadas como incidentes, nos demais casos são consideradas tentativas detetadas).

- Ameaças detetadas na proximidade de instituições, órgãos e organismos da União (por exemplo, em setores com os quais têm contactos, em comunidades de partes interessadas ou na Europa).

- Evolução das ameaças de grande envergadura observadas a nível mundial.

Além disso, a análise teve em conta a forma como as grandes mudanças em curso estão a afetar a gestão e utilização pelas instituições da União das suas infraestruturas e serviços informáticos. Essas mudanças incluem:

- O aumento do teletrabalho.

- A migração de sistemas para a nuvem.

- Um aumento da contratação externa de serviços informáticos.

Entre 2019 e 2021, o número de incidentes significativos[1] que afetaram as instituições, órgãos e organismos da União envolvendo ameaças persistentes avançadas (APA) aumentou dramaticamente. No primeiro semestre de 2021 foram observados incidentes significativos a um nível equivalente a todo o ano de 2020. Esse aumento refletiu-se igualmente no número de imagens forenses (instantâneos do conteúdo dos sistemas ou dispositivos afetados) que o CERT-UE analisou em 2020, que triplicou em comparação com 2019, ao passo que o número de incidentes significativos mais do que decuplicou desde 2018.

Em 2020, o Comité Diretor do CERT-UE estabeleceu um novo objetivo estratégico no sentido de que o CERT-UE garantisse um nível abrangente de ciberdefesa para todas as instituições, órgãos e organismos, com uma amplitude e profundidade adequadas e uma adaptação contínua às ameaças atuais ou iminentes, incluindo ataques contra dispositivos móveis, ambientes de computação em nuvem e dispositivos da Internet das Coisas.

Em complemento da análise de ameaças do CERT-UE, a Comissão realizou uma avaliação do funcionamento da cibersegurança em 20 instituições, órgãos e organismos da União, que permitiu conhecer melhor as práticas de cibersegurança estabelecidas, bem como as capacidades de gestão dessa mesma cibersegurança, por meio de uma validação externa do desempenho de alguns controlos técnicos de segurança.

Esta avaliação baseou-se em questionários junto dessas instituições, órgãos e organismos, em dados públicos e em dados fornecidos diretamente pelas próprias instituições, órgãos e organismos da União, proporcionando informações suficientes sobre a situação atual que permitem retirar as seguintes conclusões:

- A maturidade em termos de cibersegurança, a dimensão da infraestrutura informática e os níveis de capacidade variam substancialmente nas diferentes instituições, órgãos e organismos da União avaliados.

- Embora de forma geral já existam capacidades de deteção e resposta consolidadas em diversas instituições, órgãos e organismos da União, as suas capacidades de governação da cibersegurança apresentam níveis variáveis de gestão integrada dos riscos.

- Embora os quadros de cibersegurança (estratégia, políticas e regras de base) das instituições, órgãos e organismos da União avaliados estejam, de forma geral, bem estabelecidos nos principais domínios da cibersegurança, enumerados no anexo I do regulamento, algumas instituições, órgãos e organismos da União carecem de uma maior maturidade em termos de gestão da continuidade das atividades, de conformidade, de auditoria e de aperfeiçoamento contínuo.

- Verificou-se que as instituições, órgãos e organismos da União avaliados aplicavam de forma desigual as medidas técnicas consideradas como as melhores práticas.

Em resumo, a análise das 20 instituições, órgãos e organismos da União mostra que a sua governação, ciber-higiene, capacidade global e maturidade apresentam grandes variações, pelo que é fundamental exigir que todas as instituições e órgãos da União apliquem uma base de referência em matéria de cibersegurança, de forma a colmatar esta disparidade de

[1] «Incidente significativo», qualquer incidente, a menos que tenha um impacto limitado e seja suscetível de já ser bem compreendido em termos de método ou tecnologia.

maturidade e para elevar todas as instituições e órgãos da União a um nível comum reforçado de cibersegurança.

Até à data, nenhuma legislação da União se concentrou na cibersegurança das instituições, órgãos e organismos da União e abordou de forma abrangente o panorama das ameaças à cibersegurança e dos riscos informáticos emergentes decorrentes da digitalização.

- **Consultas das partes interessadas**

A Comissão consultou as partes interessadas em todas as instituições, órgãos e organismos da União, bem como representantes dos Estados-Membros, no Conselho, e das partes interessadas, no Parlamento Europeu. Em 25 de junho de 2021, os representantes dos Estados-Membros e das partes interessadas das instituições, órgãos e organismos da União participaram num ateliê organizado pela Comissão para debater o conteúdo da futura proposta de regulamento.

- **Avaliação de impacto**

O impacto da presente proposta incide sobretudo nas instituições, órgãos e organismos da União. Uma vez que não haverá efeitos ao nível dos Estados-Membros, não foi necessária uma avaliação de impacto específica.

- **Direitos fundamentais**

A União Europeia está empenhada em assegurar elevados níveis de proteção dos direitos fundamentais. Toda a partilha de informações com base no presente regulamento deverá ser efetuada em ambientes de confiança e no pleno respeito do direito à proteção dos dados pessoais, como estabelecido no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia e na legislação pertinente em matéria de proteção de dados, nomeadamente no Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho.

4. INCIDÊNCIA ORÇAMENTAL

Os estudos e parâmetros de referência do mercado[2] demonstram que as despesas diretas com a cibersegurança têm tendido a variar entre 4 e 7 % das despesas informáticas agregadas das organizações. No entanto, a análise de ameaças realizada pelo CERT-UE em apoio da presente proposta legislativa indica que os organismos internacionais e as organizações políticas enfrentam riscos acrescidos, pelo que um nível de 10 % das despesas informáticas em cibersegurança se afigura uma meta mais adequada. Não é possível determinar o custo preciso de tais esforços, devido à falta de informações pormenorizadas sobre as despesas informáticas das instituições, órgãos e organismos da União e sobre a correspondente proporção de despesas em cibersegurança.

[2] Fonte: Gartner, *Identifying the Real Information Security Budget* (2016). Acresce às despesas indiretas em segurança informática, como as relativas à segurança das redes, incluindo *firewalls* ou antivírus, ou às responsabilidades dos proprietários dos sistemas, como a avaliação dos riscos e a aplicação de controlos de segurança. Um estudo publicado em 2020 estimava que as despesas das instituições financeiras em cibersegurança representariam 10-11% das suas despesas totais com informática, fonte: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

Embora seja portanto provável que muitas instituições, órgãos e organismos da União despendam menos em cibersegurança do que deveriam, o presente regulamento não provocará, por si só, um aumento dessas despesas correntes. Mesmo sem o regulamento, cada entidade teria de assegurar um nível adequado de cibersegurança. O regulamento dá seguimento à anterior cooperação no quadro do Comité Diretor da CERT-UE e formaliza um nível de intercâmbio de informações já parcialmente existente hoje em dia. Tal como especificado na ficha financeira legislativa, o CERT-UE necessitará de recursos adicionais para desempenhar o seu papel alargado, recursos esses que deverão ser reafetados pelas instituições, órgãos e organismos da União que beneficiam dos serviços do CERT-UE.

5. OUTROS ELEMENTOS

- **Planos de execução e acompanhamento, avaliação e prestação de informações**

O Conselho Interinstitucional para a Cibersegurança (IICB), com a assistência do CERT-UE, deverá analisar o funcionamento do presente regulamento, conduzir avaliações e apresentar à Comissão um relatório com as respetivas conclusões. A Comissão deve assegurar uma comunicação regular de informações ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões.

O CERT-UE pode elaborar uma proposta de documento de orientação ou de recomendação, que o IICB poderá ou não adotar. Um documento de orientação assume o caráter de aconselhamento e é dirigido a todos ou a um conjunto de instituições, órgãos e organismos da União, ao passo que uma recomendação é dirigida a instituições, órgãos e organismos da União a título individual. Os apelos à ação assumem a forma de um aconselhamento do CERT-UE que descreve medidas urgentes de segurança que as instituições, órgãos e organismos da União são instados a tomar num determinado prazo.

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

Disposições gerais

O regulamento estabelece medidas destinadas a assegurar um elevado nível comum de cibersegurança e é aplicável às instituições, órgãos e organismos da União, para que possam desempenhar as respetivas missões de forma aberta, eficiente e independente. (Artigos 1.º–3.º e 23.º–25.º)

Medidas destinadas a garantir um elevado nível comum de cibersegurança

As instituições, órgãos e organismos da União são obrigados a estabelecer um quadro interno de gestão, governação e controlo dos riscos de cibersegurança que assegure uma gestão eficaz e prudente de todos os riscos de cibersegurança. Essas instituições, órgãos e organismos devem, além disso, adotar uma base de referência em matéria de cibersegurança para fazer face aos riscos identificados no âmbito do quadro, realizar periodicamente avaliações da maturidade em matéria de cibersegurança e adotar um plano de cibersegurança. (Artigos 4.º–8.º)

Conselho Interinstitucional para a Cibersegurança

É estabelecido o Conselho Interinstitucional para a Cibersegurança, que será responsável pelo acompanhamento da aplicação do presente regulamento pelas instituições, órgãos e

organismos da União, bem como pela supervisão da concretização das prioridades e dos objetivos gerais por parte do CERT-UE e pela definição da sua direção estratégica. (Artigos 9.º–11.º)

CERT-UE

O CERT-UE contribui para a segurança do ambiente informático de todas as instituições, órgãos e organismos da União, aconselhando-as, ajudando a prevenir, detetar, atenuar e dar resposta a incidentes e agindo como plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes para as partes. (Artigos 12.º–17.º)

Obrigações de cooperação e notificação

O regulamento assegura a cooperação e o intercâmbio de informações entre o CERT-UE e as instituições, órgãos e organismos da União, de forma a desenvolver a confiança e a fiabilidade. Para o efeito, o CERT-UE pode solicitar que as instituições, órgãos e organismos da União lhe forneçam informações pertinentes e pode partilhar informações específicas sobre incidentes com essas mesmas instituições, órgãos e organismos da União, para facilitar a deteção de ciberameaças ou incidentes semelhantes, sem o consentimento do constituinte afetado. O CERT-UE só pode partilhar informações específicas sobre um determinado incidente de cibersegurança que revelem a identidade do seu alvo com o consentimento do constituinte afetado.

