Conselho da
União Europeia

Bruxelas, 31 de outubro de 2022
(OR. en)

14128/22

Dossiê interinstitucional:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

NOTA PONTO "I/A"

de:	Secretariado-Geral do Conselho
para:	Comité de Representantes Permanentes (2.ª Parte)/Conselho
n.º doc. ant.:	10097/5/22 REV 5
n.° doc. Com.:	7474/22 + ADD 1
Assunto:	Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União – Orientação geral

INTRODUÇÃO

1. Em 22 de março de 2022, a Comissão adotou a proposta de regulamento que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União. A proposta faz parte das medidas previstas na Estratégia de Cibersegurança da UE para a Década Digital[1], que visa reforçar a resiliência coletiva da União contra as ciberameaças.

[1] 14133/20.

Nas suas conclusões de 22 de março de 2021 sobre a referida estratégia[2], o Conselho salientou que a cibersegurança "é vital para o funcionamento da administração pública e das instituições, tanto a nível nacional como da UE, bem como para a nossa sociedade e a economia no seu todo".

2. A proposta da Comissão, baseada no artigo 298.º do Tratado sobre o Funcionamento da União Europeia, visa melhorar o nível de cibersegurança nas instituições, órgãos e organismos da União através do estabelecimento de um quadro comum, tendo devidamente em conta a autonomia de cada entidade da União. Em especial, os objetivos da proposta são os seguintes:

   – Reforçar o mandato e o financiamento da CERT-UE (equipa interinstitucional autónoma de resposta a emergências informáticas para as entidades da União);

   – Criar uma estrutura interinstitucional (Conselho Interinstitucional para a Cibersegurança (IICB)) que reúna representantes de todas as entidades da União, a fim de assegurar a correta aplicação do regulamento;

   – Introduzir a obrigação de as entidades da União partilharem informações (não classificadas) sobre incidentes com a CERT-UE e de a notificarem de ameaças, vulnerabilidades e incidentes significativos; e

   – Promover a coordenação e a cooperação no âmbito da resposta a incidentes significativos.

3. O Parlamento Europeu designou Henna Virkkunen (PPE) relatora da Comissão ITRE, que é a comissão competente quanto à matéria de fundo. O projeto de relatório foi publicado em 7 de outubro de 2022.

4. A Autoridade Europeia para a Proteção de Dados emitiu parecer em 17 de maio de 2022[3].

---

[2] 6722/21.
[3] 9252/22.

5. No Conselho, a análise da proposta pelo Grupo Horizontal das Questões do Ciberespaço teve início durante a Presidência francesa, a 29 de março de 2022. A Presidência francesa elaborou o primeiro texto de compromisso, que foi debatido no Grupo Horizontal das Questões do Ciberespaço em junho de 2022, e apresentou um relatório intercalar[4] ao Conselho em 21 de junho de 2022.

6. Durante a Presidência checa, o Grupo Horizontal das Questões do Ciberespaço dedicou oito reuniões[5] a debates sobre a proposta e sobre vários textos de compromisso consecutivos.

7. Em 23 de maio de 2022, a Presidência solicitou um parecer ao Comité de Segurança do Conselho (CSC) sobre os aspetos da proposta relacionados com a segurança da informação, em especial as informações classificadas. O CSC emitiu o seu parecer em 19 de setembro de 2022[6]. Tal como sugerido pelo CSC, as informações classificadas da UE foram explicitamente excluídas do âmbito do regulamento. As disposições relativas à dispensa das obrigações de partilha e comunicação de informações no que se refere às informações que provenham de fora das entidades da União foram alteradas em conformidade.

8. Em 28 de outubro de 2022, o Grupo Horizontal das Questões do Ciberespaço chegou a acordo sobre o compromisso da Presidência que consta do anexo.

---

4 9719/22.

5 6 e 20 de julho, 13, 21 e 28 de setembro, 5, 19 e 28 de outubro de 2022.

6 12603/22 + COR 1.

PRINCIPAIS QUESTÕES

9. Os Estados-Membros congratularam-se com a proposta, considerando-a oportuna e complementar à futura diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (Diretiva SRI 2), e apoiaram os seus objetivos gerais. No entanto, os Estados-Membros apelaram a um maior alinhamento pela "SRI 2" e a mais reciprocidade no intercâmbio de informações entre as entidades da União e os Estados-Membros, tendo ainda salientado o caráter demasiado voluntário de algumas das medidas propostas. Os Estados-Membros também expressaram a sua preferência pela supressão das referências à Ciberunidade Conjunta, cujo mandato e composição estão ainda por definir.

