UNIÃO EUROPEIA

PARLAMENTO EUROPEU **CONSELHO**

Bruxelas, 29 de novembro de 2023
(OR. en)

2022/0085 (COD) **PE-CONS 57/23**

CYBER 215
TELECOM 267
INST 341
CSC 445
CSCI 163
INF 206
FIN 928
BUDGET 27
DATAPROTECT 236
CODEC 1607

ATOS LEGISLATIVOS E OUTROS INSTRUMENTOS

Assunto:	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

REGULAMENTO (UE, Euratom) 2023/…
DO PARLAMENTO EUROPEU E DO CONSELHO

de …

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[1],

[1] Posição do Parlamento Europeu de 21 de novembro de 2023 (ainda não publicada no Jornal Oficial) e decisão do Conselho de … .

Considerando o seguinte:

(1) Na era digital, as tecnologias da informação e comunicação constituem 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 as entidades da União mais vulneráveis a ameaças e incidentes informáticos, o que constitui uma ameaça à continuidade das suas atividades e à garantia de proteção dos seus dados. Embora o aumento da utilização dos serviços de computação em nuvem, o recurso generalizado às tecnologias da informação e comunicação (TIC), o elevado nível de digitalização, o trabalho à distância e a evolução tecnológica e da conectividade sejam características essenciais de todas as atividades das entidades da União, a resiliência digital ainda não foi suficientemente incorporada.

(2) O panorama das ciberameaças com que as entidades 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: furtar informações confidenciais valiosas, obter ganhos pecuniários, manipular a opinião pública ou comprometer as infraestruturas digitais. O ritmo a que os perpetradores conduzem tais ciberataques continua a intensificar-se, com atuações cada vez mais sofisticadas e automatizadas, que visam áreas de ataque expostas que continuam a expandir-se e a explorar rapidamente qualquer vulnerabilidade.

(3) Os ambientes das TIC das entidades da União apresentam interdependências e fluxos de dados integrados, e os seus utilizadores colaboram estreitamente entre si. Essa interligação implica que qualquer perturbação, mesmo que inicialmente confinada a uma única entidade da União, pode ter repercussões mais vastas e resultar em impactos negativos generalizados e duradouros noutras entidades da União. Além disso, os ambientes das TIC de certas entidades da União estão ligados aos ambientes das TIC dos Estados-Membros, levando a que um incidente numa entidade da União possa representar um risco de cibersegurança para os ambientes das TIC dos Estados-Membros e vice-versa. A partilha de informações específicas sobre incidentes poderá facilitar a deteção de ciberameaças ou incidentes semelhantes que afetem os Estados-Membros.

(4) As entidades da União constituem 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 as capacidades de deteção e resposta a atividades informáticas maliciosas variam significativamente entre essas entidades. Para assegurar o correto funcionamento das entidades da União, é, portanto, necessário que estas atinjam um elevado nível comum de cibersegurança por meio da aplicação de medidas de cibersegurança proporcionais aos riscos de cibersegurança identificados, do intercâmbio de informações e da colaboração.

(5) A Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[1] visa reforçar a ciber-resiliência e as capacidades de resposta a incidentes das entidades públicas e privadas, das autoridades e organismos competentes e da União no seu conjunto. Por conseguinte, é necessário que as entidades da União sigam o mesmo exemplo, assegurando a existência de regras coerentes com a Diretiva (UE) 2022/2555 e que reflitam o seu nível de ambição.

(6) Para garantir um elevado nível comum de cibersegurança, será necessário que cada entidade da União estabeleça um regime interno de gestão, governação e controlo dos riscos de cibersegurança («regime») que 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. O regime deverá estabelecer políticas em matéria de cibersegurança, incluindo objetivos e prioridades, para a segurança dos sistemas de rede e informação que abranjam a totalidade do ambiente das TIC não classificado. O regime deverá basear-se numa abordagem multirriscos que visa a proteção dos sistemas de rede e informação, bem como do ambiente físico desses sistemas, contra incidentes como furtos, incêndios, inundações, falhas de telecomunicações ou de energia, ou contra o acesso físico não autorizado e danos às informações e às instalações de tratamento de informações de uma entidade da União, ou interferências em tais informações e instalações, suscetíveis de comprometer a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos, tratados ou acessíveis através sistemas de rede e informação.

---

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

(7) Para gerir os riscos de cibersegurança identificados no âmbito do regime, cada entidade da União deverá tomar as medidas técnicas, operacionais e organizacionais adequadas e proporcionadas. Essas medidas deverão abordar os domínios e as medidas de gestão dos riscos de cibersegurança previstos no presente regulamento para reforçar a cibersegurança de cada entidade da União.

(8) Os ativos e os riscos de cibersegurança identificados no regime, bem como as conclusões tiradas de avaliações periódicas da maturidade em matéria de cibersegurança deverão ser refletidos no plano de cibersegurança estabelecido por cada entidade da União. O plano de cibersegurança deverá incluir as medidas de gestão dos riscos de cibersegurança adotadas.

(9) Uma vez que garantir a cibersegurança é um processo contínuo, a adequação e eficácia das medidas tomadas em conformidade com o presente regulamento deverão ser periodicamente revistas tendo em conta a evolução dos riscos de cibersegurança, dos ativos e da maturidade da cibersegurança das entidades da União. O regime deverá ser reexaminado periodicamente e, pelo menos, de quatro em quatro anos, ao passo que o plano de cibersegurança deverá ser reexaminado de dois em dois anos, ou mais frequentemente se necessário, na sequência de avaliações da maturidade em matéria de cibersegurança ou de cada reexame importante do regime.

(10) As medidas de gestão dos riscos de cibersegurança adotadas pelas entidades da União deverão incluir políticas destinadas, sempre que possível, a tornar o código-fonte transparente, tendo em conta as salvaguardas dos direitos de terceiros ou entidades da União. Essas políticas deverão ser proporcionais ao risco de cibersegurança e destinam-se a facilitar a análise das ciberameaças, sem criar obrigações de divulgação ou direitos de acesso a códigos de terceiros além das condições contratuais aplicáveis.

(11) As ferramentas e aplicações de código aberto em matéria de cibersegurança podem contribuir para um maior grau de abertura. As normas abertas facilitam a interoperabilidade entre as ferramentas de segurança, com benefícios para a segurança dos intervenientes. As ferramentas e aplicações de código aberto em matéria de cibersegurança podem mobilizar a comunidade mais ampla de programadores, o que permite diversificar os fornecedores. A fonte aberta pode conduzir a um processo de verificação mais transparente das ferramentas relacionadas com a cibersegurança e a um processo comunitário de deteção de vulnerabilidades. As entidades da União deverão, por conseguinte, estar em condições de promover a utilização de software de código aberto e de normas abertas, aplicando políticas relativas à utilização de dados abertos e de fontes abertas no regime da segurança através da transparência.

(12) As diferenças existentes entre as entidades da União exigem flexibilidade na aplicação do presente regulamento. As medidas destinadas a garantir um elevado nível comum de cibersegurança, dispostas no presente regulamento, não deverão incluir nenhuma obrigação que interfira diretamente no exercício das missões das entidades da União ou prejudique a sua autonomia institucional. Por conseguinte, essas entidades deverão estabelecer os seus próprios regimes e adotar as suas próprias medidas de gestão dos riscos de cibersegurança e planos de cibersegurança. Aquando da aplicação de tais medidas, deverão ser tidas devidamente em conta as sinergias existentes entre as entidades da União, com o objetivo de garantir a gestão adequada dos recursos e a otimização dos custos. Importa também assegurar que as medidas não afetem negativamente a eficiência do intercâmbio de informações e a cooperação entre entidades da União e entre as entidades da União e as contrapartes dos Estados-Membros.

(13) A fim de otimizar a utilização dos recursos, o presente regulamento deverá prever a possibilidade de duas ou mais entidades da União com estruturas semelhantes cooperarem na realização das avaliações da maturidade em matéria de cibersegurança das respetivas entidades.

(14) Para evitar impor encargos financeiros e administrativos desproporcionados às entidades da União, os requisitos de gestão dos riscos de cibersegurança deverão ser proporcionados em relação ao risco de cibersegurança para os sistemas de rede e informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas. Cada entidade da União deverá procurar afetar uma percentagem adequada do seu orçamento destinado às TIC à melhoria do respetivo nível de cibersegurança. A mais longo prazo deverá procurar-se alcançar uma meta indicativa da ordem dos 10 %, no mínimo. A avaliação da maturidade em matéria de cibersegurança deverá ainda apreciar se as despesas de uma determinada entidade da União no domínio da cibersegurança são proporcionais aos riscos de cibersegurança que a mesma enfrenta. Sem prejuízo das regras relativas ao orçamento anual da União ao abrigo dos Tratados, na sua proposta para o primeiro orçamento anual a adotar após a entrada em vigor do presente regulamento, a Comissão deverá ter em conta as obrigações decorrentes do presente regulamento ao avaliar as necessidades orçamentais e de pessoal das entidades da União resultantes das suas estimativas de despesas.

(15) Um elevado nível comum de cibersegurança exige que esses aspetos sejam supervisionados pela direção ao mais alto nível de cada entidade da União. A direção ao mais alto nível da entidade da União deverá ser responsável pela aplicação do presente regulamento, nomeadamente pela criação do regime, pela adoção de medidas de gestão dos riscos de cibersegurança e pela aprovação do plano de cibersegurança. A cultura de cibersegurança, que corresponde às práticas de rotina em termos de segurança informática, constituirá parte integrante do regime e das medidas de gestão dos riscos de cibersegurança correspondentes em todas as entidades da União.

(16) A segurança dos sistemas de rede e informação que tratam informações classificadas da UE (ICUE) é essencial. As entidades da União que tratam ICUE são obrigadas a aplicar os regimes regulamentares abrangentes em vigor para proteger essas informações, incluindo procedimentos específicos de governação, políticas e gestão de riscos. É necessário que os sistemas de rede e informação que tratam ICUE cumpram normas de segurança mais rigorosas do que os sistemas de rede e informação que tratam informações não classificadas. Por conseguinte, os sistemas de rede e informação que tratam ICUE são mais resilientes às ciberameaças e aos incidentes de cibersegurança. Assim, embora reconhecendo a necessidade de um regime comum a este respeito, o presente regulamento não deverá aplicar-se aos sistemas de rede e informação que tratam ICUE. No entanto, se tal for explicitamente solicitado por uma entidade da União, a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) deverá poder prestar assistência a essa entidade da União em relação a incidentes em ambientes das TIC classificados.

(17) As entidades da União deverão avaliar os riscos de cibersegurança 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. As medidas de cibersegurança deverão ser especificadas em orientações ou recomendações emitidas pela CERT-UE. No estabelecimento das medidas e orientações, deverão ser tidos em devida conta os progressos técnicos mais recentes e, se aplicável, as normas europeias e internacionais pertinentes, bem como o direito e as políticas pertinentes da União, incluindo as avaliações dos risco de cibersegurança e as recomendações emitidas pelo grupo de cooperação criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555, como a avaliação coordenada da avaliação dos riscos de cibersegurança das redes 5G, por parte da UE, e o conjunto de instrumentos da UE para a cibersegurança das redes 5G. Além disso, tendo em conta o panorama das ciberameaças e a importância de reforçar a ciber-resiliência das entidades da União, poderá ser exigida a certificação de produtos, serviços e processos de TIC pertinentes, ao abrigo de sistemas europeus específicos de certificação da cibersegurança adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[1].

[1] 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).