Todas as instituições, órgãos e organismos da União devem nomeadamente notificar o CERT-UE das ciberameaças, vulnerabilidades e incidentes de caráter significativo sem demora injustificada e, em todo o caso, o mais tardar no prazo de 24 horas após terem tomado conhecimento dos mesmos. (Artigos 18.° -22.º)

2022/0085 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 298.º,

Tendo em conta o Tratado que institui a Comunidade Europeia da Energia Atómica, nomeadamente o artigo 106.º-A,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos Parlamentos nacionais,

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) Na era digital, as tecnologias da informação e da comunicação constituem uma pedra angular de uma administração europeia aberta, eficiente e independente. A evolução tecnológica e a crescente complexidade e interligação dos sistemas digitais amplificam os riscos de cibersegurança, tornando a administração europeia mais vulnerável a ameaças e incidentes informáticos, o que, em última análise, constitui uma ameaça para a continuidade das atividades da administração e para a garantia da proteção dos seus dados. Embora o aumento da utilização dos serviços de computação em nuvem, o recurso generalizado às tecnologias da informação, a elevada digitalização, o trabalho à distância e a evolução tecnológica sejam atualmente características essenciais de todas as atividades das entidades administrativas da União, a resiliência digital ainda não foi suficientemente incorporada.

(2) O panorama das ciberameaças com que as instituições, órgãos e organismos da União se confrontam está em constante mutação. As táticas, técnicas e procedimentos utilizados pelos perpetradores das ameaças estão em constante evolução, mas os principais motivos para tais ataques não mudam muito: roubar informações confidenciais valiosas, obter ganhos pecuniários, manipular a opinião pública ou comprometer as infraestruturas digitais. O ritmo dos ataques desses perpetradores continua a intensificar-se, com campanhas cada vez mais sofisticadas e automatizadas que visam as partes mais expostas de sistemas cada vez mais alargados, explorando rapidamente qualquer vulnerabilidade.

(3) Os ambientes informáticos das instituições, órgãos e organismos da União apresentam interdependências e fluxos de dados integrados, e os seus utilizadores colaboram estreitamente entre si. Esta interligação implica que qualquer perturbação, mesmo que inicialmente confinada a uma instituição, órgão ou organismo, pode ter repercussões mais vastas e resultar em impactos negativos generalizados e duradouros nos outros. Além disso, os ambientes informáticos de certas instituições, órgãos e organismos estão ligados aos ambientes informáticos dos Estados-Membros, levando a que um incidente numa entidade da União possa representar um risco de cibersegurança para os ambientes informáticos dos Estados-Membros e vice-versa.

(4) As instituições, órgãos e organismos da União são alvos atrativos que enfrentam perpetradores com um elevado nível de competências e recursos, bem como outras ameaças. Ao mesmo tempo, o nível e a maturidade da ciber-resiliência e das capacidades de deteção e resposta a atividades informáticas maliciosas variam significativamente entre estas entidades. Para assegurar o correto funcionamento da administração europeia, é portanto necessário que as instituições, órgãos e organismos da União atinjam um elevado nível comum de cibersegurança por meio de uma base de referência na matéria (um conjunto mínimo de regras de cibersegurança que as redes e os sistemas de informação têm de cumprir, de modo a minimizar os riscos de cibersegurança), do intercâmbio de informações e da colaboração.

(5) A diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União [proposta SRI 2] visa reforçar a resiliência em matéria de cibersegurança e as capacidades de resposta a incidentes das entidades públicas e privadas, das autoridades e organismos nacionais competentes e da União no seu conjunto. Por conseguinte, é necessário que as instituições, órgãos e organismos da União sigam o mesmo exemplo, assegurando a existência de regras coerentes com a diretiva [proposta SRI 2] e que reflitam o seu nível de ambição.

(6) Para garantir um elevado nível comum de cibersegurança, será necessário que cada instituição, órgão e organismo da União estabeleça um quadro interno de gestão, governação e controlo dos riscos de cibersegurança, assegure uma gestão eficaz e prudente de todos os riscos de cibersegurança e tenha em conta as questões da continuidade das atividades e da gestão das crises.

(7) As diferenças existentes entre as instituições, órgãos e organismos da União exigem flexibilidade na aplicação, uma vez que uma única abordagem não se adequará a todos os casos. As medidas destinadas a garantir um elevado nível comum de cibersegurança não devem incluir nenhuma obrigação que interfira diretamente no exercício das missões das instituições, órgãos e organismos da União ou prejudique a sua autonomia institucional. Por conseguinte, essas instituições, órgãos e organismos devem estabelecer os seus próprios quadros de gestão, governação e controlo dos riscos de cibersegurança, bem como adotar os seus próprios planos de cibersegurança e bases de referência.

(8) Para evitar impor encargos financeiros e administrativos desproporcionados às instituições, órgãos e organismos da União, os requisitos de gestão dos riscos de cibersegurança devem ser proporcionados em relação ao risco das redes e dos sistemas de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas. Cada instituição, órgão e organismo da União deve procurar afetar uma percentagem adequada do seu orçamento informático à melhoria do

respetivo nível de cibersegurança, devendo a mais longo prazo procurar alcançar uma meta da ordem dos 10 %.

(9) Um elevado nível comum de cibersegurança exige que esses aspetos sejam supervisionados ao mais alto nível da direção de cada instituição, órgão e organismo da União, que deverá aprovar uma base de referência na matéria com vista a fazer face os riscos identificados ao abrigo do quadro próprio que deverá ser estabelecido por cada entidade. A cultura de cibersegurança, que corresponde às práticas de rotina em termos de segurança informática, constituirá parte integrante da base de referência em matéria de cibersegurança em todas as instituições, órgãos e organismos da União.

(10) As instituições, órgãos e organismos da União devem avaliar os riscos ligados ao seu relacionamento com fornecedores e prestadores de serviços, incluindo prestadores de serviços de armazenamento e tratamento de dados ou de serviços de segurança sob gestão de terceiros, e tomar medidas adequadas para os acautelar. Estas medidas devem integrar a base de referência em matéria de cibersegurança e ser especificadas em documentos de orientação ou recomendações emitidos pelo CERT-UE. Na definição das medidas e orientações, devem ser tidas em devida conta a legislação e as políticas pertinentes da UE, incluindo as avaliações de risco e as recomendações emitidas pelo grupo de cooperação SRI, como a avaliação coordenada dos riscos a nível da UE e o conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G. Além disso, poderá ser exigida a certificação de produtos, serviços e processos de TIC pertinentes, ao abrigo de sistemas específicos de certificação da cibersegurança da UE adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881.

(11) Em maio de 2011, os secretários-gerais das instituições e organismos da União decidiram pré-configurar uma equipa de resposta a emergências informáticas para as instituições, órgãos e organismos da UE («CERT-UE»), supervisionada por um Comité Diretor interinstitucional. Em julho de 2012, os secretários-gerais confirmaram as disposições práticas e concordaram em manter a CERT-UE como entidade permanente para continuar a ajudar a melhorar o nível global de segurança das tecnologias da informação das instituições, órgãos e organismos da União, num exemplo bem visível da cooperação interinstitucional em matéria de cibersegurança. Em setembro de 2012, a CERT-UE foi criada na qualidade de grupo de trabalho da Comissão Europeia com um mandato interinstitucional. Em dezembro de 2017, as instituições e organismos da União celebraram um acordo interinstitucional sobre a organização e o funcionamento da CERT-UE[3]. Este acordo deverá continuar a evoluir em apoio da aplicação do presente regulamento.

(12) O CERT-UE deve mudar o seu nome de «Equipa de Resposta a Emergências Informáticas» para «Centro de Cibersegurança» para as instituições, órgãos e organismos da União, em consonância com a evolução registada nos Estados-Membros e a nível mundial, onde muitas entidades desse tipo passaram a designar-se Centros de Cibersegurança, mas deverá manter-se a designação abreviada «CERT-UE», devido ao reconhecimento do nome.

[3] JO C 12 de 13.1.2018, p. 11.

(13) Muitos ciberataques enquadram-se em campanhas mais alargadas que visam grupos de instituições, órgãos e organismos da União ou comunidades de interesse que incluem instituições, órgãos e organismos da União. A fim de permitir a deteção proativa, a resposta em caso de incidente ou a tomada de medidas de atenuação, as instituições, órgãos e organismos da União devem notificar o CERT-UE das ciberameaças, vulnerabilidades e incidentes de caráter significativo, bem como partilhar pormenores técnicos adequados para permitir a deteção, atenuação ou resposta a ameaças, vulnerabilidades e incidentes informáticos similares que possam afetar outras instituições, órgãos e organismos da União. Aplicando a mesma abordagem prevista na diretiva [proposta SRI 2], quando tenham tido conhecimento de um incidente significativo as entidades devem proceder à notificação inicial ao CERT-UE no prazo de 24 horas. Este intercâmbio de informações permitirá ao CERT-UE divulgar as informações a outras instituições, órgãos e organismos da União, bem como às devidas contrapartes, de forma a proteger todos os ambientes informáticos, tanto da União como das suas contrapartes, contra incidentes, ameaças e vulnerabilidades semelhantes.

(14) Para além da afetação de novas atribuições e de um papel mais interventivo ao CERT-UE, deve ser instituído um Conselho Interinstitucional para a Cibersegurança (IICB) que facilite um elevado nível comum de cibersegurança entre as instituições, órgãos e organismos da União, acompanhando a forma como aplicam o presente regulamento, supervisionando a concretização das prioridades e objetivos gerais pelo CERT-UE e conferindo-lhe uma direção estratégica. O IICB deve assegurar a representação das instituições e integrar representantes dos diferentes órgãos e organismos, por meio da Rede de Agências da União.

(15) O CERT-UE deve apoiar a implementação de medidas destinadas a garantir um elevado nível comum de cibersegurança por meio da apresentação de propostas de documentos de orientação e recomendações ao IICB ou do lançamento de apelos à ação. Os referidos documentos de orientação e recomendações deverão ser aprovados pelo IICB. Sempre que necessário, o CERT-UE deve lançar apelos à ação descrevendo medidas de segurança urgentes que as instituições, órgãos e organismos da União são instados a tomar num determinado prazo.