10. Com base nos debates realizados a nível do Grupo Horizontal das Questões do Ciberespaço, foram identificados como principais questões políticas a tratar os seguintes pontos:

a) Alinhamento pela futura Diretiva SRI 2

Tal como solicitado pelos Estados-Membros, procedeu-se a novos alinhamentos pela futura Diretiva SRI 2, nomeadamente:

- Algumas definições (artigo 3.º) foram alinhadas pelas que constam da "SRI 2";
- Foi aditado um novo artigo 7.º-A sobre avaliações voluntárias pelos pares, em consonância com a "SRI 2", adaptado às necessidades das entidades da União;
- As obrigações de comunicação de informações constantes do artigo 20.º foram alinhadas pelas da "SRI 2".

b) Composição do Conselho Interinstitucional para a Cibersegurança (IICB) (artigo 9.º)

Na sequência dos debates sobre a participação adequada dos representantes dos Estados-Membros nos trabalhos do IICB, foi alcançado um compromisso sob a forma de uma declaração do Conselho a exarar na ata.

c) Autonomia institucional

Foi encontrada uma abordagem equilibrada entre a vontade dos Estados-Membros de reforçar os mecanismos de conformidade e a necessidade de respeitar o princípio da autonomia institucional, em especial no que diz respeito às auditorias e às medidas disciplinares (artigo 11.º).

Por último, a referência a uma percentagem específica do orçamento informático dedicada à cibersegurança foi suprimida do considerando 8.

CONCLUSÃO

11. Convida-se o Comité de Representantes Permanentes a:

a) Aprovar o texto de compromisso tal como consta do anexo, que constituirá o mandato para as negociações com o Parlamento Europeu;

b) Convidar o Conselho a aprovar o texto de compromisso, tal como consta do anexo, na sua reunião de 18 de novembro de 2022, e a exarar em ata a declaração do Conselho que consta da adenda ao presente documento.

ANEXO

2022/0085 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

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

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

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

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

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos Parlamentos nacionais,

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

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

(2) O panorama das ciberameaças com que as [...] **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: roubar informações confidenciais valiosas, obter ganhos pecuniários, manipular a opinião pública ou comprometer as infraestruturas digitais. O ritmo dos ataques desses perpetradores continua a intensificar-se, com campanhas cada vez mais sofisticadas e automatizadas que visam as partes mais expostas de sistemas cada vez mais alargados, explorando rapidamente qualquer vulnerabilidade.

(3) Os ambientes informáticos das **entidades** [...] da União apresentam interdependências e fluxos de dados integrados, e os seus utilizadores colaboram estreitamente entre si. Esta interligação implica que qualquer perturbação, mesmo que inicialmente confinada a uma [...] **entidade** da União, pode ter repercussões mais vastas e resultar em impactos negativos generalizados e duradouros nos outros. Além disso, os ambientes informáticos de certas [...] **entidades da União** estão ligados aos ambientes informáticos dos Estados-Membros, levando a que um incidente numa entidade da União possa representar um risco de cibersegurança para os ambientes informáticos dos Estados-Membros e vice-versa. **Além disso, as entidades da União tratam grandes volumes de informações muitas vezes sensíveis dos Estados-Membros e, por conseguinte, os incidentes poderão também ter um impacto negativo nos Estados-Membros. Por esse motivo, a cibersegurança das entidades da União reveste-se de grande importância também para os Estados--Membros**. **Informações específicas sobre incidentes poderão ainda facilitar a deteção de ciberameaças ou incidentes semelhantes que afetem os Estados-Membros.**

(4) As [...] **entidades** da União são alvos atrativos que enfrentam perpetradores com um elevado nível de competências e recursos, bem como outras ameaças. Ao mesmo tempo, o nível e a maturidade da ciber-resiliência e das capacidades de deteção e resposta a atividades informáticas maliciosas variam significativamente entre estas entidades. Para assegurar o correto funcionamento da administração europeia, é portanto necessário que as [...] **entidades** da União atinjam um elevado nível comum de cibersegurança por meio **da aplicação de medidas de cibersegurança,** [...] do intercâmbio de informações e da colaboração.

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

(6) Para garantir um elevado nível comum de cibersegurança, será necessário que cada [...] **entidade** da União estabeleça um quadro interno de gestão, governação e controlo dos riscos de cibersegurança que assegure uma gestão eficaz e prudente de todos os riscos de cibersegurança [...]. **O quadro deverá estabelecer políticas de cibersegurança, incluindo procedimentos de avaliação da eficácia das medidas de cibersegurança aplicadas. O quadro deverá basear-se numa abordagem multirriscos que visa a proteção das redes e dos sistemas de 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 da 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 de redes e sistemas de informações. O quadro deverá refletir as constatações das análises dos riscos, tendo em conta todos os riscos técnicos, operacionais e organizacionais pertinentes para a cibersegurança da entidade da União em causa.**

(6-A) Para gerir os riscos identificados no âmbito do quadro, cada entidade da União deverá assegurar que são tomadas medidas técnicas, operacionais e organizacionais adequadas e proporcionadas. Essas medidas deverão abordar os domínios, incluindo as medidas de cibersegurança estipuladas no presente regulamento para reforçar a cibersegurança de cada entidade da União.