(18) Em maio de 2011, os secretários-gerais das instituições e organismos da União decidiram criar uma pré-configuração da 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 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[1]. O presente regulamento deverá proporcionar um conjunto abrangente de regras relativas à organização, ao funcionamento e à operação da CERT-UE. As disposições do presente regulamento prevalecem sobre as disposições do acordo interinstitucional sobre a organização e o funcionamento da CERT-UE celebrado em dezembro de 2017.

(19) A CERT-UE deverá mudar o seu nome para Serviço de Cibersegurança para as instituições, órgãos e organismos da União, mas deverá manter-se a designação abreviada «CERT-UE», devido ao reconhecimento do nome.

---

1 Acordo entre o Parlamento Europeu, o Conselho Europeu, o Conselho da União Europeia, a Comissão Europeia, o Tribunal de Justiça da União Europeia, o Banco Central Europeu, o Tribunal de Contas Europeu, o Serviço Europeu para a Ação Externa, o Comité Económico e Social Europeu, o Comité das Regiões Europeu e o Banco Europeu de Investimento sobre a organização e o funcionamento de uma equipa de resposta a emergências informáticas das instituições, órgãos e organismos da União (CERT-UE) (JO C 12 de 13.1.2018, p. 1).

(20) Para além da afetação de novas atribuições e de conferir um papel mais interventivo à CERT-UE, o presente regulamento deverá criar o Conselho Interinstitucional para a Cibersegurança (IICB, do inglês Interinstitutional Cybersecurity Board)., a fim de facilitar um elevado nível comum de cibersegurança entre as entidades da União. O IICB deverá desempenhar um papel exclusivo no acompanhamento e apoio da forma como as entidades da União aplicam o presente regulamento, supervisionando a concretização das prioridades e objetivos gerais da CERT-UE e conferindo-lhe uma direção estratégica. Por conseguinte, o IICB deverá assegurar a representação das instituições da União e deverá integrar representantes dos órgãos e organismos da União por meio da Rede de Agências da UE. A organização e o funcionamento do IICB deverão ser regulados, além disso, pelo respetivo regulamento interno, que poderá incluir regras pormenorizadas para as reuniões periódicas do IICB, nomeadamente as reuniões anuais a nível político nas quais os representantes da direção ao mais alto nível de cada membro do IICB poderiam ter um debate estratégico e formular orientações estratégicas para o IICB. Além disso, o IICB deverá poder criar um comité executivo para o assistir nos seus trabalhos e delegar nele algumas das suas atribuições e competências, em especial no que se refere às atribuições que exigem conhecimentos especializados dos seus membros, por exemplo, a aprovação do catálogo de serviços e eventuais atualizações do mesmo, termos dos acordos de nível de serviço, avaliações de documentos e relatórios emitidos pelas entidades da União para o IICB nos termos do presente regulamento, ou atribuições relacionadas com a preparação de decisões sobre medidas de conformidade emitidas pelo IICB e com o acompanhamento da sua aplicação. Cabe ao IICB estabelecer o regulamento interno do comité executivo, incluindo as respetivas atribuições e poderes.

(21) O IICB tem por objetivo apoiar as entidades da União a melhorar as respetivas posturas de cibersegurança graças à aplicação do presente regulamento. A fim de apoiar as entidades da União, o IICB deverá dar orientações ao diretor da CERT-UE, adotar uma estratégia plurianual para aumentar o nível de cibersegurança nas entidades da União, estabelecer a metodologia e outros aspetos das avaliações voluntárias pelos pares e facilitar a criação de um grupo informal de agentes locais da cibersegurança, apoiado pela Agência da União Europeia para a Cibersegurança (ENISA), com o objetivo de proceder ao intercâmbio de boas práticas e de informações relacionadas com a aplicação do presente regulamento.

(22) A fim de alcançar um elevado nível de cibersegurança em todas as entidades da União, os interesses dos órgãos e organismos da União que gerem o seu próprio ambiente de TIC deverão ser representados no IICB por três representantes designados pela Rede de Agências da UE. A segurança do tratamento de dados pessoais e, por conseguinte, também a sua cibersegurança constituem uma pedra angular da proteção de dados. À luz das sinergias entre a proteção de dados e a cibersegurança, a Autoridade Europeia para a Proteção de Dados deverá estar representada no IICB na sua qualidade de entidade da União abrangida pelo presente regulamento, com conhecimentos especializados específicos no domínio da proteção de dados, incluindo a segurança das redes de comunicações eletrónicas. Tendo em conta a importância da inovação e da competitividade no domínio da cibersegurança, o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança deverá estar representado no IICB. Tendo em vista o papel da ENISA enquanto centro de conhecimentos especializados em cibersegurança e o apoio prestado pela ENISA, e tendo em vista a importância da cibersegurança das infraestruturas e serviços espaciais da União, a ENISA e a Agência da União Europeia para o Programa Espacial deverão estar representadas no IICB. À luz do papel atribuído à CERT-UE ao abrigo do presente regulamento, o presidente do IICB deverá convidar o diretor da CERT-UE para todas as reuniões do IICB, exceto se o IICB debater questões diretamente relacionadas com o diretor da CERT-UE.

(23) O IICB deverá acompanhar o cumprimento do presente regulamento e a aplicação das suas orientações e recomendações, bem como aos apelos à ação. O IICB deverá ser apoiado em questões técnicas por grupos consultivos técnicos, com a composição que o IICB entenda. Esses grupos consultivos técnicos deverão trabalhar em estreita cooperação com a CERT-UE, as entidades da União e outras partes interessadas, conforme necessário.

(24) Quando concluir que a entidade da União não aplicou eficazmente o presente regulamento nem as orientações, as recomendações ou os apelos à ação emitidos ao abrigo do presente regulamento, o IICB deverá poder, sem prejuízo dos procedimentos internos da entidade da União em causa, avançar com medidas de conformidade. O IICB deverá aplicar medidas de conformidade de forma progressiva - ou seja, o IICB deverá, em primeiro lugar, adotar a medida menos severa, a saber, um parecer fundamentado e apenas se necessário medidas cada vez mais severas, culminando na medida mais severa, a saber, uma recomendação de suspensão temporária dos fluxos de dados para a entidade da União em causa. Essa recomendação só deverá ser aplicada em casos excecionais de infração prolongada, deliberada, reiterada ou grave ao presente regulamento por parte da entidade da União em causa.

(25) O parecer fundamentado representa a medida de conformidade menos severa para colmatar as lacunas observadas na aplicação do presente regulamento. O IICB deverá poder dar seguimento a um parecer fundamentado com orientações para ajudar a entidade da União a assegurar que o seu regime, medidas de gestão dos riscos de cibersegurança, plano de cibersegurança e comunicação de informações cumpram o disposto no presente regulamento e, em seguida, através de um alerta para corrigir, num prazo especificado, as deficiências identificadas na entidade da União. Se as deficiências identificadas no alerta não tiverem sido suficientemente corrigidas, o IICB deverá poder emitir uma notificação fundamentada.

(26) O IICB deverá poder recomendar a realização de uma auditoria a uma entidade da União. A entidade da União deverá poder recorrer à sua função de auditoria interna para este efeito. O IICB deverá ainda poder solicitar a realização de uma auditoria por um terceiro prestador de serviços de auditoria, nomeadamente por um prestador de serviços do setor privado mutuamente acordado.

(27) Em casos excecionais de infração prolongada, deliberada, reiterada ou grave ao presente regulamento por parte de uma entidade da União, o IICB deverá poder recomendar, como medida de último recurso, a todos os Estados-Membros e a todas as entidades da União, a suspensão temporária dos fluxos de dados para a entidade da União em causa, suspensão que produzirá efeitos até que a entidade da União ponha fim à infração. Essa recomendação deverá ser comunicada através de canais de comunicação adequados e seguros.

(28) A fim de assegurar a correta aplicação do presente regulamento, o IICB deverá, se considerar que uma infração persistente do presente regulamento por parte de uma entidade da União foi causada diretamente por ações ou omissões de um membro do seu pessoal, inclusive da direção ao mais alto nível, solicitar à entidade da União em causa que tome as medidas adequadas, nomeadamente solicitando-lhe que pondere tomar medidas de natureza disciplinar, em conformidade com as regras e os procedimentos estabelecidos no Estatuto dos Funcionários da União Europeia e no Regime Aplicável aos Outros Agentes da União Europeia, estabelecidos no Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho[1] («Estatuto dos Funcionários») e quaisquer outras regras e procedimentos aplicáveis.

(29) A CERT-UE deverá contribuir para a segurança do ambiente de TIC de todas as entidades da União. Ao ponderar prestar aconselhamento técnico ou informações técnicas sobre questões estratégicas pertinentes a pedido de uma entidade da União, a CERT-UE deverá assegurar que tal não constitui um obstáculo à realização de outras atribuições conferidas nos termos do presente regulamento. A CERT-UE deverá exercer, em nome das entidades da União, uma função equivalente à do coordenador designado para fins de divulgação coordenada das vulnerabilidades, nos termos do artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555.

---

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

(30) A CERT-UE deverá apoiar a aplicação de medidas destinadas a garantir um elevado nível comum de cibersegurança por meio da apresentação de propostas de orientações e recomendações ao IICB ou emitindo apelos à ação. As referidas orientações e recomendações deverão ser aprovadas pelo IICB. Sempre que necessário, a CERT-UE deverá emitir apelos à ação descrevendo medidas de segurança urgentes que as entidades da União são instadas a tomar num determinado prazo. O IICB deverá dar instruções à CERT-UE no sentido de que esta emita, retire ou modifique uma proposta de orientações ou de recomendação, ou um apelo à ação.

(31) A CERT-UE deverá também desempenhar o papel que lhe é conferido pela Diretiva (UE) 2022/2555 em matéria de cooperação e intercâmbio de informações com a rede de equipas de resposta a incidentes de segurança informática (CSIRT) criada nos termos do artigo 15.º da referida diretiva. Além disso, em consonância com a Recomendação (UE) 2017/1584 da Comissão[1], a CERT-UE deverá cooperar e coordenar uma resposta com as partes interessadas relevantes. A fim de contribuir para um elevado nível de cibersegurança na União, a CERT-UE deverá partilhar informações específicas sobre incidentes com as suas contrapartes dos Estados-Membros. A CERT-UE deverá igualmente colaborar com outras contrapartes públicas e privadas, nomeadamente da Organização do Tratado do Atlântico Norte, sob reserva da aprovação prévia do IICB.

---

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

(32) No apoio à cibersegurança operacional, a CERT-UE deverá recorrer aos conhecimentos especializados disponíveis da ENISA por meio de uma cooperação estruturada, conforme previsto no Regulamento (UE) 2019/881. Se for caso disso, deverão ser acordadas entre as duas entidades as disposições adequadas para definir o modo de pôr em prática essa cooperação e evitar a duplicação de atividades. A CERT-UE deverá cooperar com a ENISA na análise das ciberameaças e partilhar periodicamente com a ENISA o seu relatório sobre o panorama das ameaças.

(33) A CERT-UE deverá poder cooperar e trocar informações com as comunidades de cibersegurança pertinentes na União e nos seus Estados-Membros, de forma a promover a cooperação operacional e permitir que as redes existentes realizem todo o seu potencial na proteção da União.

(34) Uma vez que os serviços e as atribuições da CERT-UE assumem interesse para as entidades da União, cada uma dessas entidades que suporte despesas no domínio das TIC deverá contribuir com uma parte equitativa para esses serviços e atribuições. Essa contribuição não prejudica a autonomia orçamental das entidades da União.