(16) O IICB deve acompanhar o cumprimento do presente regulamento e o seguimento dado aos seus documentos de orientação e recomendações, bem como aos apelos à ação lançados pelo CERT-UE. O IICB deve ser apoiado em questões técnicas por grupos consultivos técnicos, com a composição que o IICB entenda, os quais devem trabalhar em estreita cooperação com o CERT-UE, as instituições, órgãos e organismos da União e outras partes interessadas, conforme necessário. Se necessário, o IICB deve emitir alertas não vinculativos e recomendar a realização de auditorias.

(17) O CERT-UE deve ter como missão contribuir para a segurança do ambiente informático de todas as instituições, órgãos e organismos da União. O CERT-UE deve exercer uma função equivalente à do coordenador designado para as instituições, órgãos e organismos da União, para fins de divulgação coordenada das vulnerabilidades ao respetivo registo europeu referido no artigo 6.º da diretiva [proposta SRI 2].

(18) Em 2020, o Comité Diretor do CERT-UE estabeleceu um novo objetivo estratégico no sentido de que o CERT-UE garantisse um nível abrangente de ciberdefesa para todas

as instituições, órgãos e organismos da União, com uma amplitude e profundidade adequadas e uma adaptação contínua às ameaças atuais ou iminentes, incluindo ataques contra dispositivos móveis, ambientes de computação em nuvem e dispositivos da Internet das Coisas. Esse objetivo estratégico inclui igualmente centros de operações de segurança de largo espetro responsáveis pela monitorização das redes e das ameaças de maior gravidade. O CERT-UE deve apoiar as equipas de segurança informática das instituições, órgãos e organismos de maior dimensão, nomeadamente na monitorização permanente de primeira linha, prestando todos os serviços nesse contexto às instituições, órgãos e organismos de pequena dimensão, bem como a alguns de média dimensão.

(19) O CERT-UE deve também desempenhar o papel que lhe é conferido pela diretiva [proposta SRI 2] em matéria de cooperação e intercâmbio de informações com a rede de equipas de resposta a incidentes de segurança informática (CSIRT). Além disso, em consonância com a Recomendação (UE) 2017/1584 da Comissão[4], o CERT-UE deve cooperar e coordenar a resposta com as partes interessadas relevantes. A fim de contribuir para um elevado nível de cibersegurança na União, o CERT-UE deve partilhar informações específicas sobre incidentes com as suas contrapartes a nível nacional. O CERT-UE deve igualmente colaborar com outras contrapartes públicas e privadas, nomeadamente da NATO, sob reserva da aprovação prévia do IICB.

(20) No apoio à cibersegurança operacional, o CERT-UE deve recorrer aos conhecimentos especializados disponíveis da Agência da União Europeia para a Cibersegurança por meio de uma cooperação estruturada, conforme previsto no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[5]. Sempre que pertinente, devem ser acordadas entre as duas organizações as disposições adequadas para definir o modo de pôr em prática essa cooperação e evitar a duplicação de atividades. O CERT-UE deve cooperar com a Agência da União Europeia para a Cibersegurança na análise das ameaças e partilhar periodicamente com a agência o seu relatório sobre o panorama das ameaças.

(21) No apoio à Ciberunidade Conjunta criada nos termos da Recomendação da Comissão de 23 de junho de 2021[6], o CERT-UE deve cooperar e trocar informações com as partes interessadas, de forma a promover a cooperação operacional e permitir que as redes existentes realizem todo o seu potencial na proteção da União.

(22) Qualquer tratamento de dados pessoais ao abrigo do presente regulamento deve respeitar a legislação em matéria de proteção de dados, incluindo o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[7].

---

4 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 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 Recomendação da Comissão de 23 de junho de 2021 relativa à criação de uma Ciberunidade Conjunta.

7 Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

(23) O tratamento das informações pela CERT-UE e pelas instituições, órgãos e organismos da União deve ser consentâneo com as regras estabelecidas no [proposta de regulamento relativo à segurança da informação]. A fim de assegurar a coordenação quanto às questões de segurança, todos os contactos com o CERT-UE iniciados ou solicitados pelos serviços nacionais de segurança e de informações devem ser comunicados, sem demora injustificada, à Direção-Geral da Segurança da Comissão Europeia e ao presidente do IICB.

(24) Uma vez que os serviços e as atribuições do CERT-UE assumem interesse para todas as instituições, órgãos e organismos da União, cada uma dessas entidades que suporte despesas no domínio das tecnologias da informação deve contribuir com uma parte equitativa para esses serviços e atribuições. Essa contribuição não prejudica a autonomia orçamental das instituições, órgãos e organismos da União.

(25) O IICB, com a assistência do CERT-UE, deve analisar e avaliar a implementação do presente regulamento, reportando à Comissão. Com base nessas informações, a Comissão apresentará relatório ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões.

ADOTARAM O PRESENTE REGULAMENTO:

Capítulo I
DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto

O presente regulamento estabelece:

(a) Obrigações no sentido de que as instituições, órgãos e organismos da União criem um quadro interno de gestão, governação e controlo dos riscos de cibersegurança;

(b) Obrigações de gestão e notificação dos riscos de cibersegurança aplicáveis às instituições, órgãos e organismos da União;

(c) Regras relativas à organização e ao funcionamento do Centro de Cibersegurança para as instituições, órgãos e organismos da União («CERT-UE») e relativas à organização e ao funcionamento do Conselho Interinstitucional para a Cibersegurança («IICB»).

Artigo 2.º
Âmbito

O presente regulamento é aplicável à gestão, governação e controlo dos riscos de cibersegurança por todas as instituições, órgãos e organismos da União, bem como à organização e ao funcionamento do CERT-UE e do IICB.

Artigo 3.º
Definições

Para efeitos do presente regulamento, entende-se por:

(1) «Instituições, órgãos e organismos da União», as instituições, órgãos e organismos estabelecidos pelo Tratado da União Europeia, pelo Tratado sobre o Funcionamento da União Europeia ou pelo Tratado que institui a Comunidade Europeia da Energia Atómica, ou com base nesses tratados;

(2) «Rede e sistema de informação», uma rede e sistema de informação na aceção do artigo 4.º, n.º 1, da diretiva [proposta SRI 2];

(3) «Segurança das redes e dos sistemas de informação», a segurança das redes e dos sistemas de informação na aceção do artigo 4.º, n.º 2, da diretiva [proposta SRI 2];

(4) «Cibersegurança», a cibersegurança na aceção do artigo 4.º, n.º 3, da diretiva [proposta SRI 2];

(5) «Direção ao mais alto nível», um dirigente ou um organismo de direção ou de coordenação e supervisão ao mais alto nível administrativo, tendo em conta as disposições em matéria de governação ao mais alto nível em cada instituição, órgão ou organismo da União;

(6) «Incidente», um incidente na aceção do artigo 4.º, n.º 5, da diretiva [proposta SRI 2];

(7) «Incidente significativo», qualquer incidente, a menos que tenha um impacto limitado e seja suscetível de já ser bem compreendido em termos de método ou tecnologia;

(8) «Ataque de grande envergadura», todo o incidente que exija mais recursos do que os disponíveis na instituição, órgão ou organismo da União afetados e no CERT-UE;

(9) «Tratamento de incidentes», o tratamento de incidentes na aceção do artigo 4.º, n.º 6, da diretiva [proposta SRI 2];

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

(11) «Ciberameaça significativa», uma ciberameaça com intenção, oportunidade e capacidade de causar um incidente significativo;

(12) «Vulnerabilidade», a vulnerabilidade na aceção do artigo 4.º, n.º 8, da diretiva [proposta SRI 2];

(13) «Vulnerabilidade significativa», uma vulnerabilidade suscetível de conduzir a um incidente significativo, se for explorada;

(14) «Risco de cibersegurança», qualquer circunstância ou evento razoavelmente identificável com potenciais efeitos adversos para a segurança das redes e dos sistemas de informação;

(15) «Ciberunidade Conjunta», uma plataforma virtual e física de cooperação para as diversas comunidades de cibersegurança na União, centrada na coordenação operacional e técnica contra ciberameaças e incidentes transnacionais de grande envergadura na aceção da Recomendação da Comissão de 23 de junho de 2021;

(16) «Base de referência em matéria de cibersegurança», um conjunto mínimo de regras de cibersegurança que as redes e os sistemas de informação têm de cumprir, de modo a minimizar os riscos de cibersegurança.

Capítulo II
MEDIDAS DESTINADAS A GARANTIR UM ELEVADO NÍVEL COMUM DE CIBERSEGURANÇA

Artigo 4.º
Gestão, governação e controlo dos riscos

1. Cada instituição, órgão e organismo da União deve estabelecer o seu próprio quadro interno de gestão, governação e controlo dos riscos de cibersegurança («o quadro»), em apoio da missão da entidade e no exercício da sua autonomia institucional. Este trabalho deve ser supervisionado ao mais alto nível de direção da entidade, a fim de assegurar uma gestão eficaz e prudente de todos os riscos de cibersegurança. O quadro deve ser posto em prática o mais tardar até ... [15 meses após a entrada em vigor do presente regulamento].

2. O quadro deve abranger a totalidade do ambiente informático da instituição, órgão ou organismo em causa, incluindo todos os ambientes informáticos nas instalações, os ativos e serviços contratados externamente em ambientes de computação em nuvem ou alojados por terceiros, os dispositivos móveis, as redes institucionais, as redes institucionais não ligadas à Internet e todos os dispositivos ligados ao ambiente informático. O quadro deve ter em conta as questões da continuidade das atividades e da gestão das crises e abranger a segurança da cadeia de abastecimento, bem como a gestão dos riscos humanos suscetíveis de afetar a cibersegurança da instituição, órgão ou organismo da União em causa.

3. Cabe à direção ao mais alto nível de cada instituição, órgão e organismo da União assegurar a supervisão do cumprimento, por parte da respetiva organização, das obrigações relacionadas com a gestão, governação e controlo dos riscos de cibersegurança, sem prejuízo das responsabilidades formais dos demais níveis da direção pelo cumprimento das regras e pela gestão dos riscos nos respetivos domínios de competência.

4. Cada instituição, órgão e organismo da União deve dispor de mecanismos eficazes para assegurar que uma percentagem adequada do orçamento para as tecnologias da informação seja aplicada em cibersegurança.