(6-B) Os ativos e riscos identificados no quadro, bem como as conclusões tiradas de avaliações periódicas da maturidade deverão ser refletidos no plano de cibersegurança estabelecido por cada entidade da União. O plano de cibersegurança deverá incluir as medidas de cibersegurança adotadas, com o objetivo de aumentar a cibersegurança global da entidade da União em causa.

(6-C) Uma vez que garantir a cibersegurança é um processo contínuo, a adequação e eficácia de todas as medidas deverão ser regularmente revistas tendo em conta a evolução dos riscos, dos ativos e da maturidade das entidades da União. O quadro deverá ser revisto periodicamente e, no mínimo, de três em três anos, ao passo que o plano de cibersegurança deverá ser revisto pelo menos de dois em dois anos ou na sequência de cada avaliação da maturidade ou de cada revisão do quadro.

(6-D) As entidades da União deverão trocar periodicamente informações pertinentes, incluindo no que diz respeito a incidentes e ciberameaças pertinentes, garantindo ao mesmo tempo a confidencialidade e uma proteção adequada das informações prestadas pela entidade da União que as comunica.

(6-E) Deverá ser implementado um mecanismo que assegure a eficácia do intercâmbio de informações, da coordenação e da cooperação das entidades da União em caso de incidentes de grande envergadura, incluindo a determinação clara das funções e responsabilidades das entidades da União envolvidas. As informações trocadas deverão ser tidas em conta pelo ponto de contacto designado para a EU-CyCLONe aquando da partilha de informações pertinentes com esta rede a título de contributo para o conhecimento situacional comum.

(7) As diferenças existentes entre as [...] **entidades** da União exigem flexibilidade na aplicação, uma vez que uma única abordagem não se adequará a todos os casos. As medidas destinadas a garantir um elevado nível comum de cibersegurança não devem incluir nenhuma obrigação que interfira diretamente no exercício das missões das [...] **entidades** da União ou prejudique a sua autonomia institucional. Por conseguinte, essas [...] **entidades da União** deverão estabelecer os seus próprios quadros de gestão, governação e controlo dos riscos de cibersegurança **e planos de cibersegurança**, bem como adotar [...] [...] **medidas** 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 afetam negativamente a eficiência das operações e do intercâmbio de informações das entidades da União com outras entidades da União e autoridades nacionais competentes.**

(8) Para evitar impor encargos financeiros e administrativos desproporcionados às [...] **entidades** da União, os requisitos de gestão dos riscos de cibersegurança devem ser proporcionados em relação ao risco das redes e dos sistemas de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas. Cada [...] **entidade** da União deve procurar afetar uma percentagem adequada do seu orçamento informático à melhoria do respetivo nível de cibersegurança [...]. **A avaliação da maturidade deverá ainda averiguar se as despesas de uma determinada entidade da União no domínio da cibersegurança são proporcionais aos riscos que a mesma enfrenta.**

(9) Um elevado nível comum de cibersegurança exige que esses aspetos sejam supervisionados ao mais alto nível da direção de cada [...] **entidade** da União. [...] **A supervisão da aplicação do presente regulamento deverá incumbir à direção ao mais alto nível, além do estabelecimento do quadro de gestão, governação e controlo dos riscos e de planos de cibersegurança que incluam medidas de cibersegurança**. A cultura de cibersegurança, que corresponde às práticas de rotina em termos de segurança informática, constituirá parte integrante **do quadro** [...] em matéria de cibersegurança em todas as **entidades** [...] da União.

(10) [...] [...] Estas medidas **de cibersegurança** devem integrar [...] **o plano** em matéria de cibersegurança e ser especificadas em documentos de orientação ou recomendações emitidos pela CERT-UE. Na definição das medidas e orientações, devem ser tidas em devida conta **os progressos técnicos mais recentes e, se for caso disso, as normas europeias e internacionais pertinentes, bem como** a legislação e as políticas pertinentes da UE, incluindo as avaliações de risco e as recomendações emitidas pelo grupo de cooperação SRI, como a avaliação coordenada dos riscos a nível da UE e o conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G. Além disso, poderá ser exigida a certificação de produtos, serviços e processos de TIC pertinentes, ao abrigo de sistemas específicos de certificação da cibersegurança da UE adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881. **Se for caso disso, a CERT-UE deverá cooperar com a ENISA.**