(35) Muitos ciberataques enquadram-se em campanhas mais alargadas que visam grupos de entidades da União ou comunidades de interesse que incluem entidades da União. A fim de permitir a deteção pró-ativa, a resposta em caso de incidente ou a tomada de medidas de atenuação e a recuperação de incidentes, as entidades da União deverão poder informar a CERT-UE dos incidentes, ciberameaças, vulnerabilidades e quase incidentes, bem como partilhar pormenores técnicos adequados para permitir a deteção, atenuação ou resposta a incidentes, ciberameaças, vulnerabilidades e quase incidentes similares que possam afetar outras entidades da União. Aplicando a mesma abordagem da Diretiva (UE) 2022/2555, as entidades da União deverão enviar um alerta rápido à CERT-UE no prazo de 24 horas depois de terem tomado conhecimento de um incidente significativo. Esse intercâmbio de informações deverá permitir à CERT-UE divulgar as informações a outras entidades da União, bem como às devidas contrapartes, de forma a proteger os ambientes das TIC, tanto das entidades da União como das suas contrapartes, contra incidentes semelhantes.

(36) O presente regulamento estabelece uma abordagem com várias etapas para a notificação de incidentes significativos, por forma a encontrar o equilíbrio adequado entre, por um lado, uma notificação célere que ajude a atenuar a potencial disseminação de incidentes significativos e permita às entidades da União procurar assistência e, por outro lado, uma notificação aprofundada que permita retirar ensinamentos importantes de incidentes individuais e melhorar ao longo do tempo a ciber-resiliência das entidades individuais da União e contribuir para aumentar a sua postura global em matéria de cibersegurança. A este respeito, o presente regulamento deverá incluir a notificação de informações relativas a incidentes que, com base numa avaliação inicial efetuada pela entidade da União em causa, poderiam causar graves perturbações operacionais no funcionamento da entidade da União em causa ou perdas financeiras para a mesma, ou afetar outras pessoas singulares ou coletivas causando danos materiais ou imateriais consideráveis. Essa avaliação inicial deverá ter em conta, nomeadamente, os sistemas de rede e informação afetados, em especial a sua importância para o funcionamento da entidade da União, a gravidade e as características técnicas da ciberameaça e quaisquer vulnerabilidades subjacentes que estejam a ser exploradas, bem como a experiência da entidade da União com incidentes semelhantes. Indicadores como a medida em que o funcionamento da entidade da União é afetado, a duração de um incidente ou o número de pessoas singulares ou coletivas afetadas poderão desempenhar um papel importante para determinar se a perturbação operacional é grave.

(37) Visto que as infraestruturas e os sistemas de rede e informação da entidade da União pertinente e do Estado-Membro onde essa entidade da União se encontra estão interligados, é essencial que esse Estado-Membro em causa seja informado, sem demora injustificada, de um incidente significativo na entidade da União em causa. Para o efeito, a entidade da União afetada deverá informar as contrapartes pertinentes dos Estados-Membros designadas ou estabelecidas nos termos dos artigos 8.º e 10.º da Diretiva (UE) 2022/2555 da ocorrência de um incidente significativo sobre o qual informa a CERT-UE. Caso tome conhecimento de um incidente significativo ocorrido num Estado-Membro, a CERT-UE deverá informar quaisquer contrapartes relevantes nesse Estado-Membro.

(38) Deverá ser posto em funcionamento um mecanismo que assegure a eficácia do intercâmbio de informações, da coordenação e da cooperação das entidades da União em caso de incidentes graves, incluindo a determinação clara das funções e responsabilidades das entidades da União envolvidas. O representante da Comissão no IICB deverá, sob reserva do plano de gestão de cibercrises, ser o ponto de contacto para facilitar a partilha, por parte do IICB, de informações pertinentes sobre incidentes graves com a Rede europeia de organizações de coordenação de cibercrises (UE-CyCLONe), como contributo para o conhecimento comum da situação. O papel do representante da Comissão no IICB como ponto de contacto não deverá prejudicar o papel separado e distinto da Comissão na UE-CyCLONe, nos termos do artigo 16.º, n.º 2, da Diretiva (UE) 2022/2555.

(39) O Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[1] é aplicável a todo o tratamento de dados pessoais ao abrigo do presente regulamento. O tratamento de dados pessoais pode ter lugar em relação a medidas adotadas no contexto da gestão dos riscos de cibersegurança, do tratamento de vulnerabilidades e incidentes, da partilha de informações sobre incidentes, ciberameaças e vulnerabilidades, e da coordenação e cooperação da resposta a incidentes. Tais medidas poderão exigir o tratamento de determinadas categorias de dados pessoais, tais como endereços IP, localizadores uniformes de recursos (URL), nomes de domínio, endereços de correio eletrónico, funções organizacionais do titular dos dados, carimbos temporais, assuntos do correio eletrónico ou nomes de ficheiros. Todas as medidas tomadas nos termos do presente regulamento deverão respeitar o regime de proteção de dados e privacidade, e as entidades da União, a CERT-UE e, se for caso disso, o IICB, deverão adotar todas as salvaguardas técnicas e organizativas pertinentes para assegurar esse cumprimento de forma responsável.

(40) O presente regulamento estabelece a base jurídica para o tratamento de dados pessoais pelas entidades da União, pela CERT-UE e, se for caso disso, pelo IICB, para efeitos do exercício das suas atribuições e do cumprimento das obrigações que lhes incumbem por força do presente regulamento, em conformidade com o artigo 5.º, n.º 1, alínea b), do Regulamento (UE) 2018/1725. A CERT-UE pode atuar como subcontratante ou responsável pelo tratamento, dependendo da função que desempenha nos termos do Regulamento (UE) 2018/1725.

---

[1] 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).

(41) Em certos casos, para efeitos do cumprimento das obrigações que lhes incumbem por força do presente regulamento a fim de assegurar um elevado nível de cibersegurança e, em especial, no contexto do tratamento de vulnerabilidades e incidentes, pode ser necessário que as entidades da União e a CERT-UE tratem categorias especiais de dados pessoais, tal como referido no artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725. O presente regulamento estabelece a base jurídica para o tratamento de categorias especiais de dados pessoais pelas entidades da União e pela CERT-UE, em conformidade com o artigo 10.º, n.º 2, alínea g), do Regulamento (UE) 2018/1725. O tratamento de categorias especiais de dados pessoais ao abrigo do presente regulamento deverá ser estritamente proporcional ao objetivo prosseguido. Sob reserva das condições estabelecidas no artigo 10.º, n.º 2, alínea g), do referido regulamento, as entidades da União e a CERT-UE deverão poder tratar esses dados apenas na medida do necessário e quando explicitamente previsto no presente regulamento. Ao tratar categorias especiais de dados pessoais, as entidades da União e a CERT-UE deverão respeitar a essência do direito à proteção de dados e prever medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses dos titulares dos dados.

(42) Nos termos do artigo 33.º do Regulamento (UE) 2018/1725, as entidades da União e a CERT-UE, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e as liberdades das pessoas singulares, deverão aplicar medidas técnicas e organizativas apropriadas para assegurar um nível adequado de segurança dos dados pessoais, como a concessão de direitos de acesso limitados em função da necessidade de tomar conhecimento, a aplicação dos princípios da pista de auditoria, a adoção de uma cadeia de custódia, o armazenamento de dados em repouso num ambiente controlado e passível de auditoria, procedimentos operacionais normalizados e medidas de preservação da privacidade, como a pseudonimização ou a cifragem. Essas medidas não deverão ser aplicadas de forma a afetar os objetivos do tratamento de incidentes e a integridade das provas. Caso uma entidade da União ou a CERT-UE transfira dados pessoais relacionados com um incidente, incluindo categorias especiais de dados pessoais, para uma contraparte ou um parceiro para efeitos do presente regulamento, essas transferências deverão cumprir o disposto no Regulamento (UE) 2018/1725. Caso sejam transferidas categorias especiais de dados pessoais para terceiros, as entidades da União e a CERT-UE deverão assegurar que o terceiro aplica medidas relativas à proteção de dados pessoais a um nível equivalente ao do Regulamento (UE) 2018/1725.

(43) Os dados pessoais tratados para efeitos do presente regulamento só deverão ser conservados durante o tempo necessário, em conformidade com o Regulamento (UE) 2018/1725. As entidades da União e, se aplicável, a CERT-UE agindo na qualidade de responsável pelo tratamento, deverão fixar períodos de conservação limitados ao necessário para alcançar as finalidades especificadas. Especialmente no que diz respeito aos dados pessoais recolhidos para o tratamento de incidentes, as entidades da União e a CERT-UE deverão prever uma distinção entre os dados pessoais recolhidos para a deteção de uma ciberameaça nos seus ambientes das TIC, a fim de prevenir um incidente, e os dados pessoais recolhidos para efeitos de atenuação, resposta e recuperação de um incidente. Para a deteção de uma ciberameaça, é importante ter em conta o tempo durante o qual um perpetrador de ameaças pode permanecer num sistema sem ser detetado. Para efeitos de atenuação, resposta e recuperação de um incidente, é importante ponderar se os dados pessoais são necessários para rastrear e tratar um incidente recorrente ou um incidente de natureza semelhante para o qual possa ser demonstrada uma correlação.

(44) O tratamento das informações pela CERT-UE e pelas entidades da União deverá cumprir as regras aplicáveis relativas à segurança da informação. A inclusão da segurança dos recursos humanos como medida de gestão dos riscos de cibersegurança deverá também cumprir as regras aplicáveis.

(45) Para efeitos de partilha de informações, são utilizadas marcações visíveis para indicar que existem restrições à partilha das informações pelos destinatários, com base em, em especial, acordos de não divulgação ou acordos de não divulgação informais, como o protocolo de sinalização luminosa ou outras indicações claras fornecidas pelo remetente. O protocolo de sinalização luminosa deverá ser visto como um meio para prestar informações sobre eventuais restrições impostas à divulgação ulterior das informações. É utilizado por quase todas as CSIRT e em alguns centros de análise e partilha de informações.

(46) O presente regulamento deverá ser avaliado com regularidade à luz de futuras negociações de quadros financeiros plurianuais que permitam a tomada de novas decisões relativamente ao funcionamento e ao papel institucional da CERT-UE, nomeadamente a possível instituição da CERT-UE como organismo da União.

(47) O IICB, com a assistência da CERT-UE, deverá analisar e avaliar a aplicação do presente regulamento, reportando à Comissão. Com base nessas informações, a Comissão deverá apresentar relatório ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Esse relatório, com o contributo do IICB, deverá avaliar a conveniência de incluir os sistemas de rede e informação que tratam ICUE no âmbito do presente regulamento, em especial na ausência de regras de segurança da informação comuns às entidades da União.

(48) De acordo com o princípio da proporcionalidade, é necessário e conveniente, para alcançar o objetivo fundamental de lograr um elevado nível comum de cibersegurança nas entidades da União, estabelecer normas em matéria de cibersegurança para as entidades da União. O presente regulamento não excede o necessário para alcançar o objetivo previsto, em cumprimento do artigo 5.º, n.º 4, do Tratado da União Europeia.

(49) O presente regulamento reflete o facto de as entidades da União divergirem em dimensão e capacidade, nomeadamente em termos de recursos financeiros e humanos.

(50) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 e emitiu um parecer em 17 de maio de 2022[1],

ADOTARAM O PRESENTE REGULAMENTO:

[1] JO C 258 de 5.7.2022, p. 10.

Capítulo I
Disposições gerais

Artigo 1.º

Objeto

O presente regulamento estabelece medidas destinadas a alcançar um elevado nível comum de cibersegurança nas entidades da União no respeitante ao seguinte:

a) Criação por cada entidade da União de um regime interno de gestão, governação e controlo dos riscos de cibersegurança nos termos do artigo 6.º;

b) Gestão e notificação dos riscos de cibersegurança, bem como partilha de informações sobre esses riscos;

c) Organização, funcionamento e operação do Conselho Interinstitucional para a Cibersegurança criado nos termos do artigo 10.º, bem como a organização, funcionamento e operação do Serviço de Cibersegurança para as instituições, órgãos e organismos da União (CERT-UE);

d) Acompanhamento da aplicação do presente regulamento.