5. Cada instituição, órgão e organismo da União deve designar um responsável local pela cibersegurança, ou função equivalente, que atue como ponto de contacto único relativamente a todos os aspetos de cibersegurança.

Artigo 5.º

Base de referência em matéria de cibersegurança

1. Cabe à direção ao mais alto nível de cada instituição, órgão e organismo da União aprovar a sua própria base de referência em matéria de cibersegurança para fazer face aos riscos identificados no quadro referido no artigo 4.º, n.º 1, em apoio da sua missão e no exercício da sua autonomia institucional. A referida base de referência em matéria de cibersegurança deve ser criada o mais tardar até ... [18 meses após a entrada em vigor do presente regulamento] e abranger os domínios enumerados no anexo I e as medidas enumeradas no anexo II.

2. A direção de topo de cada instituição, órgão e organismo da União deve frequentar regularmente ações específicas de formação, a fim de adquirir conhecimentos e competências suficientes para compreender e avaliar os riscos de segurança e as práticas de gestão, bem como o seu impacto no funcionamento da organização.

Artigo 6.º

Avaliação da maturidade

Cada instituição, órgão e organismo da União efetua uma avaliação da maturidade em matéria de cibersegurança, pelo menos de três em três anos, incorporando todos os elementos do seu ambiente informático, tal como descrito no artigo 4.º, e tendo em conta os documentos de orientação e as recomendações pertinentes adotados em conformidade com o artigo 13.º.

Artigo 7.º

Planos de cibersegurança

1. Na sequência das conclusões extraídas da avaliação da maturidade e tendo em conta os ativos e riscos identificados nos termos do artigo 4.º, a direção ao mais alto nível de cada instituição, órgão e organismo da União deve aprovar um plano de cibersegurança, sem demora injustificada, após o estabelecimento do quadro de gestão, governação e controlo dos riscos e da base de referência em matéria de cibersegurança. O plano visa reforçar a cibersegurança global da entidade em causa e, por conseguinte, contribuir para a consecução ou o reforço de um elevado nível comum de cibersegurança em todas as instituições, órgãos e organismos da União. A fim de apoiar a missão da entidade com base na sua autonomia institucional, o plano deve incluir pelo menos os domínios enumerados no anexo I, as medidas enumeradas no anexo II, bem como medidas relacionadas com a preparação, a resposta e a recuperação em caso de incidente, incluindo a monitorização da segurança e a conservação de registos. O plano é revisto pelo menos de três em três anos, na sequência de avaliações da maturidade realizadas nos termos do artigo 6.º.

2. O plano de cibersegurança deve incluir as funções e responsabilidades dos diferentes membros do pessoal necessárias à sua execução.

3. O plano de cibersegurança deve considerar os eventuais documentos de orientação e recomendações aplicáveis emitidos pelo CERT-UE.

Artigo 8.º
Implementação

1. Uma vez concluídas as avaliações da maturidade, as instituições, órgãos e organismos da União devem transmiti-las ao Conselho Interinstitucional para a Cibersegurança. Uma vez concluídos os planos de segurança, as instituições, órgãos e organismos da União devem notificar esse facto ao Conselho Interinstitucional para a Cibersegurança. Mediante pedido do Conselho, devem comunicar informações sobre aspetos específicos do presente capítulo.

2. A implementação das disposições do presente capítulo será apoiada nos documentos de orientação e recomendações emitidos em conformidade com o artigo 13.º.

Capítulo III
CONSELHO INTERINSTITUCIONAL PARA A CIBERSEGURANÇA

Artigo 9.º
Conselho Interinstitucional para a Cibersegurança

1. É criado o Conselho Interinstitucional para a Cibersegurança («IICB»).

2. Cabe ao IICB:

   (a) Acompanhar a implementação do presente regulamento por parte das instituições, órgãos e organismos da União; e

   (b) Supervisionar a concretização das prioridades e objetivos gerais pelo CERT-UE e conferir-lhe uma direção estratégica.

3. O IICB é composto por três representantes nomeados pela Rede de Agências da União Europeia (EUAN), mediante proposta do seu Comité Consultivo para as TIC, para representar os interesses dos órgãos e organismos que administram os seus próprios ambientes informáticos, e por um representante designado por cada uma das seguintes entidades:

   (a) O Parlamento Europeu;

   (b) O Conselho da União Europeia;

   (c) A Comissão Europeia;

   (d) O Tribunal de Justiça da União Europeia;

   (e) O Banco Central Europeu;

   (f) O Tribunal de Contas Europeu;

   (g) O Serviço Europeu para a Ação Externa;

   (h) O Comité Económico e Social Europeu;

(i) O Comité das Regiões Europeu;

(j) O Banco Europeu de Investimento;

(k) A Agência da União Europeia para a Cibersegurança.

Os membros podem ser assistidos por um suplente. O presidente pode convidar outros representantes das organizações acima enumeradas ou de outras instituições, órgãos e organismos da União para participarem nas reuniões do IICB, sem direito de voto.

4. Cabe ao IICB aprovar o seu regulamento interno.

5. O IICB designa um presidente de entre os seus membros, nos termos do seu regulamento interno, por um período de quatro anos. O seu suplente torna-se membro efetivo do IICB durante o mesmo período.

6. O IICB reúne-se por iniciativa do seu presidente, a pedido do CERT-UE ou a pedido de um dos seus membros.

7. Cada membro do IICB dispõe de um voto. As decisões do IICB são tomadas por maioria simples, salvo disposição em contrário no presente regulamento. O presidente não participa na votação, exceto em caso de empate, caso em que poderá exercer um voto de qualidade.

8. O IICB pode deliberar por procedimento escrito simplificado em conformidade com o seu regulamento interno, ao abrigo do qual as decisões pertinentes devem ser consideradas aprovadas no prazo estabelecido pelo presidente, exceto se um membro se opuser.

9. O diretor do CERT-UE, ou o seu suplente, participa nas reuniões do IICB, salvo decisão em contrário do IICB.

10. O secretariado do IICB é assegurado pela Comissão.

11. Os representantes nomeados pela EUAN mediante proposta do Comité Consultivo para as TIC transmitem as decisões do IICB aos organismos e empresas comuns da União. Todos os órgãos e organismos da União têm o direito de suscitar junto dos representantes ou do presidente do IICB qualquer questão que considerem que deve ser dada a conhecer ao IICB.

12. O IICB pode, por iniciativa do seu presidente, deliberar por procedimento escrito simplificado, ao abrigo do qual as decisões pertinentes serão consideradas aprovadas no prazo estabelecido pelo presidente, exceto se um membro se opuser.

13. O IICB pode nomear um Comité Executivo para o assistir nos seus trabalhos e delegar-lhe algumas das suas atribuições e competências. Cabe ao IICB estabelecer o regulamento interno do Comité Executivo, incluindo as respetivas atribuições e poderes e a duração do mandato dos seus membros.

Artigo 10.º
Atribuições do IICB

No exercício das suas responsabilidades, o IICB deve, em particular:

(a) Analisar quaisquer relatórios solicitados ao CERT-UE sobre o estado de implementação do presente regulamento pelas instituições, órgãos e organismos da União;

(b) Aprovar, com base numa proposta do diretor do CERT-UE, o programa de trabalho anual do CERT-UE e acompanhar a sua execução;

(c) Aprovar, com base numa proposta do diretor do CERT-UE, o catálogo de serviços do CERT-UE;

(d) Aprovar, com base numa proposta apresentada pelo diretor do CERT-UE, o plano financeiro anual de receitas e despesas, nomeadamente despesas de pessoal, para as atividades do CERT-UE;

(e) Aprovar, com base numa proposta do diretor do CERT-UE, as modalidades dos acordos de nível de serviço;

(f) Examinar e aprovar o relatório anual elaborado pelo diretor do CERT-UE relativo às atividades e à gestão dos fundos do CERT-UE;

(g) Aprovar e acompanhar os indicadores-chave de desempenho do CERT-UE, definidos por proposta do seu diretor;

(h) Aprovar acordos de cooperação, acordos de nível de serviço ou contratos entre o CERT-UE e outras entidades nos termos do artigo 17.º;

(i) Estabelecer os grupos consultivos técnicos necessários para assistir nos trabalhos do IICB, aprovar os respetivos estatutos e designar os respetivos presidentes.

Artigo 11.º
Conformidade

Cabe ao IICB acompanhar a implementação, por parte das instituições, órgãos e organismos da União, do presente regulamento e dos documentos de orientação, recomendações e apelos à ação adotados. Quando concluir que as instituições, órgãos e organismos da União não aplicaram ou implementaram efetivamente o presente regulamento ou algum dos documentos de orientação, recomendações ou apelos à ação emitidos ao abrigo do presente regulamento, o IICB pode, sem prejuízo dos procedimentos internos da instituição, órgão ou organismo da União em causa:

(a) Emitir um alerta que, quando necessário à luz de um manifesto risco de cibersegurança, deverá ser reservado a um universo devidamente restrito;

(b) Recomendar que um serviço de auditoria pertinente realize uma auditoria.

Capítulo IV
CERT-UE

Artigo 12.º
Missão e atribuições do CERT-UE

1. A missão do CERT-UE, o centro interinstitucional autónomo para a cibersegurança de todas as instituições, órgãos e organismos da União, será contribuir para a segurança do ambiente informático não classificado de todas as instituições, órgãos e organismos da União, aconselhando-os em matéria de cibersegurança, ajudando-os a prevenir, detetar, atenuar e dar resposta a incidentes e agindo como plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes.

2. O CERT-UE desempenha as seguintes funções em relação às instituições, órgãos e organismos da União:

   (a) Apoiá-los na aplicação do presente regulamento e contribuir para a coordenação dessa aplicação, por meio das medidas enumeradas no artigo 13.º, n.º 1, ou através de relatórios *ad hoc* solicitados pelo IICB;

   (b) Apoiá-los por meio de um pacote de serviços de cibersegurança descritos no seu catálogo de serviços («serviços de base»);

   (c) Manter uma rede de pares e parceiros para apoiar os serviços, conforme previsto nos artigos 16.º e 17.º;

   (d) Chamar a atenção do IICB para qualquer questão relacionada com a implementação do presente regulamento e dos documentos de orientação, recomendações e apelos à ação;

   (e) Apresentar relatórios sobre as ciberameaças com que se confrontam as instituições, órgãos e organismos da União e contribuir para o conhecimento situacional dessa matéria na UE.