(11) Em maio de 2011, os secretários-gerais das instituições e organismos da União decidiram pré-configurar uma equipa de resposta a emergências informáticas para as instituições, órgãos e organismos da UE (CERT-UE), supervisionada por um Comité Diretor interinstitucional. Em julho de 2012, os secretários-gerais confirmaram as disposições práticas e concordaram em manter a CERT-UE como entidade permanente para continuar a ajudar a melhorar o nível global de segurança das tecnologias da informação das instituições, órgãos e organismos da União, num exemplo bem visível da cooperação interinstitucional em matéria de cibersegurança. Em setembro de 2012, a CERT-UE foi criada na qualidade de grupo de trabalho da Comissão Europeia com um mandato interinstitucional. Em dezembro de 2017, as instituições e organismos da União celebraram um acordo interinstitucional sobre a organização e o funcionamento da CERT-UE[7]. 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**.

[...]

[7] JO C 12 de 13.1.2018, p. 1.

(13) 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 proativa, a resposta em caso de incidente ou a tomada de medidas de atenuação, as [...] **entidades** da União deverão notificar a CERT-UE das ciberameaças, vulnerabilidades**, quase incidentes e** [...] incidentes [...] , bem como partilhar pormenores técnicos adequados para permitir a deteção, atenuação ou resposta a ciberameaças, vulnerabilidades**, quase incidentes** e incidentes informáticos similares que possam afetar outras [...] **entidades** da União. Aplicando a mesma abordagem prevista na diretiva [proposta SRI 2], quando tenham tido conhecimento de um incidente significativo as entidades **da União** deverão [...] **desencadear um alerta rápido** dirigido à CERT-UE no prazo de 24 horas. Este intercâmbio de informações permitirá à CERT-UE divulgar as informações a outras [...] **entidades** da União, bem como às devidas contrapartes, de forma a proteger todos os ambientes informáticos, tanto da União como das suas contrapartes, contra incidentes [...] semelhantes.

(13-A) O presente regulamento define uma abordagem em várias etapas da comunicação de informações relativas a incidentes significativos, a fim de estabelecer o equilíbrio adequado entre, por um lado, uma comunicação de informações célere que ajude a minimizar a potencial propagação de incidentes significativos e permita às entidades da União procurar apoio e, por outro lado, uma comunicação de informações exaustiva que retire ensinamentos valiosos de incidentes individuais e melhore gradualmente a resiliência das entidades individuais da União face às ciberameaças . A este respeito, o presente regulamento deverá incluir a comunicação de informações relativas a incidentes que, com base numa avaliação inicial efetuada pela entidade da União, poderiam causar graves perturbações operacionais no funcionamento da entidade da União ou perdas financeiras para a entidade da União em causa, ou afetar outras pessoas singulares ou coletivas causando danos materiais ou imateriais consideráveis. Essa avaliação inicial deverá ter em conta, nomeadamente, as redes e os sistemas de 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.

(13-B) Visto que as infraestruturas e as redes 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 notificar a contraparte nacional da CERT-UE, designada pelo Estado-Membro nos termos da diretiva [proposta SRI 2], dentro do mesmo prazo para notificar um incidente significativo à CERT-UE. A CERT-UE deverá igualmente notificar a contraparte nacional em causa sempre que tenha conhecimento de um incidente significativo no Estado-Membro, exceto se esse incidente já tiver sido notificado pela entidade da União afetada.

(14) Para além da afetação de novas atribuições e de um papel mais interventivo à CERT-UE, deverá ser instituído um Conselho Interinstitucional para a Cibersegurança (IICB) que, **para facilitar um elevado nível comum de cibersegurança entre as entidades da União,** deverá **desempenhar um papel exclusivo** [...] [...] **no** acompanhamento da forma como aplicam o presente regulamento, supervisionando a concretização das prioridades e objetivos gerais pela CERT-UE e conferindo-lhe uma direção estratégica. **Por conseguinte,** o IICB deve assegurar a representação das instituições e integrar representantes dos diferentes órgãos e organismos, por meio da Rede de Agências da União. **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 do IICB. Além disso, o IICB poderá estabelecer 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, modalidades para 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.**

(15) A CERT-UE deve apoiar a implementação de medidas destinadas a garantir um elevado nível comum de cibersegurança por meio da apresentação de propostas de documentos de orientação e recomendações ao IICB ou do lançamento de apelos à ação. Os referidos documentos de orientação e recomendações deverão ser aprovados pelo IICB. Sempre que necessário, a CERT-UE deve lançar apelos à ação descrevendo medidas de segurança urgentes que [...] **entidades** da União são instadas a tomar num determinado prazo**.**
O IICB pode dar instruções à CERT-UE no sentido de que este emita, retire ou modifique uma proposta de documento de orientação ou de recomendação, ou um apelo à ação.