Artigo 2.º

Âmbito

1. O presente regulamento é aplicável às entidades da União, ao Conselho Interinstitucional para a Cibersegurança criado nos termos do artigo 10.º e à CERT-UE.

2. O presente regulamento é aplicável sem prejuízo da autonomia institucional nos termos dos Tratados.

3. Com exceção do artigo 13.º, n.º 8, o presente regulamento não se aplica aos sistemas de rede e informação que tratem informações classificadas da UE (ICUE).

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Entidades da União», as instituições, órgãos e organismos criados nos termos do Tratado da União Europeia, do Tratado sobre o Funcionamento da União Europeia (TFUE) ou do Tratado que institui a Comunidade Europeia da Energia Atómica;

2) «Sistema de rede e informação», um sistema de rede e informação na aceção do artigo 6.º, ponto 1, da Diretiva (UE) 2022/2555;

3) «Segurança dos sistemas de rede e informação», a segurança dos sistemas de rede e informação na aceção do artigo 6.º, ponto 2, da Diretiva (UE) 2022/2555;

4) «Cibersegurança», a cibersegurança na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2019/881;

5) «Direção ao mais alto nível», um dirigente, um organismo de direção ou um organismo de coordenação e supervisão, que é responsável pelo funcionamento de uma entidade da União ao mais alto nível administrativo, incumbido de adotar ou autorizar decisões em conformidade com as disposições em matéria de governação ao mais alto nível da entidade da União em causa, sem prejuízo das responsabilidades formais que incumbam a outros níveis de direção pela conformidade e gestão dos riscos de cibersegurança nos respetivos domínios de responsabilidade;

6) «Quase incidente», um quase incidente na aceção do artigo 6.º, ponto 5, da Diretiva (UE) 2022/2555;

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

8) «Incidente grave», um incidente que causa um nível de perturbação que excede a capacidade de resposta de uma entidade da União e da CERT-UE ou que tem um impacto significativo em pelo menos duas entidades da União;

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

10) «Tratamento de incidentes», o tratamento de incidentes na aceção do artigo 6.º, ponto 8, da Diretiva (UE) 2022/2555;

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

12) «Ciberameaça significativa», uma ciberameaça significativa na aceção do artigo 6.º, ponto 11, da Diretiva (UE) 2022/2555;

13) «Vulnerabilidade», uma vulnerabilidade na aceção do artigo 6.º, ponto 15, da Diretiva (UE) 2022/2555;

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

15) «Serviço de computação em nuvem», um serviço de computação em nuvem na aceção do artigo 6.º, ponto 30, da Diretiva (UE) 2022/2555.

Artigo 4.º

Tratamento de dados pessoais

1. O tratamento de dados pessoais ao abrigo do presente regulamento pela CERT-UE, o Conselho Interinstitucional para a Cibersegurança criado nos termos do artigo 10.º e as entidades da União é efetuado nos termos do Regulamento (UE) 2018/1725.

2. Caso desempenhem funções ou cumpram obrigações nos termos do presente regulamento, a CERT-UE, o Conselho Interinstitucional para a Cibersegurança criado nos termos do artigo 10.º e as entidades da União tratam e procedem ao intercâmbio de dados pessoais apenas na medida do necessário e com o objetivo único de desempenhar essas funções ou de cumprir essas obrigações.

3. O tratamento de categorias especiais de dados pessoais a que se refere o artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725, é considerado necessário por motivos de interesse público importante, nos termos do artigo 10.º, n.º 2, alínea g), do mesmo regulamento. Esses dados só podem ser tratados na medida do necessário para a aplicação das medidas de gestão dos riscos de cibersegurança a que se referem os artigos 6.º e 8.º, para a prestação de serviços pela CERT-UE nos termos do artigo 13.º, a partilha de informações específicas sobre incidentes nos termos do artigo 17.º, n.º 3, e do artigo 18.º, n.º 3, para a partilha de informações nos termos do artigo 20.º, para as obrigações de comunicação de informações ao abrigo do artigo 21.º, para a coordenação e cooperação da resposta a incidentes nos termos do artigo 22.º e para a gestão de incidentes graves nos termos do artigo 23.º do presente regulamento. As entidades da União e a CERT-UE, quando atuam na qualidade de responsáveis pelo tratamento de dados, aplicam medidas técnicas para impedir o tratamento de categorias especiais de dados pessoais para outros fins e preveem medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses dos titulares dos dados.

Capítulo II
Medidas destinadas a garantir um elevado nível comum de cibersegurança

Artigo 5.º

Aplicação de medidas

1. Até … [oito meses a contar da data de entrada em vigor do presente regulamento], o Conselho Interinstitucional para a Cibersegurança, criado nos termos do artigo 10.º, emite, após consulta à Agência da União Europeia para a Cibersegurança (ENISA) e após receber orientações da CERT-UE, orientações destinadas às entidades da União para efeitos de uma análise inicial da cibersegurança e para criar um regime interno de gestão, governação e controlo dos riscos de cibersegurança nos termos do artigo 6.º, para realizar avaliações da maturidade em matéria de cibersegurança nos termos do artigo 7.º, tomar medidas de gestão dos riscos de cibersegurança nos termos do artigo 8.º e adotar o plano de cibersegurança nos termos do artigo 9.º.

2. Ao aplicar os artigos 6.º a 9.º, as entidades da União têm em conta as orientações a que se refere o n.º 1 do presente artigo, bem como as orientações e recomendações pertinentes adotadas nos termos dos artigos 11.º e 14.º.

Artigo 6.º

Regime de gestão, governação e controlo dos riscos de cibersegurança

1. Até … [15 meses a contar da data de entrada em vigor do presente regulamento], cada entidade da União estabelece, após efetuar uma análise inicial da cibersegurança, designadamente uma auditoria, um regime interno de gestão, governação e controlo dos riscos de cibersegurança («regime»). O estabelecimento do regime é supervisionado pela direção ao mais alto nível da entidade da União e é da sua responsabilidade.

2. O regime abrange a totalidade do ambiente das TIC não classificado da entidade da União em causa, incluindo todos os ambientes das TIC nas instalações, a rede de tecnologia operacional locais, os ativos e serviços subcontratados 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 aos referidos ambientes («ambiente das TIC»). O regime baseia-se numa abordagem que tem em conta todos os perigos.

3. O regime garante um elevado nível de cibersegurança. Estabelece políticas internas de cibersegurança, incluindo objetivos e prioridades, para a segurança dos sistemas de rede e informação, bem como as funções e responsabilidades do pessoal da entidade da União encarregado de assegurar a aplicação efetiva do presente regulamento. O regime inclui também mecanismos para medir a eficácia da aplicação.

4. O regime é reexaminado periodicamente, na perspetiva da evolução dos riscos de cibersegurança, e, pelo menos, de quatro em quatro anos. Se for caso disso e na sequência de um pedido do Conselho Interinstitucional para a Cibersegurança, criado nos termos do artigo 10.º, o regime de uma entidade da União pode ser atualizado com base nas orientações da CERT-UE sobre incidentes identificados ou eventuais lacunas observadas na aplicação do presente regulamento.

5. Incumbe à direção ao mais alto nível de cada entidade da União a responsabilidade pela aplicação do presente regulamento, assim como a supervisão do cumprimento, por parte da respetiva organização, das obrigações relacionadas com o regime.

6. Se for caso disso e sem prejuízo da sua responsabilidade pela aplicação do presente regulamento, a direção ao mais alto nível de cada entidade da União pode delegar obrigações específicas ao abrigo do presente regulamento em altos funcionários, na aceção do artigo 29.º, n.º 2, do Estatuto dos Funcionários, ou noutros funcionários de nível equivalente, dentro da entidade da União em causa. Independentemente dessa delegação, a direção ao mais alto nível pode ser considerada responsável por infrações ao presente regulamento cometidas pela entidade da União em causa.

7. Cada entidade da União deve dispor de mecanismos eficazes para assegurar que uma percentagem adequada do orçamento para as TIC seja aplicada em cibersegurança. O regime é devidamente tido em conta na definição da referida percentagem.

8. Cada entidade da União designa um responsável local pela cibersegurança, ou função equivalente, que atue como ponto de contacto único relativamente a todos os aspetos de cibersegurança. O responsável local pela cibersegurança facilita a aplicação do presente regulamento e reporta diretamente à direção ao mais alto nível, numa base periódica, o ponto da situação no que se refere à aplicação. Sem prejuízo do facto de o responsável local pela cibersegurança ser o ponto de contacto único em cada entidade da União, uma entidade da União pode delegar na CERT-UE determinadas atribuições do responsável local pela cibersegurança no que diz respeito à aplicação do presente regulamento, com base num acordo de nível de serviço celebrado entre essa entidade da União e a CERT-UE, ou essas atribuições podem ser partilhadas por várias entidades da União. Caso essas atribuições sejam delegadas na CERT-UE, o Comité Interinstitucional para a Cibersegurança, criado nos termos do artigo 10.º, decide se a prestação desse serviço deve fazer parte dos serviços de base da CERT-UE, tendo em conta os recursos humanos e financeiros da entidade da União em causa. Cada entidade da União informa a CERT-UE, sem demora injustificada, do responsável local pela cibersegurança designado e de eventuais alterações subsequentes a este respeito.

A CERT-UE cria a lista de responsáveis locais pela cibersegurança designados e garante a respetiva atualização.

9. Os altos funcionários na aceção do artigo 29.º, n.º 2, do Estatuto dos Funcionários ou outros funcionários de nível equivalente de cada entidade da União, bem como todos os membros do pessoal pertinentes incumbidos da aplicação das medidas de gestão dos riscos de cibersegurança e do cumprimento das obrigações previstas no presente regulamento, frequentam periodicamente 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 entidade da União.

Artigo 7.º

Avaliação da maturidade em matéria de cibersegurança

1. Até … [18 meses a contar da data de entrada em vigor do presente regulamento] e, posteriormente, pelo menos de dois em dois anos, cada entidade da União realiza uma avaliação da maturidade em matéria de cibersegurança que inclua todos os elementos do seu ambiente das TIC.

2. As avaliações da maturidade em matéria de cibersegurança são, se for caso disso, realizadas com a assistência de um terceiro especializado.

3. As entidades da União com estruturas semelhantes podem cooperar na realização de avaliações da maturidade em matéria de cibersegurança para as respetivas entidades.

4. Com base num pedido do pedido do Conselho Interinstitucional para a Cibersegurança, criado nos termos do artigo 10.º, e com o consentimento explícito da entidade da União em causa, os resultados de uma avaliação da maturidade em matéria de cibersegurança podem ser debatidos no âmbito do Conselho ou no âmbito da rede de responsáveis locais pela cibersegurança, tendo em vista tirar ilações da aplicação e partilhar boas práticas de excelência.

Artigo 8.º

Medidas de gestão dos riscos de cibersegurança

1. Sem demora injustificada e, em qualquer caso, até … [20 meses a contar da data de entrada em vigor do presente regulamento], cada entidade da União toma, sob a supervisão da direção ao mais alto nível respetiva, medidas técnicas, operacionais e organizativas adequadas e proporcionadas para gerir os riscos de cibersegurança identificados no âmbito do regime e prevenir ou minimizar o impacto dos incidentes. Tendo em conta os progressos técnicos mais recentes e, se aplicável, as normas europeias e internacionais pertinentes, essas medidas garantem um nível de segurança dos sistemas de rede e informação em todo o ambiente de TIC proporcional aos riscos de cibersegurança criados. Aquando da avaliação da proporcionalidade dessas medidas, são devidamente tidos em conta o grau de exposição da entidade da União aos riscos de cibersegurança, a sua dimensão, a probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto nos planos societal, económico e interinstitucional.