3. O CERT-UE deve contribuir para a Ciberunidade Conjunta criada em conformidade com a Recomendação da Comissão de 23 de junho de 2021, nomeadamente nos seguintes domínios:

   (a) Preparação, coordenação em caso de incidentes, intercâmbio de informações e resposta a situações de crise a nível técnico em casos relacionados com instituições, órgãos e organismos da União;

   (b) Cooperação operacional no que respeita à rede de equipas de resposta a incidentes de segurança informática (CSIRT), nomeadamente em matéria de assistência mútua, bem como à comunidade de cibersegurança em geral;

   (c) Informações sobre ciberameaças, incluindo o conhecimento situacional;

(d) Qualquer tema que exija os conhecimentos técnicos especializados de cibersegurança do CERT-UE.

4. O CERT-UE enceta uma cooperação estruturada com a Agência da União Europeia para a Cibersegurança para efeitos de reforço das capacidades, cooperação operacional e análises estratégicas a longo prazo das ciberameaças, em conformidade com o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.

5. O CERT-UE pode prestar os seguintes serviços não descritos no seu catálogo de serviços («serviços sujeitos a cobrança»):

(a) Serviços de apoio à cibersegurança do ambiente informático das instituições, órgãos e organismos da União, distintos dos referidos no n.º 2, com base em acordos de nível de serviço e sob reserva dos recursos disponíveis;

(b) Serviços de apoio a operações ou projetos de cibersegurança das instituições, órgãos e organismos da União, distintos dos serviços destinados a proteger o respetivo ambiente informático, com base em acordos reduzidos a escrito e mediante aprovação prévia do IICB;

(c) Serviços de apoio à cibersegurança do ambiente informático de organizações distintas das instituições, órgãos e organismos da União mas que colaborem estreitamente com os mesmos, por exemplo, por possuírem atribuições ou responsabilidades ao abrigo do direito da União, com base em acordos reduzidos a escrito e mediante aprovação prévia do IICB.

6. O CERT-UE pode organizar exercícios de cibersegurança ou recomendar a participação em exercícios existentes, em estreita colaboração com a Agência da União Europeia para a Cibersegurança, sempre que aplicável, de forma a testar o nível de cibersegurança das instituições, órgãos e organismos da União.

7. O CERT-UE pode, se o constituinte envolvido o solicitar explicitamente, prestar assistência às instituições, órgãos e organismos da União relativamente a incidentes em ambientes informáticos classificados.

Artigo 13.º
Documentos de orientação, recomendações e apelos à ação

1. O CERT-UE apoia a implementação do presente regulamento através de:

(a) Apelos à ação, descrevendo medidas urgentes de segurança que as instituições, órgãos e organismos da União são instados a tomar num determinado prazo;

(b) Propostas ao IICB com vista à adoção de documentos de orientação dirigidos a todos ou a um conjunto de instituições, órgãos e organismos da União;

(c) Propostas ao IICB com vista à adoção de recomendações dirigidas a instituições, órgãos e organismos da União a título individual.

2. Os documentos de orientação e as recomendações podem incluir:

(a) Modalidades ou melhorias da gestão dos riscos de cibersegurança e da base de referência na matéria;

(b) Modalidades das avaliações da maturidade e dos planos de cibersegurança; e

(c) Se for caso disso, a utilização em comum de uma tecnologia, arquitetura e das melhores práticas conexas no intuito de concretizar a interoperabilidade e normas comuns na aceção do artigo 4.º, n.º 10, da diretiva [proposta SRI 2].

3. O IICB pode adotar documentos de orientação ou recomendações sob proposta do CERT-UE.

4. O IICB pode dar instruções ao CERT-UE no sentido de que este emita, retire ou modifique uma proposta de documento de orientação ou de recomendação, ou um apelo à ação.

Artigo 14.º
Diretor do CERT-UE

O diretor do CERT-UE apresenta regularmente relatórios ao IICB e ao presidente do IICB sobre o desempenho do CERT-UE, o planeamento financeiro, as receitas, a execução orçamental, os acordos de nível de serviço e os acordos escritos celebrados, a colaboração com as contrapartes e os parceiros, bem como as missões realizadas pelos membros do seu pessoal, incluindo os relatórios referidos no artigo 10.º, n.º 1.

Artigo 15.º
Questões financeiras e de pessoal

1. A Comissão, tendo obtido a aprovação por unanimidade do IICB, nomeia o diretor do CERT-UE. O IICB deve ser consultado em todas as fases do processo até à nomeação do diretor do CERT-UE, em especial na elaboração dos anúncios de abertura da vaga, na análise das candidaturas e na nomeação de júris de seleção para o cargo.

2. Relativamente à aplicação dos procedimentos administrativos e financeiros, o diretor do CERT-UE está subordinado à autoridade da Comissão.

3. As atribuições e atividades do CERT-UE, incluindo os serviços que preste nos termos do artigo 12.º, n.os 2, 3, 4 e 6, e do artigo 13.º, n.º 1, às instituições, órgãos e organismos da União financiados a partir da rubrica do quadro financeiro plurianual dedicada à administração pública europeia, são financiados por uma rubrica orçamental distinta do orçamento da Comissão. Os postos afetados ao CERT-UE são especificados numa nota de rodapé no quadro de pessoal da Comissão.

4. As instituições, órgãos e organismos da União distintos dos referidos no n.º 3 devem prestar uma contribuição financeira anual ao CERT-UE para cobrir os serviços prestados pelo CERT-UE nos termos desse mesmo n.º 3. As respetivas contribuições baseiam-se nas orientações dadas pelo IICB e acordadas entre cada entidade e o CERT-UE em acordos de nível de serviço. As contribuições devem representar uma parte justa e proporcionada dos custos totais dos serviços prestados. Serão registadas

na rubrica orçamental distinta referida no n.º 3 como receitas afetadas, tal como previsto no artigo 21.º, n.º 3, alínea c), do Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho[8].

5. Os custos das atribuições definidas no artigo 12.º, n.º 5, serão recuperados junto das instituições, órgãos e organismos da União que beneficiem dos serviços do CERT-UE. As receitas são afetadas às rubricas orçamentais de apoio aos custos.

Artigo 16.º

Colaboração do CERT-UE com as suas contrapartes nos Estados-Membros

1. O CERT-UE deve colaborar e trocar informações com as suas contrapartes nos Estados-Membros, incluindo as CERT, os centros nacionais de cibersegurança, as CSIRT e os pontos de contacto únicos referidos no artigo 8.º da diretiva [proposta SRI 2], relativamente a ciberameaças, vulnerabilidades e incidentes, a possíveis contramedidas e a todas as questões pertinentes para melhorar a proteção do ambiente informático das instituições, órgãos e organismos da União, nomeadamente por meio da rede de CSIRT referida no artigo 13.º da diretiva [proposta SRI 2].

2. O CERT-UE pode trocar informações específicas sobre incidentes com as suas contrapartes nacionais nos Estados-Membros, para facilitar a deteção de ciberameaças ou incidentes semelhantes, sem o consentimento do constituinte afetado. O CERT-UE só pode partilhar informações específicas sobre um determinado incidente de cibersegurança que revelem a identidade do seu alvo com o consentimento do constituinte afetado.

Artigo 17.º

Colaboração do CERT-UE com as suas contrapartes em países terceiros

1. O CERT-UE pode colaborar com contrapartes, nomeadamente setoriais, de países terceiros em matéria de ferramentas e métodos, como técnicas, táticas, procedimentos e melhores práticas, bem como em matéria de ameaças e vulnerabilidades informáticas. No que respeita à colaboração com tais contrapartes, nomeadamente no âmbito de quadros em que contrapartes de países terceiros colaborem com contrapartes dos Estados-Membros, o CERT-UE deve obter a aprovação prévia do IICB.

2. O CERT-UE pode colaborar com outros parceiros, como entidades comerciais, organizações internacionais, entidades nacionais de países terceiros ou determinados peritos, de forma a recolher informações sobre as ciberameaças, vulnerabilidades e contramedidas possíveis, em termos gerais e específicos. Para uma colaboração mais alargada com tais parceiros, o CERT-UE deve obter a aprovação prévia do IICB.

---

[8] Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, relativo às disposições financeiras aplicáveis ao orçamento geral da União, que altera os Regulamentos (UE) n.º 1296/2013, (UE) n.º 1301/2013, (UE) n.º 1303/2013, UE n.º 1304/2013, (UE) n.º 1309/2013, (UE) n.º 1316/2013, (UE) n.º 223/2014 e (UE) n.º 283/2014, e a Decisão n.º 541/2014/UE, e revoga o Regulamento (UE, Euratom) n.º 966/2012 (JO L 193 de 30.7.2018, p. 1).

3. Mediante consentimento do constituinte afetado por um incidente, o CERT-UE pode transmitir informações relacionadas com o mesmo a parceiros que possam contribuir para a sua análise.

Capítulo V
OBRIGAÇÕES DE COOPERAÇÃO E DE COMUNICAÇÃO DE INFORMAÇÕES

Artigo 18.º
Tratamento de informações

1. O CERT-UE e as instituições, órgãos e organismos da União devem respeitar as obrigações de sigilo profissional nos termos do artigo 339.º do Tratado sobre o Funcionamento da União Europeia ou dos quadros equivalentes aplicáveis.

2. As disposições do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho[9] são aplicáveis no que respeita aos pedidos de acesso do público a documentos na posse do CERT-UE, tendo em conta a obrigação, prevista no referido regulamento, de consultar as outras instituições, órgãos e organismos da União sempre que um pedido diga respeito a documentos seus.

3. O tratamento de dados pessoais realizado ao abrigo do presente regulamento está sujeito ao cumprimento do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho.

4. O tratamento das informações pela CERT-UE e pelas instituições, órgãos e organismos da União deve ser consentâneo com as regras estabelecidas no [proposta de regulamento relativo à segurança da informação].

5. Todos os contactos com o CERT-UE iniciados ou solicitados pelos serviços nacionais de segurança e de informações devem ser comunicados, sem demora injustificada, à Direção-Geral da Segurança da Comissão e ao presidente do IICB.