(16) O IICB deve acompanhar o cumprimento do presente regulamento e o seguimento dado aos seus documentos de orientação e recomendações, bem como aos apelos à ação [...]. O IICB deve ser apoiado em questões técnicas por grupos consultivos técnicos, com a composição que o IICB entenda, os quais devem trabalhar em estreita cooperação com a CERT-UE, as [...] **entidades** da União e outras partes interessadas, conforme necessário. [...] **Quando concluir que as entidades da União não aplicaram ou implementaram o presente regulamento, incluindo os documentos de orientação, as recomendações ou os apelos à ação emitidos ao abrigo do presente regulamento, o IICB poderá, sem prejuízo dos procedimentos internos da entidade da União em causa, avançar com medidas de conformidade. O sistema de medidas de conformidade deverá ser utilizado com uma gravidade progressiva, ou seja, quando o IICB adotar as medidas de conformidade deverá começar por um alerta (como medida menos grave) e, se necessário, ir por fases até à medida mais grave, ou seja um aviso a recomendar a suspensão temporária dos fluxos de dados para a entidade da União em causa, medida essa que seria aplicável em casos excecionais de incumprimento prolongado, deliberado e/ou grave por parte da entidade em causa das obrigações que lhe incumbem por força do presente regulamento.**

(16-A) O alerta representa a medida de conformidade menos grave para colmatar lacunas identificadas em relação à entidade da União e inclui recomendações para que a referida entidade altere os respetivos documentos de cibersegurança dentro de um prazo determinado. O alerta deverá estar disponível para todas as entidades da União, sob reserva de restrições adequadas nos termos do presente regulamento.

(16-B) O IICB poderá igualmente recomendar a realização de uma auditoria a uma entidade da União. A entidade da União poderá recorrer à sua função de auditoria interna para este efeito. O IICB poderá ainda 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.

(16-C) Com base nos resultados de uma auditoria realizada mediante recomendação ou pedido do IICB, este poderá ainda exigir à entidade da União que diligencie no sentido de conformar a gestão, a governação e o controlo dos riscos de cibersegurança às disposições do presente regulamento.

(16-D) Uma vez que os Estados-Membros partilham com as entidades da União pertinentes informações de caráter potencialmente sensível, a cibersegurança do destinatário de tais informações é fundamental para os Estados-Membros. Por conseguinte, em casos excecionais de incumprimento prolongado, deliberado, reiterado e/ou grave das obrigações que incumbem à entidade da União, o IICB poderá emitir, como medida de último recurso, um aviso para todos os Estados-Membros e entidades da União a recomendar a suspensão temporária dos fluxos de dados que envolvam a entidade da União em causa, o qual permanecerá em vigor até à retificação do estado da cibersegurança da entidade. Este aviso deverá ser comunicado a todos os Estados--Membros e entidades da União através de canais de comunicação segura adequados.

(16-E) **Para assegurar a correta aplicação do presente regulamento, se considerar que existe uma violação continuada do presente regulamento por parte de uma entidade da União, diretamente resultante das ações ou omissões de um membro do seu pessoal, incluindo a direção ao mais alto nível, o IICB deverá solicitar à entidade da União em causa que tome as medidas necessárias em relação ao membro do pessoal, em conformidade com o Estatuto e outras regras equivalentes aplicáveis a determinadas entidades da União. Essas medidas poderão incluir, por exemplo, processos disciplinares e, se for caso disso, no caso específico das agências da União, um pedido à autoridade competente para que tome as medidas necessárias ao possível despedimento da pessoa potencialmente responsável pela violação continuada do presente regulamento.**

(17) O CERT-UE deve ter como missão contribuir para a segurança do ambiente informático de todas as [...] **entidades** da União. **Ao ponderar prestar aconselhamento técnico ou contribuir com informações sobre questões estratégicas pertinentes a pedido de uma entidade da União, a CERT-UE deverá assegurar que tal não prejudica o cumprimento das suas outras atribuições estabelecidas no presente regulamento.**

(17-A) O CERT-UE deve exercer uma função equivalente à do coordenador designado para as [...] **entidades** da União, para fins de divulgação coordenada das vulnerabilidades ao respetivo registo europeu referido no artigo 6.º da diretiva [proposta SRI 2] **e deverá criar uma política relativa à gestão de vulnerabilidades que inclua a promoção e facilitação da divulgação coordenada voluntária das vulnerabilidades.**

[...]