2. As entidades da União abordam, pelo menos, os seguintes domínios na aplicação das medidas de gestão dos riscos de cibersegurança:

a) Política de cibersegurança, nomeadamente as medidas necessárias para alcançar os objetivos e prioridades referidos no artigo 6.º e no n.º 3 do presente artigo;

b) Políticas relativas à análise dos riscos de cibersegurança e de segurança dos sistemas de informação;

c) Objetivos políticos relativos à utilização de serviços de computação em nuvem;

d) Auditorias de cibersegurança, se for caso disso, que podem incluir uma avaliação do risco de cibersegurança, da vulnerabilidade e das ciberameaças, bem como testes de penetração realizados regularmente por um prestador privado de confiança;

e) Aplicação das recomendações resultantes das auditorias de cibersegurança a que se refere a alínea d), através da cibersegurança e de atualizações das políticas;

f) Organização da cibersegurança, incluindo a definição das funções e responsabilidades;

g) Gestão de ativos, incluindo o inventário dos ativos de TIC e o mapeamento da rede de TIC;

h) Segurança dos recursos humanos e controlo do acesso;

i) Segurança das operações;

j) Segurança das comunicações;

k) Aquisição, desenvolvimento e manutenção dos sistemas, incluindo políticas relativas ao tratamento e à divulgação de vulnerabilidades;

l) Se exequível, políticas relativas à transparência do código-fonte;

m) Segurança da cadeia de abastecimento, incluindo aspetos relacionados com a segurança no que se refere às relações entre cada entidade da União e os seus fornecedores diretos ou prestadores de serviços;

n) Tratamento de incidentes e cooperação com a CERT-UE, designadamente no âmbito da conservação de registos e da monitorização da segurança;

o) Gestão da continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises; e

p) Promoção e desenvolvimento de programas de educação, competências, sensibilização, exercício e formação no domínio da cibersegurança.

Para efeitos do primeiro parágrafo, alínea m), as entidades da União têm em conta as vulnerabilidades específicas de cada fornecedor direto e de cada prestador de serviços, bem como a qualidade global dos produtos e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os seus procedimentos de desenvolvimento seguro.

3. As entidades da União tomam, pelo menos, as seguintes medidas específicas de gestão dos riscos de cibersegurança:

a) Disposições técnicas para permitir e manter o teletrabalho;

b) Medidas concretas para avançar rumo a princípios de «confiança zero»;

c) Utilização, por norma, da autenticação multifatorial nos sistemas de rede e informação;

d) Utilização da criptografia e da cifragem, em particular da cifragem de ponta a ponta, bem como de assinaturas digitais seguras;

e) Implantação, se for caso disso, de comunicações seguras de voz, vídeo e texto e de sistemas seguros de comunicações de emergência na entidade da União;

f) Medidas proativas para a deteção e remoção de software malicioso e de software espião;

g) Garantia da segurança da cadeia de abastecimento de software por meio de critérios para a criação e avaliação seguras de software;

h) Estabelecimento e adoção de programas de formação sobre cibersegurança adequados às atribuições prescritas e às capacidades previstas para a direção ao mais alto nível e para os membros do pessoal da entidade da União incumbidos de garantir a aplicação do presente regulamento;

i) Formação periódica do pessoal em matéria de cibersegurança;

j) Se for caso disso, participação em análises dos riscos de interconectividade entre as entidades da União;

k) Reforço das regras de contratação pública para facilitar um elevado nível comum de cibersegurança através:

   i) remoção dos obstáculos contratuais que limitam a partilha de informações com a CERT-UE por parte dos prestadores de serviços TIC sobre os incidentes, as vulnerabilidades e as ciberameaças,

   ii) obrigações contratuais de comunicar os incidentes, as vulnerabilidades e as ciberameaças, bem como de dispor de um sistema adequado de monitorização e resposta a incidentes.

Artigo 9.º

Planos de cibersegurança

1. Na sequência da conclusão da avaliação da maturidade em matéria de cibersegurança efetuada nos termos do artigo 7.º, e tendo em conta os ativos e riscos de cibersegurança identificados no regime, assim como as medidas de gestão dos riscos de cibersegurança adotadas nos termos do artigo 8.º, a direção ao mais alto nível de cada entidade da União aprova um plano de cibersegurança, sem demora injustificada, e em todo o caso até … [24 meses a contar da data de entrada em vigor do presente regulamento]. O plano de cibersegurança visa reforçar a cibersegurança global da entidade da União e, por conseguinte, contribuir para o reforço de um elevado nível comum de cibersegurança nas entidades da União. O plano de cibersegurança inclui pelo menos as medidas de gestão dos riscos de cibersegurança adotadas nos termos do artigo 8.º. O plano de cibersegurança é revisto de dois em dois anos, ou mais frequentemente se necessário, na sequência de avaliações da maturidade em matéria de cibersegurança realizadas nos termos do artigo 7.º ou de um reexame importante do regime.

2. O plano de cibersegurança inclui o plano de gestão de cibercrises da entidade da União para incidentes graves.

3. As entidades da União apresentam os seus planos de cibersegurança ao Conselho Interinstitucional para a Cibersegurança criado nos termos do artigo 10.º.

Capítulo III
Conselho interinstitucional para a cibersegurança

Artigo 10.º

Conselho Interinstitucional para a Cibersegurança

1. É criado o Conselho Interinstitucional para a Cibersegurança (IICB, na sigla inglesa).

2. Cabe ao IICB:

   a) Acompanhar e apoiar a aplicação do presente regulamento por parte das entidades da União;

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

3. O IICB é composto por:

   a) Um representante designado por cada uma das seguintes entidades:

      i) o Parlamento Europeu,

      ii) o Conselho Europeu,

iii) o Conselho da União Europeia,

iv) a Comissão,

v) o Tribunal de Justiça da União Europeia,

vi) o Banco Central Europeu,

vii) o Tribunal de Contas,

viii) o Serviço Europeu para a Ação Externa,

ix) o Comité Económico e Social Europeu,

x) o Comité das Regiões Europeu,

xi) o Banco Europeu de Investimento,

xii) o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança,

xiii) a ENISA,

xiv) a Autoridade Europeia para a Proteção de Dados (AEPD),

xv) a Agência da União Europeia para o Programa Espacial.

b) Três representantes designados pela Rede de Agências da UE, com base numa proposta do seu Comité Consultivo para as TIC, para representar os interesses dos órgãos e organismos da União que administram os seus próprios ambientes das TIC, para além dos referidos na alínea a).

As entidades da União representadas no IICB procuram alcançar o equilíbrio de género entre os representantes designados.

4. Os membros do IICB podem ser assistidos por um suplente. O presidente pode convidar outros representantes das entidades da União referidas no n.º 3 ou de outras entidades da União para participarem nas reuniões do IICB, sem direito de voto.

5. O diretor da CERT-UE e os presidentes do grupo de cooperação, da rede de CSIRT e da UE-CyCLONe, criados, respetivamente, nos termos dos artigos 14.º, 15.º e 16.º da Diretiva (UE) 2022/2555, ou os respetivos suplentes, podem participar nas reuniões do IICB na qualidade de observadores. Em casos excecionais, o IICB pode, nos termos do seu regulamento interno, decidir em contrário.

6. Cabe ao IICB aprovar o seu regulamento interno.

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

8. O IICB reúne-se pelo menos três vezes por ano por iniciativa do seu presidente, a pedido da CERT-UE ou a pedido de um dos seus membros.

9. 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 do IICB não participa na votação, exceto em caso de empate, caso em que poderá exercer um voto de qualidade.

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

11. O secretariado do IICB é assegurado pela Comissão e responde perante o presidente do IICB.

12. Os representantes designados pela Rede de Agências da UE transmitem as decisões do IICB aos membros da Rede de Agências da UE. Qualquer membro da Rede de Agências da UE tem o direito de suscitar junto dos referidos representantes ou do presidente do IICB qualquer questão que considerem que deverá ser dada a conhecer ao IICB.

13. O IICB cria um comité executivo para o assistir nos seus trabalhos e delegar algumas das suas atribuições e competências. Cabe ao IICB criar o regulamento interno do comité executivo, incluindo as respetivas atribuições e competências e a duração do mandato dos seus membros.

14. Até … [12 meses a contar da data de entrada em vigor do presente regulamento] e, posteriormente, numa base anual, o IICB apresenta ao Conselho um relatório que descreve pormenorizadamente os progressos realizados na aplicação do presente regulamento e que especifica, em especial, a amplitude da cooperação da CERT-UE com as suas contrapartes em cada Estado-Membro. O referido relatório constitui um contributo para o relatório bienal sobre o estado da cibersegurança na União, elaborado nos termos do artigo 18.º da Diretiva (UE) 2022/2555.

Artigo 11.º

Atribuições do IICB

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

a) Dar orientações ao diretor da CERT-UE;

b) Acompanhar e supervisionar eficazmente a aplicação do presente regulamento e apoiar as entidades da União no reforço da sua cibersegurança, incluindo, se for caso disso, solicitando relatórios *ad hoc* às entidades da União e à CERT-UE;

c) Adotar, na sequência de um debate estratégico, uma estratégia plurianual sobre o aumento do nível de cibersegurança nas entidades da União, avaliá-la periodicamente e, pelo menos, de cinco em cinco anos, e, se necessário, alterá-la;

d) Estabelecer a metodologia e os aspetos organizacionais para a realização de avaliações voluntárias pelos pares por entidades da União, com vista a retirar ensinamentos de experiências partilhadas, reforçar a confiança mútua, alcançar um elevado nível comum de cibersegurança, bem como reforçar as capacidades de cibersegurança das entidades da União, assegurando que essas avaliações pelos pares sejam realizadas por peritos em cibersegurança designados por uma entidade da União diferente da entidade da União objeto de análise e que a metodologia se baseie no artigo 19.º da Diretiva (UE) 2022/2555 e seja, se for caso disso, adaptada às entidades da União;

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

f) Aprovar, com base numa proposta do diretor da CERT-UE, o catálogo de serviços da CERT-UE e eventuais atualizações do mesmo;

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

h) Aprovar, com base numa proposta do diretor da CERT-UE, os termos dos acordos de nível de serviço;

i) Examinar e aprovar o relatório anual elaborado pelo chefe da CERT-UE referente às atividades e à gestão dos fundos da CERT-UE;

j) Aprovar e acompanhar os indicadores-chave de desempenho da CERT-UE, definidos com base numa proposta do seu diretor;

k) Aprovar acordos de cooperação, acordos de nível de serviço ou contratos entre a CERT-UE e outras entidades nos termos do artigo 18.º;

l) Adotar orientações e recomendações com base numa proposta da CERT-UE nos termos do artigo 14.º, e dar instruções à CERT-UE no sentido de que emita, retire ou modifique uma proposta de orientação ou de recomendação, ou um apelo à ação;

m) Criar grupos consultivos técnicos com atribuições concretas para assistir nos trabalhos do IICB, aprovar os respetivos estatutos e designar os respetivos presidentes;

n) Receber e avaliar documentos e relatórios apresentados pelas entidades da União nos termos do presente regulamento, como por exemplo avaliações da maturidade em matéria de cibersegurança;

o) Facilitar o estabelecimento de um grupo informal que reúna os responsáveis locais pela cibersegurança das entidades da União, apoiadas pela ENISA, visando o intercâmbio de práticas de excelência e de informações em relação à aplicação do presente regulamento;

p) Tendo em conta as informações sobre os riscos de cibersegurança identificados e os ensinamentos apresentados pela CERT-UE, acompanhar a adequação dos acordos de interconectividade entre os ambientes das TIC das entidades da União e prestar aconselhamento sobre possíveis melhorias;

q) Estabelecer um plano de gestão de cibercrises com vista a apoiar, a nível operacional, a gestão coordenada de incidentes graves que afetem entidades da União e a contribuir para o intercâmbio regular de informações pertinentes, em especial no que diz respeito aos impactos, à gravidade e às possíveis formas de atenuar os efeitos dos incidentes graves;

r) Coordenar a adoção dos planos de gestão de cibercrises das entidades individuais da União referidos no artigo 9.º, n.º 2;

s) Adotar recomendações relacionadas com a segurança da cadeia de abastecimento a que se refere o artigo 8.º, n.º 2, primeiro parágrafo, alínea m), tendo em conta os resultados das avaliações coordenadas a nível da UE dos riscos de segurança das cadeias de abastecimento críticas referidas no artigo 22.º da Diretiva (UE) 2022/2555, para ajudar as entidades da União a adotar medidas de gestão dos riscos de cibersegurança eficazes e proporcionadas.