Artigo 19.º
Obrigações de partilha de informações

1. Com vista a permitir ao CERT-UE coordenar a gestão das vulnerabilidades e a resposta a incidentes, o CERT-UE pode solicitar que as instituições, órgãos e organismos da União lhe transmitam informações dos respetivos inventários de sistemas informáticos que sejam relevantes para fins do apoio a prestar pelo CERT-UE. A instituição, órgão ou organismo requerido deve transmitir sem demora injustificada as informações solicitadas, bem como eventuais atualizações subsequentes dessas informações.

---

[9] Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

2. As instituições, órgãos e organismos da União, a pedido do CERT-UE, facultam-lhe sem demora injustificada as informações digitais decorrentes da utilização dos dispositivos eletrónicos envolvidos nos incidentes em causa. O CERT-UE pode especificar os tipos de informação digital de que necessita para fins de conhecimento situacional e resposta a incidentes.

3. O CERT-UE só pode partilhar informações que permitam identificar a instituição, órgão ou organismo da União afetado por um determinado incidente com o consentimento dessa entidade. O CERT-UE só pode partilhar informações específicas sobre um determinado incidente de cibersegurança que revelem a identidade do seu alvo com o consentimento da entidade afetada.

4. As obrigações de partilha não abrangem as informações classificadas da UE (ICUE) nem as informações que uma instituição, órgão ou organismo da União tenha recebido de um serviço de segurança, de informações ou de uma autoridade judiciária de um Estado-Membro na condição explícita de não serem partilhadas com o CERT-UE.

Artigo 20.º
Obrigações de notificação

1. Todas as instituições, órgãos e organismos da União devem proceder a uma notificação inicial ao CERT-UE das ciberameaças, vulnerabilidades e incidentes de caráter significativo sem demora injustificada e, em todo o caso, o mais tardar no prazo de 24 horas após terem tomado conhecimento dos mesmos.

   Em determinados casos devidamente justificados e com o acordo da CERT-UE, a instituição, órgão ou organismo da União em causa poderá não cumprir o prazo previsto no parágrafo anterior.

2. As instituições, órgãos e organismos da União devem igualmente notificar ao CERT-UE, sem demora injustificada, pormenores técnicos sobre as ciberameaças, vulnerabilidades e incidentes que permitam a adoção de medidas para a deteção, resposta ou atenuação dos efeitos desses mesmos incidentes. A notificação deve incluir, se disponível:

   (a) Indicadores de comprometimento pertinentes;

   (b) Mecanismos de deteção pertinentes;

   (c) Impacto potencial;

   (d) Medidas de atenuação pertinentes.

3. O CERT-UE apresenta mensalmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre as ciberameaças, vulnerabilidades e incidentes de caráter significativo notificados em conformidade com o n.º 1.

4. O IICB pode emitir documentos de orientação ou recomendações sobre as modalidades e o conteúdo da notificação. O CERT-UE divulga os pormenores técnicos necessários para permitir uma deteção proativa, a resposta a incidentes ou a

tomada de medidas de atenuação por parte das instituições, órgãos e organismos da União.

5. As obrigações de notificação não abrangem as ICUE nem as informações que uma instituição, órgão ou organismo da União tenha recebido de um serviço de segurança, de informações ou de uma autoridade judiciária de um Estado-Membro na condição explícita de não serem partilhadas com o CERT-UE.

Artigo 21.º

Coordenação da resposta a incidentes e cooperação em caso de incidentes significativos

1. Ao atuar enquanto plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes, o CERT-UE facilita o intercâmbio de informações sobre ciberameaças, vulnerabilidades e incidentes entre:

   (a) Instituições, órgãos e organismos da União;

   (b) As contrapartes referidas nos artigos 16.º e 17.º.

2. O CERT-UE facilita a coordenação entre as instituições, órgãos e organismos da União na resposta a incidentes, incluindo os seguintes elementos:

   (a) Contribuição para uma comunicação externa coerente;

   (b) Assistência mútua;

   (c) Utilização ideal dos recursos operacionais;

   (d) Coordenação com outros mecanismos de resposta a situações de crise a nível da União.

3. O CERT-UE deve apoiar as instituições, órgãos e organismos da União no que respeita ao conhecimento situacional das ciberameaças, vulnerabilidades e incidentes.

4. O IICB deve emitir orientações sobre a coordenação da resposta a incidentes e a colaboração em caso de incidente significativo. Quando se suspeitar que um incidente teve natureza criminosa, o CERT-UE deve emitir orientações sobre a forma como deverá ser notificado às autoridades judiciárias.

Artigo 22.º

Ataques de grande envergadura

1. O CERT-UE coordenará a resposta das instituições, órgãos e organismos da União a ataques de grande envergadura. Deve manter um inventário dos conhecimentos técnicos especializados necessários para a resposta aos incidentes quando tais ataques ocorram.

2. As instituições, órgãos e organismos da União contribuem para o inventário de conhecimentos técnicos especializados mediante a transmissão de listas, atualizadas

todos os anos, de peritos disponíveis nas respetivas organizações, pormenorizando as suas competências técnicas específicas.

3. Mediante a aprovação das instituições, órgãos e organismos da União envolvidas, o CERT-UE também pode solicitar que os peritos da lista a que se refere o n.º 2 contribuam para a resposta a um ataque de grande envergadura num Estado-Membro, em conformidade com os procedimentos operacionais da Ciberunidade Conjunta.

Capítulo VI
DISPOSIÇÕES FINAIS

Artigo 23.º
Reafetação orçamental inicial

A Comissão propõe a reafetação do pessoal e dos recursos financeiros das instituições, órgãos e organismos pertinentes da União no quadro do orçamento da Comissão. A reafetação será efetiva com a aprovação do primeiro orçamento após a entrada em vigor do presente regulamento.

Artigo 24.º
Reexame

1. O IICB, com a assistência do CERT-UE, deve comunicar periodicamente à Comissão informações sobre a implementação do presente regulamento. O IICB pode também formular recomendações dirigidas à Comissão para que esta apresente propostas de alteração do presente regulamento.

2. A Comissão apresenta um relatório sobre a implementação do presente regulamento ao Parlamento Europeu e ao Conselho o mais tardar 48 meses após a entrada em vigor do presente regulamento e, posteriormente, de três em três anos.

3. Passados pelo menos cinco anos da sua entrada em vigor, a Comissão avaliará o funcionamento do presente regulamento e apresentará ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões o correspondente relatório.

Artigo 25.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
A Presidente

Pelo Conselho
A Presidente

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

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

1.3. A proposta/iniciativa refere-se a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(ais)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e impacto esperados

1.4.4. Indicadores de desempenho

1.5. Justificação da proposta/iniciativa

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

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

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

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

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

1.6. Duração e impacto financeiro da proposta/iniciativa

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

2. MEDIDAS DE GESTÃO

2,1. Disposições em matéria de acompanhamento e prestação de informações

2.2. Sistema(s) de gestão e de controlo

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

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

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

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

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

3.2. Impacto financeiro estimado da proposta nas dotações

3.2.1. Síntese do impacto estimado nas dotações operacionais

3.2.2. Estimativa das realizações financiadas com dotações operacionais

3.2.3. Síntese do impacto estimado nas dotações de natureza administrativa

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participações de terceiros

3.3. Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

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

Administração Pública Europeia

A proposta diz respeito a medidas que garantem um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União.

1.3. A proposta/iniciativa refere-se a:

☑uma nova ação

☐ uma nova ação na sequência de um projeto-piloto/ação preparatória[10]

☐ prorrogação de uma ação existente

☑ fusão ou reorientação de uma ou mais ações para outra/uma nova ação

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(ais)

– Estabelecer um quadro destinado a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

– Estabelecer uma nova base jurídica para o CERT-UE, com vista a reforçar o seu mandato e financiamento

1.4.2. Objetivo(s) específico(s)

(1) Estabelecer obrigações no sentido de que as instituições, órgãos e organismos da União criem um quadro interno de gestão, governação e controlo dos riscos de cibersegurança

(2) Estabelecer obrigações no sentido de que as instituições, órgãos e organismos da União comuniquem informações sobre o seu quadro interno de gestão, governação e controlo dos riscos de cibersegurança, bem como sobre os incidentes de cibersegurança

[10] Na aceção do artigo 58.º, n.º 2, alínea a) ou b), do Regulamento Financeiro.

(3) Estabelecer regras relativas à organização e ao funcionamento do Centro de Cibersegurança para as instituições, órgãos e organismos da União («CERT-UE») e relativas à organização e ao funcionamento do Conselho Interinstitucional para a Cibersegurança («IICB»)

(4) Contribuir para a Ciberunidade Conjunta.

1.4.3. Resultado(s) e impacto esperados

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

– Quadros internos de gestão, governação e controlo dos riscos de cibersegurança, bases de referência em matéria de cibersegurança, avaliações da maturidade periódicas e planos de cibersegurança nas instituições, órgãos e organismos da União – Reforço da resiliência em matéria de cibersegurança e da resposta a incidentes nas instituições, órgãos e organismos da União – Modernização do CERT-UE – Contributo para a Ciberunidade Conjunta

1.4.4. Indicadores de desempenho

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

– Os quadros e as bases de referência estabelecidos, as avaliações da maturidade periódicas e os planos de cibersegurança executados nas instituições, órgãos e organismos da União – Melhor tratamento dos incidentes – Maior consciência dos riscos de cibersegurança ao mais alto nível da direção das instituições, órgãos e organismos da União – Uniformização das despesas de segurança das TIC em percentagem das despesas globais de TIC – Liderança resoluta do IICB e do CERT-UE – Intensificação da partilha de informações entre as instituições, órgãos e organismos da União, bem como com os organismos e partes interessadas pertinentes na UE – Reforço da cooperação em matéria de cibersegurança com os organismos e partes interessadas pertinentes na UE, por meio do CERT-UE e da ENISA

1.5. Justificação da proposta/iniciativa

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

A proposta visa aumentar o nível de ciber-resiliência das instituições, órgãos e organismos da União, de forma a reduzir as diferenças em termos de resiliência entres estas entidades e melhorar o nível de conhecimento situacional comum e a capacidade coletiva de preparação e resposta.