(19) A CERT-UE deve também desempenhar o papel que lhe é conferido pela diretiva [proposta SRI 2] em matéria de cooperação e intercâmbio de informações com a rede de equipas de resposta a incidentes de segurança informática (CSIRT). Além disso, em consonância com a Recomendação (UE) 2017/1584[8] da Comissão, a CERT-UE deve cooperar e coordenar a resposta com as partes interessadas relevantes. A fim de contribuir para um elevado nível de cibersegurança na União, o CERT-UE deve partilhar informações específicas sobre incidentes com as suas contrapartes a nível nacional. O CERT-UE deve igualmente colaborar com outras contrapartes públicas e privadas, nomeadamente da NATO, sob reserva da aprovação prévia do IICB.

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

(20) No apoio à cibersegurança operacional, o CERT-UE deve recorrer aos conhecimentos especializados disponíveis da Agência da União Europeia para a Cibersegurança **(ENISA)** por meio de uma cooperação estruturada, conforme previsto no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[9]. Sempre que pertinente, devem ser acordadas entre as duas organizações as disposições adequadas para definir o modo de pôr em prática essa cooperação e evitar a duplicação de atividades. O CERT-UE deve cooperar com a [...] **ENISA** na análise das ameaças e partilhar periodicamente com a agência o seu relatório sobre o panorama das ameaças.

[...][10]

(22) **As atividades da CERT-UE e o tratamento de informações levado a cabo pela mesma nos termos do presente regulamento poderão envolver o tratamento de dados pessoais.** Qualquer tratamento de dados pessoais ao abrigo do presente regulamento deve respeitar a legislação em matéria de proteção de dados, incluindo o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[11]. **Sempre que, nos termos do presente regulamento, os dados pessoais sejam transmitidos a destinatários estabelecidos na União que não sejam as entidades da União, tal deverá processar-se em conformidade com o artigo 9.º do Regulamento (UE) 2018/1725.**

---

9 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).

10 [...]

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

(23) O tratamento das informações pela CERT-UE e pelas [...] **entidades** da União deve ser consentâneo com as regras **aplicáveis** [...] relativas à segurança da informação [...]. [...]

(23-A) 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 de fornecer informações sobre eventuais restrições impostas à divulgação ulterior das informações. É utilizado por quase todas as equipas de resposta a incidentes de segurança informática (CSIRT) e em alguns centros de análise e partilha de informações.

(24) **O presente regulamento e as novas atribuições da CERT-UE não terão qualquer efeito nas despesas totais ao abrigo do quadro financeiro plurianual.** Uma vez que os serviços e as atribuições do CERT-UE assumem interesse para todas as [...] **entidades** da União, cada uma dessas entidades que suporte despesas no domínio das tecnologias da informação deve contribuir com uma parte equitativa para esses serviços e atribuições. Essa contribuição não prejudica a autonomia orçamental das [...] **entidades** da União. **Todas as entidades da União e as respetivas administrações deverão assegurar a otimização dos seus recursos ao nível atual e reforçar os ganhos de eficiência, incluindo através do aprofundamento da cooperação interinstitucional no domínio da cibersegurança. Por conseguinte, deverá ser dada preferência a uma abordagem conjunta para agrupar as despesas administrativas, em vez de despesas efetuadas por cada entidade da União.**

(25) O IICB, com a assistência do CERT-UE, deve analisar e avaliar a implementação do presente regulamento, reportando à Comissão. Com base nessas informações, a Comissão apresentará relatório ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. **Além disso, convida-se o Tribunal de Contas Europeu a avaliar periodicamente o funcionamento da CERT-UE.**

ADOTARAM O PRESENTE REGULAMENTO:

Capítulo I
DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

1. O presente regulamento estabelece **medidas destinadas a alcançar um elevado nível comum de cibersegurança nas entidades da União** [...]

2. Para o efeito, o presente regulamento estabelece:

c) Obrigações no sentido de que **cada** [...] **entidade** da União crie [...] **um** quadro de gestão, governação e controlo dos riscos de cibersegurança;

d) Obrigações de gestão [...]**,** notificação **e partilha de informações** dos riscos de cibersegurança aplicáveis às [...] **entidades** da União;

e) Regras relativas à organização**, ao funcionamento** e às atividades da [...] **equipa interinstitucional autónoma de resposta a emergências informáticas** para as [...] **entidades** da União (CERT-UE) e relativas à organização**, ao funcionamento** e às atividades do Conselho Interinstitucional para a Cibersegurança **(IICB)**;

f) **Regras relativas ao acompanhamento da aplicação do presente regulamento.**

Artigo 2.º

Âmbito

1. O presente regulamento é aplicável a [...] todas as [...] **entidades** da União, à [...] [...] CERT-UE e ao **IICB** [...].