Artigo 12.º

Conformidade

1. Cabe ao IICB, nos termos do artigo 10.º, n.º 2 e do artigo 11.º, acompanhar de forma eficaz a aplicação, por parte das entidades da União, do presente regulamento e das orientações, recomendações e apelos à ação adotados. O IICB pode solicitar às entidades da União as informações ou a documentação necessárias para o efeito. Para efeitos de adoção das medidas de conformidade nos termos do presente artigo, caso a entidade da União em causa esteja diretamente representada no IICB, não tem direito de voto.

2. Se concluir que uma entidade da União não aplicou efetivamente o presente regulamento ou alguma das orientações, recomendações ou apelos à ação emitidos nos termos do presente regulamento, o IICB pode, sem prejuízo dos procedimentos internos da entidade da União em causa, e após ter dado a oportunidade à entidade ou pessoa em causa de apresentar o seu ponto de vista:

   a) Transmitir um parecer fundamentado à entidade da União em causa, com as lacunas observadas na aplicação do presente regulamento;

   b) Dar, após consulta à CERT-UE, orientações à entidade da União em causa, por forma a colocar o respetivo regime, as medidas de gestão dos riscos de cibersegurança, os planos de cibersegurança e as obrigações de informação em conformidade com o presente regulamento num determinado prazo;

c) Emitir um alerta para abordar as lacunas identificadas num prazo especificado, incluindo recomendações para alterar medidas adotadas pela entidade da União em causa nos termos do presente regulamento;

d) Emitir uma notificação fundamentada para a entidade da União em causa, caso as deficiências identificadas num alerta emitido nos termos da alínea c) não tenham sido satisfatoriamente corrigidas no prazo especificado;

e) Emitir:

i) uma recomendação de realização de uma auditoria, ou

ii) um pedido de realização de uma auditoria por um terceiro prestador de serviços de auditoria;

f) Informar, se for caso disso, o Tribunal de Contas, no âmbito do seu mandato, do alegado incumprimento;

g) Emitir uma recomendação para que todos os Estados-Membros e todas as entidades da União apliquem uma suspensão temporária dos fluxos de dados para a entidade da União em causa.

Para efeitos do primeiro parágrafo, alínea c), o público-alvo de um alerta deve ser restringido adequadamente, se necessário tendo em conta o risco de cibersegurança.

Os alertas e recomendações emitidos ao abrigo do primeiro parágrafo são dirigidos à direção ao mais alto nível da entidade da União em causa.

3. Se o IICB tiver adotado medidas nos termos do n.º 2, primeiro parágrafo, alíneas a) a g), a entidade da União em causa apresenta ao pormenor as medidas e ações aplicadas para colmatar as alegadas lacunas identificadas pelo IICB. A entidade da União apresenta os referidos pormenores dentro de um prazo razoável a negociar com o IICB.

4. Se o IICB considerar que existe infração persistente ao presente regulamento por parte de uma entidade da União, diretamente resultante de ações ou omissões de um funcionário ou outro agente da União, incluindo da direção ao mais alto nível, o IICB exige à entidade da União em causa que tome as medidas necessárias, nomeadamente solicitando que pondere a tomada de medidas de caráter disciplinar, em conformidade com as regras e os procedimentos previstos no Estatuto dos Funcionários e em quaisquer outras regras ou quaisquer outros procedimentos aplicáveis. Para o efeito, o IICB transmite as informações necessárias à entidade da União em causa.

5. Caso as entidades da União informem da sua incapacidade para cumprir os prazos previstos no artigo 6.º, n.º 1, e no artigo 8.º, n.º 1, o IICB pode, em casos devidamente motivados, tendo em conta a dimensão da entidade da União, autorizar a prorrogação dos referidos prazos.

Capítulo IV
CERT-UE

Artigo 13.º

Missão e atribuições da CERT-UE

1. A missão da CERT-UE é contribuir para a segurança do ambiente das TIC não classificado das entidades da União, aconselhando-as em matéria de cibersegurança, ajudando-as a prevenir, detetar, gerir, atenuar e dar resposta a incidentes, assim como a recuperar após os mesmos, e agindo como plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes.

2. A CERT-UE recolhe, gere, analisa e partilha com as entidades da União as informações sobre as ciberameaças, as vulnerabilidades e os incidentes relativos à infraestrutura de TIC não classificada. Coordena as respostas a incidentes ocorridos a nível interinstitucional e da entidade da União, nomeadamente prestando ou coordenando a prestação de assistência operacional especializada.

3. A CERT-UE desempenha as seguintes atribuições em relação às entidades da União:

   a) Apoio na aplicação do presente regulamento e contributo para a coordenação dessa aplicação, por meio das medidas enumeradas no artigo 14.º, n.º 1, ou através de relatórios ad hoc solicitados pelo IICB;

b) Disponibilização de serviços normalizados da CSIRT a todas as entidades da União através de um pacote de serviços de cibersegurança descritos no seu catálogo de serviços (serviços de base);

c) Manutenção de uma rede de pares e parceiros para apoiar os serviços, conforme previsto nos artigos 17.º e 18.º;

d) Informação ao IICB relativamente a qualquer questão relacionada com a aplicação do presente regulamento e das orientações, recomendações e apelos à ação;

e) Com base nas informações referidas no n.º 2, contribuir para o conhecimento da situação cibernética na União, em estreita cooperação com a ENISA;

f) Coordenar a gestão de incidentes graves;

g) Exercer, em nome das entidades da União, uma função equivalente à do coordenador designado para fins de divulgação coordenada das vulnerabilidades, nos termos do artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555;

h) Disponibilizar, a pedido de uma entidade da União, uma análise proativa e não intrusiva dos sistemas de rede e informação acessíveis ao público dessa entidade da União.

As informações a que se refere o primeiro parágrafo, alínea e), são partilhadas com o IICB, a rede de CSIRT e o Centro de Situação e de Informações da União Europeia (INTCEN da UE), se aplicável e for caso disso, e sob reserva de condições de confidencialidade adequadas.

4. A CERT-UE pode, em conformidade com o artigo 17.º ou o artigo 18.º, conforme adequado, cooperar com as comunidades de cibersegurança pertinentes na União e nos seus Estados-Membros, 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 entidades da União;

b) Cooperação operacional no que respeita à rede CSIRT, nomeadamente em matéria de assistência mútua;

c) Informações sobre ciberameaças, incluindo o conhecimento situacional;

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

5. A CERT-UE enceta, no âmbito das suas competências, uma cooperação estruturada com a ENISA no que respeita ao reforço das capacidades, à cooperação operacional e a análises estratégicas a longo prazo das ciberameaças, em conformidade com o Regulamento (UE) 2019/881. A CERT-UE pode cooperar e trocar informações com o Centro Europeu da Cibercriminalidade da Europol.

6. A 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 de TIC das entidades da União, distintos dos referidos no n.º 3, com base em acordos de nível de serviço e sob reserva dos recursos disponíveis, nomeadamente monitorização de largo espectro da rede, inclusive a monitorização de primeira linha, a qualquer hora, das ciberameaças de maior gravidade;

b) Serviços de apoio a operações ou projetos de cibersegurança das entidades da União, distintos dos serviços destinados a proteger o respetivo ambiente das TIC, com base em acordos escritos e mediante aprovação prévia do IICB;

c) Uma análise proativa dos sistemas de rede e informação da entidade da União em causa, mediante pedido, a fim de detetar vulnerabilidades com um impacto significativo potencial;

d) Serviços de apoio à cibersegurança do ambiente das TIC de organizações distintas das entidades da União mas que colaborem estreitamente com as mesmas, por exemplo, por terem atribuições ou responsabilidades conferidas ao abrigo do direito da União, com base em acordos escritos e mediante aprovação prévia do IICB.

No respeitante ao primeiro parágrafo, alínea d), a CERT-UE pode, a título excecional, celebrar acordos de nível de serviço com entidades que não sejam as entidades da União, com a aprovação prévia do IICB.

7. A CERT-UE organiza e pode participar em exercícios de cibersegurança ou recomendar a participação em exercícios existentes, se aplicável em estreita cooperação com a ENISA, de forma a testar o nível de cibersegurança das entidades da União.

8. A CERT-UE pode prestar assistência às entidades da União relativamente a incidentes em sistemas de rede e informação que tratam ICUE, se as entidades da União envolvidas o solicitarem explicitamente, em conformidade com os respetivos procedimentos. A prestação de assistência pela CERT-UE nos termos do presente número é efetuada sem prejuízo das regras aplicáveis relacionadas com a proteção de informações classificadas.

9. A CERT-UE informa as entidades da União dos seus procedimentos e processos de tratamento de incidentes.

10. A CERT-UE contribui, com um elevado nível de confidencialidade e fiabilidade, através dos mecanismos de cooperação e canais de comunicação adequados, com informações pertinentes e anonimizadas sobre incidentes graves e a forma como foram tratados. As referidas informações são integradas no relatório a que se refere o artigo 10.º, n.º 14.

11. A CERT-UE apoia, em cooperação com a AEPD, as entidades da União em causa aquando da gestão de incidentes que tenham originado violações de dados pessoais, sem prejuízo das competências e atribuições da AEPD enquanto autoridade de supervisão nos termos do Regulamento (UE) 2018/1725.

12. Se os departamentos temáticos das entidades da União o solicitarem expressamente, a CERT-UE pode prestar aconselhamento técnico ou informações técnicas sobre questões estratégicas pertinentes.

Artigo 14.º

Orientações, recomendações e apelos à ação

1. A CERT-UE apoia a aplicação do presente regulamento através de:

a) Apelos à ação, descrevendo medidas urgentes de segurança que as entidades da União são instadas a tomar num determinado prazo;

b) Propostas ao IICB com vista à adoção de orientações dirigidas a todas ou a um conjunto de entidades da União;

c) Propostas ao IICB com vista à adoção de recomendações dirigidas a entidades individuais da União.

No que diz respeito ao primeiro parágrafo, alínea a), a entidade da União em causa informa a CERT-UE, sem demora injustificada após receber o convite à ação, da forma como as medidas de segurança urgentes foram aplicadas.