A proposta é plenamente coerente com outras iniciativas conexas, em especial com a proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, e que revoga a Diretiva (UE) 2016/1148 [proposta SRI 2].

A proposta constitui uma parte essencial da Estratégia para a União da Segurança e da Estratégia de Cibersegurança da UE para a Década Digital.

Prevê-se que a Comissão Europeia apresente a proposta de regulamento em outubro de 2021, que o Parlamento Europeu e o Conselho adotem o regulamento em 2022 e que as disposições sejam aplicáveis a partir da sua entrada em vigor. Prevê-se que o impacto financeiro e em matéria de recursos humanos descrito na presente ficha financeira legislativa tenha início em 2023. Já se iniciou um período preparatório em 2021, mas as atividades preparatórias em 2021 e 2022 não são incluídas no impacto financeiro da proposta.

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

Razões para uma ação a nível europeu (*ex ante*)

Entre 2019 e 2021, o número de incidentes significativos que afetaram as instituições, órgãos e organismos da União envolvendo ameaças persistentes avançadas aumentou dramaticamente. No primeiro semestre de 2021 foram observados incidentes significativos a um nível equivalente a todo o ano de 2020. Tal reflete-se igualmente no número de imagens forenses (instantâneos do conteúdo dos sistemas ou dispositivos afetados) que o CERT-UE analisou em 2020, que triplicou em comparação com 2019, ao passo que o número de incidentes significativos mais do que decuplicou desde 2018.

Os níveis de maturidade em termos de cibersegurança variam substancialmente de uma entidade para outra[11]. O presente regulamento garantirá que todas as instituições, órgãos e organismos da União apliquem medidas de segurança de base e

[11] Referência: [Relatório Especial do TCE sobre a cibersegurança nas instituições, órgãos e organismos da União].

cooperem entre si com o objetivo de assegurar o funcionamento aberto e eficaz da administração europeia.

Os sistemas a preservar são abrangidos pela autonomia das instituições, órgãos e organismos da União e são por eles geridos, pelo que as medidas propostas não poderiam ser tomadas pelos Estados-Membros.

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

A Diretiva SRI foi o primeiro instrumento horizontal do mercado interno destinado a melhorar a resiliência das redes e dos sistemas na União face aos riscos de cibersegurança. Desde a sua entrada em vigor, em 2016, contribuiu, em grande medida, para aumentar o nível comum de cibersegurança entre os Estados-Membros. A proposta de Diretiva SRI 2 procura reforçar estas medidas.

O regulamento procura determinar medidas semelhantes para as instituições, órgãos e organismos da União.

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

A proposta é coerente com o quadro financeiro plurianual e constitui uma parte essencial da Estratégia para a União da Segurança e da Estratégia de Cibersegurança da UE para a Década Digital.

A proposta prevê aplicar medidas que garantam um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União. A proposta é consentânea com a proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148 [proposta SRI 2].

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

A gestão das atribuições do CERT-UE exige perfis específicos e uma carga de trabalho suplementar que não podem ser absorvidos sem um aumento dos recursos humanos e financeiros.

1.6. Duração e impacto financeiro da proposta/iniciativa

☐ **duração limitada**

– ☐ em vigor entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA para as dotações de autorização e entre AAAA e AAAA para as dotações de pagamento.

☑ **duração ilimitada**

– O impacto financeiro deve ter início a partir do primeiro orçamento aprovado após a entrada em vigor do regulamento. A reafetação de recursos das instituições e dos principais órgãos da União para a Comissão ocorreria no primeiro ano,

considerado um ano de transição. Esta e outras (re)afetações de recursos ocorrerão no âmbito dos orçamentos anuais. Se o regulamento for adotado em 2022, o período transitório corresponderá ao exercício de 2023, entrando em pleno funcionamento em 2024.

1.7. Modalidade(s) de gestão prevista(s)[12]

☑ **Gestão direta** pela Comissão e por cada instituição, organismo e agência da União

– ☑ pelos seus serviços, incluindo pelo pessoal nas delegações da União;

– ☐ pelas agências de execução

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

☐ **Gestão indireta** confiando tarefas de execução orçamental:

– ☐ a países terceiros ou a organismos por estes designados,

– ☐ a organizações internacionais e respetivas agências (a especificar),

– ☐ ao BEI e ao Fundo Europeu de Investimento,

– ☐ aos organismos referidos nos artigos 70.º e 71.º do Regulamento Financeiro,

– ☐ a organismos de direito público

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

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

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

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

Observações

No que respeita à aplicação dos procedimentos administrativos e financeiros, o CERT-UE está subordinado à autoridade da Comissão. Recursos suplementares decorrentes da proposta de regulamento:

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

A aplicação dos artigos 12.º e 13.º da proposta de regulamento conduz a um aumento do catálogo de serviços, contendo serviços de base suplementares. Em pleno funcionamento, serão necessários os seguintes recursos suplementares (até à conclusão do QFP, no final de 2027): 21 ETC e 14,05 milhões de EUR.

Os recursos suplementares no quadro do orçamento para as diversas atribuições repartem-se da seguinte forma:

(a) Para o exercício das atribuições das instituições, órgãos e organismos especificadas no artigo 12.º, n.º 2, alíneas a), b), c) e e): 13,75 ETC e 11,275 milhões de EUR;

(b) Para o exercício das atribuições especificadas no artigo 12.º, n.º 3 (contribuição para a Ciberunidade Conjunta): 2 ETC e 381 000 EUR;

(c) Para o exercício das atribuições especificadas no artigo 12.º, n.º 4 (cooperação estruturada com a ENISA): 0,25 ETC e 236 000 EUR;

(d) Para o exercício das atribuições especificadas no artigo 12.º, n.º 6 (exercícios de cibersegurança): 0,25 ETC e 79 000 EUR;

(e) Para o exercício das atribuições especificadas no artigo 12.º, n.º 2, alínea d), e no artigo 13.º (análise e apresentação de relatórios sobre a aplicação do regulamento, elaboração de documentos de orientação, recomendações e apelos à ação): 3,75 ETC e 2,079 milhões de EUR.

(f) Para o exercício das atribuições de apoio ao secretariado do Conselho Interinstitucional para a Cibersegurança: 1 ETC.

Panorâmica dos recursos existentes e transição para a entrada em pleno funcionamento:

Em setembro de 2021, o CERT-UE desenvolvia a sua atividade com os seguintes recursos:

- lugares permanentes e destacados: 14 ETC,

- agentes contratuais financiados ao abrigo de acordos de nível de serviço: 24 ETC,

- 38 ETC no total.

Orçamento do CERT-UE em 2020: 250 000 EUR ao abrigo do orçamento da Comissão, 3,5 milhões de EUR por meio de receitas afetadas provenientes de acordos de nível de serviço. Total: 3,75 milhões de EUR. Constitui a totalidade do orçamento do CERT-UE, abrangendo formação, equipamento informático, *software*, missões, apoio, agentes contratuais e conferências.

Com a entrar em vigor do regulamento, prevê-se que o CERT-UE venha a dispor dos seguintes recursos:

- lugares permanentes: 34 ETC,

- agentes contratuais: 15 ETC,

- 49 ETC no total, havendo portanto um aumento líquido de 11 ETC.

A alteração do rácio entre os lugares permanentes e agentes contratuais permitirá fazer face ao problema da contratação e manutenção de quadros superiores no domínio da cibersegurança, devido à sua escassez no mercado de trabalho.

Além disso, será necessário 1 ETC agente contratual na Direção-Geral da Informática da Comissão, para apoio ao Conselho Interinstitucional para a Cibersegurança.

Por conseguinte, no total, serão necessários 21 ETC suplementares (20 ETC para o CERT-UE e 1 ETC para a Direção-Geral da Informática) para aplicar o regulamento. Tal será compensado por uma redução paralela de 9 ETC de agentes contratuais no CERT-UE, que eram antes financiados por receitas afetadas no âmbito de acordos de nível de serviço.

Em 2024, após o período de transição, o orçamento de recursos materiais do CERT-UE abrangerá as atribuições enumeradas acima nas alíneas a) a e), prevendo-se que seja financiado do seguinte modo:

- 8,921 milhões de EUR por ano das instituições da União financiadas ao abrigo da rubrica 7 do orçamento da União,

- 2,459 milhões de EUR das instituições, órgãos e organismos da União financiados ao abrigo das rubricas 1 a 6 do orçamento da União,

- 2,670 milhões de EUR de instituições, órgãos e organismos da União autofinanciados.

- Orçamento total do CERT-UE: 14,05 milhões de EUR.

As atribuições enumeradas no artigo 12.º, n.º 5, não descritas no catálogo de serviços, serão serviços sujeitos a cobrança. Estes serviços são acessórios, representam montantes relativamente baixos e são na sua maioria temporários, sendo os seus custos recuperados junto dos beneficiários dos serviços por meio de acordos de nível de serviço ou de acordos escritos.

No que respeita às contribuições para o pessoal do CERT-UE, as principais instituições e organismos da União devem contribuir com uma quota-parte proporcional à respetiva parte dos lugares AD permanentes da organização. Há que ponderar a possibilidade de o BCE e o BEI também contribuírem com uma quota-parte por meio do destacamento de pessoal permanente.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições.

A Comissão, com o apoio do IICB e do CERT-UE, examinará periodicamente o funcionamento do regulamento e apresentará um relatório ao Parlamento Europeu e ao Conselho, pela primeira vez o mais tardar 48 meses após a entrada em vigor do regulamento e, posteriormente, de três em três anos.

As fontes de dados utilizadas nos exames provirão sobretudo do IICB e do CERT-UE. Além disso, poderão ser utilizadas, quando necessário, ferramentas específicas de recolha de dados, p. ex., inquéritos às instituições, órgãos e organismos da União, à ENISA ou à rede de CSIRT.

2.2. Sistema(s) de gestão e de controlo

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

As atividades decorrentes do regulamento serão geridas em cada instituição, órgão e organismo da União em conformidade com as respetivas regras e disposições regulamentares aplicáveis.

A gestão administrativa e financeira das atividades do CERT-UE está integrada na administração da Comissão e é abrangida pelos respetivos mecanismos de gestão e execução, modalidades de pagamento e controlos aplicáveis.