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

3. Com exceção do artigo 12.º, n.º 7, o presente regulamento não se aplica às redes e sistemas de 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 estabelecidos pelo Tratado da União Europeia, pelo Tratado sobre o Funcionamento da União Europeia ou pelo Tratado que institui a Comunidade Europeia da Energia Atómica, ou com base nesses tratados;

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

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

4) "Cibersegurança", a cibersegurança [...] **na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2019/881**;

5) "Direção ao mais alto nível", um dirigente ou um organismo de direção ou de coordenação e supervisão ao mais alto nível administrativo**, com capacidades de decisão**, tendo em conta as disposições em matéria de governação ao mais alto nível em cada [...] **entidade** da União;

5-A) "Quase incidente", um quase incidente na aceção do artigo 4.º, n.º 4-A, da diretiva [proposta SRI 2];

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

[...]

8) "**Incidente** de grande envergadura [...]", todo o 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) "Tratamento de incidentes", o tratamento de incidentes [...] na aceção do artigo 4.º, n.º 6, da diretiva [proposta SRI 2];

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

[...]

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

[...]

14) "[...] Risco", **um risco na aceção do artigo 4.º, n.º 7-B, da diretiva [proposta SRI 2]** [...];

[...]

[...]

Artigo 3.º-A

Tratamento de dados pessoais

1) O tratamento de dados pessoais ao abrigo do presente regulamento pela CERT-UE, o IICB ou as entidades da União é efetuado em conformidade com o Regulamento (UE) 2018/1725.

2) A CERT-UE, o IICB e as entidades da União tratam e trocam dados pessoais na medida do necessário e exclusivamente para efeitos de cumprimento das obrigações que lhes incumbem por força do presente regulamento.

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

Artigo 4.º

Quadro de gestão, governação e controlo dos riscos

1. Cada [...] **entidade** da União deve estabelecer o seu próprio [...] quadro de gestão, governação e controlo dos riscos de cibersegurança ("o quadro"), em apoio da missão da entidade [...]**.** [...] **O quadro** deve ser supervisionado ao mais alto nível de direção da entidade, a fim de assegurar uma gestão eficaz e prudente de todos os riscos de cibersegurança. O quadro deve ser posto em prática o mais tardar até ... [15 meses após a entrada em vigor do presente regulamento].

2. O quadro deve abranger a totalidade do ambiente informático **não classificado** da **entidade** [...] **da União** em causa, incluindo todos os ambientes informáticos nas instalações, **a rede de tecnologia operacional,** os ativos e serviços contratados externamente em ambientes de computação em nuvem ou alojados por terceiros, os dispositivos móveis, as redes institucionais, as redes institucionais não ligadas à Internet e todos os dispositivos ligados ao ambiente informático. O quadro **baseia-se numa abordagem multirriscos e numa avaliação da maturidade nos termos do artigo 6.º que abrange todos os riscos técnicos, operacionais e organizacionais pertinentes suscetíveis de afetar a cibersegurança da entidade da União em causa** [...].

2-A. **O quadro estabelece políticas de cibersegurança, incluindo objetivos e prioridades para a segurança das redes e dos sistemas de informação, e políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança aplicadas e definir as funções e as responsabilidades dos membros do pessoal**.

2-B. O quadro é revisto periodicamente e, no mínimo, de três em três anos, tendo em conta a evolução dos riscos, dos ativos e da maturidade da entidade da União.

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

3-A. **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 poderá delegar noutros altos funcionários da entidade em causa obrigações específicas ao abrigo do presente regulamento. Independentemente de uma eventual delegação de obrigações específicas, a direção ao mais alto nível poderá ser considerada responsável pelo incumprimento, por parte das entidades, das obrigações que lhes incumbem por força do presente regulamento.**

3-B. A direção ao mais alto nível de cada entidade da União garante que as entidades da União aprovam o plano de cibersegurança que inclui medidas de gestão dos riscos de cibersegurança, em consonância com as respetivas análises dos riscos, para que o quadro seja aplicado em conformidade com o presente regulamento.

[...]

5. Cada [...] **entidade** da União deve designar um responsável local pela cibersegurança, ou função equivalente, que atue como ponto de contacto único relativamente a todos os aspetos de cibersegurança.

   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 um 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 a entidade da União em causa e a CERT-UE. O IICB decide se a prestação deste serviço faz 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, dos responsáveis locais pela cibersegurança que são designados e de eventuais alterações subsequentes a este respeito. A CERT-UE conserva a lista periodicamente atualizada de responsáveis locais pela cibersegurança designados.