2. As orientações e recomendações podem incluir:

a) Metodologias comuns e um modelo de avaliação da maturidade em matéria de cibersegurança das entidades da União, incluindo as escalas ou os indicadores-chave de desempenho correspondentes, que sirva de referência para apoiar uma melhoria contínua da cibersegurança em todas as entidades da União e facilitar a atribuição de prioridades dos domínios e medidas de cibersegurança, tendo em conta a postura das entidades em matéria de cibersegurança;

b) Disposições práticas ou melhorias relativas à gestão dos riscos de cibersegurança e das medidas de gestão dos riscos de cibersegurança;

c) Disposições práticas relativas às avaliações da maturidade em matéria de cibersegurança e aos planos de cibersegurança;

d) Se for caso disso, a utilização em comum de uma tecnologia, arquitetura, fonte aberta e das boas práticas conexas no intuito de concretizar a interoperabilidade e normas comuns, incluindo uma abordagem coordenada no que diz respeito à segurança da cadeia de abastecimento;

e) Se for caso disso, informações destinadas a facilitar a utilização de instrumentos de contratação pública colaborativa para a aquisição de serviços e produtos de cibersegurança relevantes a fornecedores terceiros;

f) Acordos de partilha de informações nos termos do artigo 20.º.

Artigo 15.º

Diretor da CERT-UE

1. A Comissão, tendo obtido a aprovação por maioria de dois terços dos membros do IICB, nomeia o diretor da CERT-UE. O IICB é consultado em todas as fases do processo de nomeação do diretor da CERT-UE, em especial no que respeita à elaboração dos anúncios de abertura de vaga, à análise das candidaturas e à nomeação de júris de seleção para o cargo. O processo de seleção, incluindo a lista restrita final de candidatos para a nomeação do diretor da CERT-UE, assegura uma representação equitativa de cada género, tendo em conta as candidaturas apresentadas.

2. O diretor da CERT-UE é responsável pelo bom funcionamento da CERT-UE, atuando no âmbito das suas competências e sob a direção do IICB. O diretor da CERT-UE presta periodicamente informações ao presidente do IICB e apresenta relatórios **ad hoc** ao IICB, a pedido do referido presidente.

3. O diretor da CERT-UE presta assistência ao gestor orçamental delegado competente na elaboração do relatório anual de atividades que contém informações financeiras e de gestão, incluindo os resultados dos controlos, e é elaborado nos termos do artigo 74.º, n.º 9, do Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho[1], e informa-o regularmente sobre a aplicação das medidas para as quais tenham sido subdelegadas competências no diretor da CERT-UE.

4. O diretor da CERT-UE elabora anualmente um planeamento financeiro das receitas e despesas administrativas relacionadas com as suas atividades, uma proposta de programa de trabalho anual, uma proposta de catálogo de serviços da CERT-UE e as respetivas revisões, uma proposta dos termos dos acordos de nível de serviço e uma proposta de indicadores-chave de desempenho para a CERT-UE, com vista à sua aprovação pelo IICB nos termos do artigo 11.º. No âmbito da revisão da lista de serviços incluídos no catálogo de serviços da CERT-UE, o diretor da CERT-UE tem em conta os recursos afetados à CERT-UE.

---

[1] 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).

5. O diretor da CERT-UE apresenta, pelo menos anualmente, relatórios ao IICB e ao presidente do IICB sobre as atividades e o desempenho da CERT-UE durante o período de referência, inclusive sobre a execução do orçamento, 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 11.º. Os referidos relatórios incluem um programa de trabalho para o período seguinte, o planeamento financeiro das receitas e despesas, incluindo o pessoal, as atualizações previstas do catálogo de serviços da CERT-UE e uma avaliação do impacto esperado dessas atualizações em termos de recursos financeiros e humanos.

Artigo 16.º

Questões financeiras e de pessoal

1. A CERT-UE é integrada na estrutura administrativa de uma direção-geral da Comissão, a fim de beneficiar das estruturas de apoio administrativo, financeiro e contabilístico da Comissão, mantendo simultaneamente o seu estatuto de prestador de serviços interinstitucional autónomo para todas as entidades da União. A Comissão informa o IICB sobre a localização da sede administrativa da CERT-UE, bem como de qualquer alteração desta. A Comissão reexamina periodicamente as disposições administrativas relacionadas com a CERT-UE e, em qualquer caso, antes da criação de qualquer quadro financeiro plurianual nos termos do artigo 312.º do TFUE, a fim de permitir a adoção de medidas adequadas. O reexame deve incluir a possibilidade de criar a CERT-UE como um serviço da União.

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

3. As atribuições e atividades da CERT-UE, incluindo os serviços que preste nos termos do artigo 13.º, n.ºs 3, 4, 5 e 7, e do artigo 14.º, n.º 1, às entidades da União financiados a partir da rubrica do quadro financeiro plurianual dedicada à administração pública europeia, são financiadas por uma rubrica orçamental distinta do orçamento da Comissão. Os postos afetados à CERT-UE são especificados numa nota de rodapé no quadro de pessoal da Comissão.

4. As entidades da União distintas das referidas no n.º 3 do presente artigo devem prestar uma contribuição financeira anual à CERT-UE para cobrir os serviços prestados pela CERT-UE nos termos desse mesmo número. As contribuições baseiam-se nas orientações dadas pelo IICB e acordadas entre cada entidade da União e a 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 do presente artigo como receitas afetadas internas, tal como previsto no artigo 21.º, n.º 3, alínea c), do Regulamento (UE, Euratom) 2018/1046.

5. Os custos dos serviços indicados no artigo 13.º, n.º 6, devem ser recuperados junto das entidades da União que beneficiem dos serviços da CERT-UE. As receitas são afetadas às rubricas orçamentais de apoio aos custos.

Artigo 17.º

Colaboração da CERT-UE com as contrapartes dos Estados-Membros

1. A CERT-UE deve, sem demora injustificada, colaborar e trocar informações com as contrapartes dos Estados-Membros, incluindo as CSIRT designadas ou estabelecidas nos termos do artigo 10.º da Diretiva (UE) 2022/2555, ou, se aplicável, as autoridades competentes e pontos de contacto únicos designados ou estabelecidos nos termos do artigo 8.º dessa diretiva, relativamente a incidentes, ciberameaças, vulnerabilidades, quase incidentes, a possíveis contramedidas, bem como a boas práticas e a todas as questões pertinentes para melhorar a proteção do ambiente das TIC das entidades da União, nomeadamente por meio da rede de CSIRT referida no artigo 15.º da Diretiva (UE) 2022/2555. A CERT-UE apoia a Comissão no âmbito da UE-CyCLONe estabelecida nos termos do artigo 16.º da Diretiva (UE) 2022/2555 no que diz respeito à gestão coordenada a incidentes e crises de cibersegurança em grande escala.

2. Caso tome conhecimento de um incidente significativo ocorrido no território de um Estado-Membro, a CERT-UE informa, sem demora, quaisquer contrapartes relevantes nesse Estado-Membro, em conformidade com o n.º 1.

3. Desde que os dados pessoais estejam protegidos em conformidade com a legislação aplicável da União em matéria de proteção de dados, a CERT-UE deve, sem demora injustificada, trocar informações específicas pertinentes sobre incidentes com as contrapartes dos Estados-Membros para facilitar a deteção de ciberameaças ou incidentes semelhantes, ou contribuam para a análise de um incidente, sem a autorização da entidade da União afetada. A CERT-UE só partilha informações específicas sobre incidentes que revelem a identidade do seu alvo num dos seguintes casos:

a) A entidade da União afetada der o seu consentimento;

b) A entidade da União afetada não der o consentimento previsto na alínea a) mas a divulgação da identidade da entidade da União afetada aumentar a probabilidade de evitar ou atenuar incidentes noutros locais.

c) A entidade da União afetada já tenha tornado público o facto de ter sido afetada.

As decisões relativas ao intercâmbio de informações específicas sobre um incidente que revelem a identidade do alvo do incidente nos termos do primeiro parágrafo, alínea b), são aprovadas pelo diretor da CERT-UE. Antes de emitir essa decisão, a CERT-UE contacta por escrito a entidade da União afetada, explicando claramente de que forma a divulgação da sua identidade contribuiria para evitar ou atenuar incidentes noutros locais. O diretor da CERT-UE apresenta a explicação e solicita explicitamente à entidade da União que declare se dá o seu consentimento dentro de um determinado prazo. O diretor da CERT-UE informa igualmente a entidade da União de que, à luz da explicação fornecida, se reserva o direito de divulgar as informações, mesmo na falta de consentimento. A entidade da União afetada é informada antes da divulgação das informações.

Artigo 18.º

Colaboração da CERT-UE com outras contrapartes

1. A CERT-UE pode colaborar com contrapartes da União distintas das mencionadas no artigo 17.º que estejam sujeitas aos requisitos da União em matéria de cibersegurança, nomeadamente contrapartes setoriais, em matéria de ferramentas e métodos, como técnicas, táticas, procedimentos e boas práticas, bem como em matéria de ciberameaças e vulnerabilidades informáticas. No que respeita à colaboração com tais contrapartes, a CERT-UE deve obter a aprovação prévia do IICB numa base casuística. Caso estabeleça a cooperação com tais contrapartes, a CERT-UE informa todas as contrapartes pertinentes dos Estados-Membros referidas no artigo 17.º, n.º 1, no Estado-Membro onde a contraparte se encontre. Se aplicável e for caso disso, essa cooperação e as respetivas condições, nomeadamente em matéria de cibersegurança, proteção de dados e tratamento de informações, são estabelecidas em acordos de confidencialidade específicos, tais como contratos ou convénios administrativos. Os acordos de confidencialidade não carecem da aprovação prévia do IICB mas são levados ao conhecimento do seu presidente. Em caso de necessidade urgente e iminente de trocar informações em matéria de cibersegurança no interesse das entidades da União ou de outra parte, a CERT-UE pode fazê-lo com uma entidade cuja competência, capacidade e conhecimentos específicos sejam justificadamente necessários para prestar assistência em caso de uma tal necessidade urgente e iminente, mesmo que a CERT-UE não disponha de um acordo de confidencialidade com essa entidade. Nesses casos, a CERT-UE informa imediatamente o presidente do IICB e mantém o IICB informado através de relatórios periódicos ou reuniões.

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

3. Mediante consentimento da entidade da União afetada por um incidente e desde que exista um acordo ou contrato de não divulgação com a contraparte ou parceiro em causa, a CERT-UE pode transmitir informações relacionadas com o incidente específico às contrapartes ou parceiros a que se referem os n.ºs 1 e 2 unicamente com o objetivo de contribuir para a sua análise.

Capítulo V

Obrigações de cooperação e de comunicação de informações

Artigo 19.º

Tratamento de informações

1. As entidades da União e a CERT-UE devem respeitar as obrigações de sigilo profissional nos termos do artigo 339.º do TFUE ou dos regimes equivalentes aplicáveis.

2. O Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho[1] é aplicável no que respeita aos pedidos de acesso do público a documentos na posse da CERT-UE, tendo em conta a obrigação, prevista no referido regulamento, de consultar as outras entidades da União ou, se for caso disso, os Estados-Membros, sempre que um pedido diga respeito a documentos seus.

3. O tratamento das informações pelas entidades da União e pela CERT-UE deve cumprir as regras aplicáveis relativas à segurança da informação.

Artigo 20.º

Acordos de partilha de informações sobre cibersegurança

1. As entidades da União podem, a título voluntário, informar a CERT-UE e prestar-lhe informações sobre incidentes, ciberameaças, quase incidentes e vulnerabilidades que as afetem. A CERT-UE garante a disponibilidade de meios de comunicação eficientes, com um nível elevado de rastreabilidade, confidencialidade e fiabilidade, com o objetivo de facilitar a partilha de informações com as entidades da União. No tratamento de notificações, a CERT-UE pode dar prioridade ao tratamento das notificações obrigatórias em detrimento das notificações voluntárias. Sem prejuízo do artigo 12.º, a notificação voluntária não pode resultar na imposição à entidade da União notificadora de quaisquer obrigações adicionais às quais esta não estaria sujeita se não tivesse procedido à notificação.