O auditor interno da Comissão exerce, em relação ao CERT-UE, os mesmos poderes que exerce em relação aos serviços da Comissão.

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

Risco muito baixo, uma vez que o CERT-UE já se encontra na dependência administrativa do diretor-geral da Direção-Geral da Informática enquanto grupo de trabalho da Comissão, e o IICB utiliza o modelo do atual Comité Diretor do CERT-UE. Por conseguinte, já existe um ecossistema para a gestão financeira e o controlo interno.

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

Já existem e já foram bem testados os procedimentos de contratação, gestão financeira e controlo. A relação custo-eficácia dos controlos e os níveis de risco de erro correspondem aos de cada instituição, órgão ou organismo da União e da Comissão, no caso das atividades do CERT-UE.

2.3. Medidas de prevenção de fraudes e irregularidades

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

Os sistemas de gestão financeira e de controlo interno da Comissão são aplicáveis às atividades do CERT-UE.

Na luta contra a fraude, a corrupção e outras ações ilegais, são aplicáveis sem quaisquer restrições, as disposições do Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho, de 11 de setembro de 2013, relativo aos inquéritos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF).

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

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

- Rubricas orçamentais existentes

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

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Tipo de despesa	Participação			
	Número	DD/DND[13]	dos países da EFTA[14]	dos países candidatos [15]	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
1 a 6	Rubricas orçamentais que abrangem as contribuições da União para os órgãos e organismos descentralizados	DD	NÃO	NÃO	NÃO	NÃO
7	Rubricas orçamentais que abrangem as remunerações do pessoal, despesas em TI e outras despesas administrativas nas diferentes secções do orçamento da UE	DND	NÃO	NÃO	NÃO	NÃO

- Novas rubricas orçamentais, cuja criação é solicitada

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

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Tipo de despesa	Participação			
	Número	DD/DND	dos países da EFTA	dos países candidatos	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
	Nenhuma		SIM/NÃO	SIM/NÃO	SIM/NÃO	SIM/NÃO

[13] DD = dotações diferenciadas/DND = dotações não diferenciadas.
[14] EFTA: Associação Europeia de Comércio Livre.
[15] Países candidatos e, se aplicável, países candidatos potenciais dos Balcãs Ocidentais.

3.2. Impacto financeiro estimado da proposta nas dotações

3.2.1. Síntese do impacto estimado nas dotações operacionais

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

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

Em milhões de EUR (três casas decimais)

Rubrica do quadro financeiro plurianual	1 a 6	Rubricas que abrangem as contribuições para os órgãos e organismos descentralizados

DG: Diversas			Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**TOTAL**
○ Dotações operacionais								
Rubricas orçamentais que abrangem as contribuições da União para organismos descentralizados (xx 10 xx xx)[16]	Autorizações	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamentos	(2 a)	2,459	2,459	2,459	2,459	2,459	12,293
Dotações de natureza administrativa financiadas a partir da dotação de programas específicos[17]								
Rubrica orçamental		(3)						
TOTAL das dotações para a DG: Diversas	Autorizações	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamentos	=2a+2b	2,459	2,459	2,459	2,459	2,459	12,293

[16] De acordo com a nomenclatura orçamental oficial.

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

		+3						

○ TOTAL das dotações operacionais	Autorizações	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamentos	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)						
TOTAL das dotações ao abrigo das RUBRICAS 1 a 6 do quadro financeiro plurianual	Autorizações	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamentos	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

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

○ TOTAL das dotações operacionais (todas as rubricas operacionais)	Autorizações	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamentos	(5)	2,459	2,459	2,459	2,459	2,459	12,293
TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos (todas as rubricas operacionais)		(6)						
TOTAL das dotações ao abrigo das RUBRICAS 1 a 6 do quadro financeiro plurianual (Montante de referência)	Autorizações	=4+ 6	2,459	2,459	2,459	2,459	2,459	12,293
	Pagamentos	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

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

Esta secção deve ser preenchida com «dados orçamentais de natureza administrativa» a inserir em primeiro lugar no anexo da ficha financeira legislativa (anexo V das regras internas), que é carregado no DECIDE para efeitos das consultas interserviços.

Em milhões de EUR (três casas decimais)

		Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	**Ano 2027**	**TOTAL**
DG: DIGIT (CERT-UE)							
○ Recursos humanos		1,184	2,126	2,754	3,225	3,225	12,514
○ Outras despesas administrativas		7,938	8,921	8,921	8,921	8,921	43,622
TOTAL DG DIGIT (CERT-UE)	Dotações	9,122	11,047	11,675	12,146	12,146	56,136

TOTAL das dotações no âmbito da RUBRICA 7 do quadro financeiro plurianual	(Total das autorizações = Total dos pagamentos)	9,122	11,047	11,675	12,146	12,146	**56,136**

Em milhões de EUR (três casas decimais)

		Ano 2023	Ano 2024	Ano 2025	Ano 2026	Ano 2027	**TOTAL**
TOTAL das dotações ao abrigo das RUBRICAS 1 a 7 do quadro financeiro plurianual (*)	Autorizações	11,581	13,506	14,134	14,605	14,605	68,429
	Pagamentos	11,581	13,506	14,134	14,605	14,605	68,429

(*) Prevê-se que as contribuições das instituições, órgãos e organismos autofinanciados da União sejam de 2,670 milhões de EUR por ano (13,350 milhões de EUR no total dos cinco anos). As contribuições constituirão receitas afetadas à CERT-UE. Os quadros acima contêm apenas o impacto total estimado no orçamento da União, não incluindo essas contribuições.

3.2.2. Estimativa das realizações financiadas com dotações operacionais

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

Indicar os objetivos e as realizações ⇩			Ano **N**		Ano **N+1**		Ano **N+2**		Ano **N+3**		Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)						**TOTAL**	
	REALIZAÇÕES																	
	Tipo[18]	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º Total	Custo total
OBJETIVO ESPECÍFICO N.º 1[19]…																		
- Realização																		
- Realização																		
- Realização																		
Subtotal do objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2…																		
- Realização																		
Subtotal do objetivo específico n.º 2																		
TOTAIS																		

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

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

3.2.3. Síntese do impacto estimado nas dotações de natureza administrativa

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

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

Em milhões de EUR (três casas decimais)

	Ano 2023	Ano 2024	Ano 2025	Ano 2026	Ano 2027	**TOTAL**
RUBRICA 7 do quadro financeiro plurianual						
Recursos humanos						
Pessoal permanente (Graus AD)	1,099	2,041	2,669	3,14	3,14	12,089
Agentes contratuais	0,085	0,085	0,085	0,085	0,085	0,425
Outras despesas administrativas	7,938	8,921	8,921	8,921	8,921	43,622
Subtotal RUBRICA 7 do quadro financeiro plurianual	9,122	11,047	11,675	12,146	12,146	56,136

Com exclusão da RUBRICA 7[20] do quadro financeiro plurianual						
Recursos humanos						
Outras despesas de natureza administrativa						
Subtotal com exclusão da RUBRICA 7 do quadro financeiro plurianual						

TOTAL	9,122	11,047	11,675	12,146	12,146	56,136

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

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

3.2.3.1. Necessidades estimadas de recursos humanos

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

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

As estimativas devem ser expressas em termos de equivalente a tempo completo.

	Ano 2023	Ano 2024	Ano 2025	Ano 2026	Ano 2027
O Lugares do quadro do pessoal (funcionários e agentes temporários)					
20 01 02 01 (na sede e nos gabinetes de representação da Comissão)	7	13	17	20	20
20 01 02 03 (nas delegações)					
01 01 01 01 (investigação indireta)					
01 01 01 11 (investigação direta)					
Outras rubricas orçamentais (especificar)					
O Pessoal externo (em equivalente a tempo completo: ETC)[21]					
20 02 01 (AC, PND e TT da «dotação global»)	1	1	1	1	1
20 02 03 (AC, AL, PND, TT e JPD nas delegações)					
XX 01 xx **yy zz** [22] - na sede					
XX 01 xx **yy zz** [22] - nas delegações					
01 01 01 02 (AC, PND, TT — Investigação indireta)					
01 01 01 12 (AC, PND, TT — Investigação direta)					
Outras rubricas orçamentais (especificar)					
TOTAL	**8**	**14**	**18**	**21**	**21**

XX constitui o domínio de intervenção ou título em causa.

As necessidades em matéria de recursos humanos serão cobertas pelo pessoal da DG já afetado à gestão da ação e/ou reafetado na DG e, se necessário, pelas eventuais afetações adicionais à DG gestora que podem ser realizadas no âmbito do processo de afetação anual e atendendo às restrições orçamentais.

Descrição das tarefas a executar:

Funcionários e agentes temporários	Os funcionários executarão as tarefas e atividades do CERT-UE em conformidade com o regulamento, em especial os capítulos IV e V.
Pessoal externo	O agente contratual assistirá as funções de secretariado do Conselho Interinstitucional para a Cibersegurança.

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

[22] Sublimite máximo para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

A proposta/iniciativa:

– ☑ pode ser integralmente financiada por meio da reafetação de fundos no quadro da rubrica em causa do quadro financeiro plurianual (QFP).

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

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

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

– ☐ implica uma revisão do QFP.

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

3.2.5. Participações de terceiros

A proposta/iniciativa:

– ☑ não prevê o cofinanciamento por terceiros[23]

– ☐ prevê o cofinanciamento por terceiros a seguir estimado:

Dotações em milhões de EUR (três casas decimais)

	Ano **N**[24]	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)			Total
Especificar o organismo de cofinanciamento								
TOTAL das dotações cofinanciadas								

[23] As receitas afetadas provenientes da prestação esporádica de serviços a organizações que não sejam constituintes, prevista no artigo 12.º, n.º 5, alínea c), não foram estimadas, uma vez que se prevê que sejam marginais.

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

3.3. Impacto estimado nas receitas

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

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

– ☐ nos recursos próprios

– ☐ noutras receitas

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

Em milhões de EUR (três casas decimais)

Rubrica orçamental das receitas:	Dotações disponíveis para o exercício em curso	Impacto da proposta/iniciativa[25]						
		Ano **N**	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)		
Artigo ……								

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

Outras observações [por exemplo, método/fórmula utilizado(a) para o cálculo do impacto sobre as receitas ou qualquer outra informação].

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