---

[1] 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. Com vista a cumprir a sua missão e as atribuições conferidas nos termos do artigo 13.º, a CERT-UE pode solicitar que as entidades da União lhe transmitam informações dos respetivos inventários de sistemas das TIC, incluindo informações relacionadas com ciberameaças, quase incidentes, vulnerabilidades, indicadores de exposição a riscos, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança destinadas a detetar incidentes de cibersegurança. A entidade da União requerida deve transmitir sem demora injustificada as informações solicitadas, bem como eventuais atualizações subsequentes dessas informações.

3. A CERT-UE pode partilhar com as entidades da União informações específicas sobre incidentes que permitam identificar a entidade da União afetada por um determinado incidente, desde que a entidade da União afetada em tal consinta. Caso uma entidade da União recuse dar o seu consentimento, deve indicar à CERT-UE os motivos que fundamentam essa decisão.

4. As entidades da União, mediante pedido, partilham informações com o Parlamento Europeu e o Conselho sobre a conclusão dos planos de cibersegurança.

5. O IICB ou a CERT-UE, consoante o caso, partilham, mediante pedido, orientações, recomendações e apelos à ação com o Parlamento Europeu e o Conselho.

6. As obrigações de partilha impostas no presente artigo não abrangem:

   a) As ICUE;

b) As informações cuja distribuição posterior tenha sido excluída por meio de uma marcação visível, a menos que a sua partilha com a CERT-UE tenha sido explicitamente autorizada.

Artigo 21.º

Obrigações de comunicação de informações

1. Considera-se que um incidente é significativo se:

a) Tiver causado ou for suscetível de causar graves perturbações operacionais no que se refere ao funcionamento da entidade da União ou perdas financeiras para a entidade da União em causa;

b) Tiver afetado ou for suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis.

2. As entidades da União apresentam à CERT-UE:

a) Sem demora injustificada e, em qualquer caso, no prazo de 24 horas depois de terem tomado conhecimento do incidente significativo, um alerta rápido, que, se aplicável, indica se há suspeitas de que o incidente significativo foi causado por um ato ilícito ou malicioso ou se pode ter um impacto transfronteiriço ou transversal a várias entidades;

b) Sem demora injustificada e, em qualquer caso, no prazo de 72 horas depois de terem tomado conhecimento do incidente significativo, uma notificação de incidente, que, se aplicável, deve atualizar as informações a que se refere a alínea a) e disponibilizar uma avaliação inicial do incidente significativo, incluindo da sua gravidade e do seu impacto, bem como, se disponíveis, dos indicadores de exposição a riscos;

c) A pedido da CERT-UE, um relatório intercalar com atualizações de estado pertinentes;

d) O mais tardar um mês após a apresentação da notificação de incidente mencionada na alínea b), um relatório final que contenha os seguintes elementos:

   i) uma descrição pormenorizada do incidente, incluindo da sua gravidade e do seu impacto,

   ii) o tipo de ameaça ou provável causa primária suscetível de ter desencadeado o incidente,

   iii) medidas de atenuação aplicadas e em curso,

   iv) se aplicável, o impacto transfronteiriço ou transversal a várias entidades do incidente significativo;

e) Em caso de incidente em curso no momento da apresentação do relatório final referido na alínea d), um relatório intercalar nessa altura e um relatório final no prazo de um mês após terem tratado o incidente.

3. Sem demora injustificada e, em qualquer caso, no prazo de 24 horas depois de ter tomado conhecimento de um incidente significativo, uma entidade da União informa as contrapartes pertinentes dos Estados-Membros a que se refere o artigo 17.º, n.º 1, no Estado-Membro em que está localizada de que ocorreu um incidente significativo.

4. As entidades da União comunicam, nomeadamente, quaisquer informações que permitam à CERT-UE determinar qualquer impacto transversal às entidades, impacto no Estado-Membro de acolhimento ou impacto transfronteiriço após a ocorrência de um incidente significativo. Sem prejuízo do artigo 12.º, a mera notificação não sujeita a entidade da União notificadora a responsabilidades acrescidas.

5. Se aplicável, as entidades da União comunicam, sem demora injustificada, aos utilizadores dos sistemas de rede e informação afetados, ou de outros componentes do ambiente das TIC, que serão potencialmente afetados por um incidente significativo ou por uma ciberameaça significativa, e, se for caso disso, que necessitam de tomar medidas de atenuação, e as medidas proativas ou corretivas que podem ser tomadas em resposta ao incidente ou à ameaça. Se for caso disso, as entidades da União devem informar esses utilizadores da própria ciberameaça significativa.

6. Se um incidente significativo ou uma ciberameaça significativa afetar um sistema de rede e informação ou um componente do ambiente das TIC de uma entidade da União que se saiba estar ligado ao ambiente das TIC de outra entidade da União, a CERT-UE emite um alerta de cibersegurança pertinente.

7. As entidades da União, a pedido da CERT-UE, facultam-lhe sem demora injustificada as informações digitais decorrentes da utilização dos dispositivos eletrónicos envolvidos nos incidentes em causa. A CERT-UE pode dar mais pormenores sobre os tipos de informação de que necessita para fins de conhecimento situacional e resposta a incidentes.

8. A CERT-UE apresenta, a cada três meses, ao IICB, à ENISA, ao INTCEN da UE e à rede de CSIRT, um relatório de síntese que inclua dados anonimizados e agregados sobre incidentes significativos, incidentes, ciberameaças, quase incidentes e vulnerabilidades nos termos do artigo 20.º e incidentes significativos notificados nos termos do n.º 2 do presente artigo. O referido relatório de síntese constitui um contributo para o relatório bienal sobre o estado da cibersegurança na União, elaborado nos termos do artigo 18.º da Diretiva (UE) 2022/2555.

9. Até … [seis meses a contar da data de entrada em vigor do presente regulamento], o IICB emite orientações ou recomendações no sentido de especificar melhor as modalidades, o formato e o conteúdo da comunicação de informações nos termos do presente artigo. Ao elaborar essas orientações ou recomendações, o IICB deve ter em conta quaisquer atos de execução adotados nos termos do artigo 23.º, n.º 11, da Diretiva (UE) 2022/2555 que especifiquem o tipo de informações, o formato e o procedimento das notificações. A 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 entidades da União.

10. As obrigações de comunicação de informações impostas no presente artigo não abrangem:

a) As ICUE;

b) As informações cuja distribuição posterior tenha sido excluída por meio de uma marcação visível, a menos que a sua partilha com a CERT-UE tenha sido explicitamente autorizada.

Artigo 22.º

Coordenação da resposta a incidentes e cooperação

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

a) Entidades da União;

b) As contrapartes referidas nos artigos 17.º e 18.º.

2. A CERT-UE facilita, se for caso disso em estreita cooperação com a ENISA, a coordenação entre as entidades da União na resposta a incidentes, incluindo os seguintes elementos:

a) Contribuição para uma comunicação externa coerente;

b) Apoio mútuo, como a partilha de informações relevantes para as entidades da União ou a prestação de assistência, se for caso disso diretamente no local;

c) Utilização ideal dos recursos operacionais;

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

3. A CERT-UE apoia, em estreita cooperação com a ENISA, as entidades da União no que respeita ao conhecimento situacional de incidentes, ciberameaças, vulnerabilidades e quase incidentes, bem como no que respeita à partilha dos mais recentes avanços no domínio da cibersegurança.

4. Até … [12 meses a contar da data de entrada em vigor do presente regulamento], o IICB adota, com base numa proposta da CERT-UE, orientações ou recomendações sobre a coordenação da resposta a incidentes e a colaboração em caso de incidente significativo. Quando se suspeitar que um incidente teve natureza criminosa, a CERT-UE deve emitir, sem demora injustificada, orientações sobre a forma como o incidente deve ser notificado às autoridades competentes para a aplicação da lei.

5. Na sequência de um pedido específico de um Estado-Membro e com a aprovação das entidades da União em causa, a CERT-UE pode recorrer a peritos da lista referida no artigo 23.º, n.º 4, para contribuírem para a resposta a um incidente grave com impacto nesse Estado-Membro, ou a um incidente de cibersegurança em grande escala, em conformidade com o artigo 15.º, n.º 3, alínea g), da Diretiva (UE) 2022/2555. As regras específicas sobre o acesso e o recurso a peritos técnicos provenientes de entidades da União são aprovadas pelo IICB, mediante proposta da CERT-UE.

Artigo 23.º

Gestão de incidentes graves

1. A fim de apoiar, a nível operacional, a gestão coordenada de incidentes graves que afetem entidades da União e de contribuir para o intercâmbio regular de informações pertinentes entre as entidades da União e com os Estados-Membros, o IICB elabora, nos termos do artigo 11.º, alínea q), um plano de gestão de cibercrises com base nas atividades descritas no artigo 22.º, n.º 2, em estreita cooperação com a CERT-UE e a ENISA. O plano de gestão de cibercrises inclui, pelo menos, os seguintes elementos:

   a) Disposições relativas à coordenação e ao fluxo de informações entre as entidades da União para gestão de incidentes graves a nível operacional;

   b) Instruções permanentes normalizadas comuns;

   c) Uma taxonomia comum da gravidade de incidentes graves e pontos de desencadeamento de crises;

   d) Exercícios regulares;

   e) Canais de comunicação segura a utilizar.

2. Sujeito ao plano de gestão de cibercrises estabelecido nos termos do n.º 1 do presente artigo e sem prejuízo do artigo 16.º, n.º 2, primeiro parágrafo, da Diretiva (UE) 2022/2555, o representante da Comissão no IICB é o ponto de contacto para a partilha de informações pertinentes relativas a incidentes graves com a UE-CyCLONe.

3. A CERT-UE coordena a gestão dos incidentes graves entre as entidades da União. Deve manter um inventário dos conhecimentos técnicos especializados disponíveis necessários para a resposta aos incidentes quando incidentes graves ocorram e prestar assistência ao IICB na coordenação dos planos de gestão de cibercrises das entidades da União para incidentes graves referidos no artigo 9.º, n.º 2.

4. As entidades 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.

Capítulo VI
Disposições finais

Artigo 24.º

Reafetação orçamental inicial

A fim de assegurar o funcionamento adequado e estável da CERT-UE, a Comissão pode propor a reafetação de pessoal e de recursos financeiros no âmbito do orçamento da Comissão para utilização em operações da CERT-UE. A reafetação será efetiva com a aprovação do primeiro orçamento anual da União, após a entrada em vigor do presente regulamento.

Artigo 25.º

Reexame

1. Até … [12 meses a contar da data de entrada em vigor do presente regulamento] e, posteriormente, numa base anual, o IICB, com a assistência da CERT-UE, deve comunicar à Comissão informações sobre a aplicação do presente regulamento. O IICB pode formular recomendações dirigidas à Comissão para que esta reexamine o presente regulamento.

2. Até … [36 meses a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de dois em dois anos, a Comissão avalia a aplicação do presente regulamento e apresenta ao Parlamento Europeu e ao Conselho um relatório sobre essa matéria e sobre a experiência adquirida a nível estratégico e operacional.

O relatório a que se refere o primeiro parágrafo do presente número deve incluir o reexame a que se refere o artigo 16.º, n.º 1, relativa à possibilidade de a CERT-UE ser constituída um organismo da União.

3. Até … [cinco anos a contar da data de entrada em vigor do presente regulamento], a Comissão avalia o funcionamento do presente regulamento e apresenta um relatório ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. A Comissão avalia igualmente a conveniência de incluir no âmbito de aplicação do presente regulamento os sistemas de rede e informação que tratam ICUE, tendo em conta outros atos legislativos da União aplicáveis a esses sistemas. Se necessário, o relatório é acompanhado de uma proposta legislativa.

Artigo 26.º

Entrada em vigor

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

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

Feito em …, em

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