6. Os altos funcionários na aceção do artigo 29.º, n.º 2, do Estatuto[12] ou outros funcionários de nível equivalente que fazem parte de cada entidade da União frequentam ações específicas de formação numa base periódica, a fim de adquirirem conhecimentos e competências suficientes para compreender e avaliar os riscos e as práticas de gestão da cibersegurança, bem como o seu impacto nas atividades da organização.

---

12 Regulamento 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, JO L 56 de 4 de março de 1968.

7. Cada entidade da União deve dispor de mecanismos eficazes para assegurar que uma percentagem adequada do orçamento para as tecnologias da informação seja aplicada em cibersegurança. O quadro é devidamente tido em conta aquando da definição dessa percentagem.

Artigo 5.º

Medidas de gestão dos riscos de cibersegurança [...]

1. [...] **Cada entidade da União assegura, sob supervisão da respetiva** direção ao mais alto nível [...] [...], **que são aplicadas medidas técnicas, operacionais e organizacionais adequadas e proporcionadas para gerir os riscos identificados ao abrigo do quadro referido no artigo 4.º, n.º 1, e para prevenir e/ou atenuar o impacto de incidentes. Tendo em conta os progressos técnicos mais recentes e, se for caso disso, as normas europeias e internacionais pertinentes, bem como os custos da sua aplicação, estas medidas asseguram um nível de segurança das redes e dos sistemas de informação adequado aos riscos presentes. Ao avaliar a proporcionalidade dessas medidas, é devidamente tido em conta o grau de exposição da entidade aos riscos, a sua dimensão, a probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto nos planos societal e económico.**

[...]

3. As entidades da União abordam pelo menos os seguintes domínios específicos na aplicação das medidas de gestão dos riscos de cibersegurança no âmbito dos seus planos de cibersegurança, em consonância com os documentos de orientação e as recomendações do IICB:

a) Política de cibersegurança, em termos de especificação das ferramentas e medidas necessárias para alcançar os objetivos e as prioridades referidos no artigo 4.º e no artigo 5.º, n.º 4;

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

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

d) Gestão de ativos, incluindo o inventário dos ativos informáticos e o mapeamento da rede informática;

e) Segurança dos recursos humanos e controlo do acesso;

f) Segurança das operações;

g) Segurança das comunicações;

h) Aquisição, desenvolvimento e manutenção dos sistemas, incluindo tratamento e divulgação de vulnerabilidades;

i) 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 o seu prestador de serviços. 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;

j) Tratamento de incidentes e cooperação com a CERT-UE, por exemplo no quadro da conservação de registos e da monitorização da segurança;

k) Gestão da continuidade das atividades, como gestão de cópias de segurança e recuperação de catástrofes, e gestão de crises; e

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

4. As entidades da União incluem, no mínimo, as seguintes medidas específicas de gestão dos riscos de cibersegurança na aplicação de medidas a este respeito no âmbito dos seus planos de cibersegurança, em consonância com os documentos de orientação e as recomendações do IICB:

a) Objetivos e prioridades no que respeita à utilização de serviços de computação em nuvem na aceção do artigo 4.º, n.º 19, da diretiva [proposta SRI 2] e disposições técnicas que permitam o teletrabalho;

b) Medidas concretas para a utilização futura de princípios de confiança zero, incluindo um modelo de segurança e uma estratégia coordenada de cibersegurança e de gestão de sistemas assente no reconhecimento da existência de ameaças tanto dentro como fora das fronteiras tradicionais da rede;

c) Adoção por norma da autenticação multifatorial na rede e nos sistemas de informação;

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

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

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

ii) Da obrigação contratual de comunicar os incidentes, as vulnerabilidades e as ciberameaças, bem como de dispor de um sistema adequado de monitorização e resposta a incidentes;

f) A utilização de criptografia e cifragem, em especial a cifragem ponto a ponto;

g) Sistemas de comunicação segura dentro da organização.

Artigo 6.º

Avaliação da maturidade

1. Cada [...] **entidade** da União efetua**, quando adequado com a ajuda de terceiros especializados, uma** [...] avaliação da maturidade, pelo menos de três em três anos, incorporando todos os elementos do seu ambiente informático, tal como descrito no artigo 4.º, e tendo em conta os documentos de orientação e as recomendações pertinentes adotados em conformidade com o artigo 13.º.

2. O IICB, mediante recomendação da CERT-UE e após consultar a Agência da União Europeia para a Cibersegurança (ENISA), adota, no prazo de 4 meses a contar da entrada em vigor do presente regulamento, orientações metodológicas sobre a realização de avaliações da maturidade.

3. Uma vez concluída a avaliação da maturidade [...]**, a entidade da União transmite-a ao IICB. A primeira avaliação da maturidade é efetuada, o mais tardar, [12 meses após a entrada em vigor do presente regulamento].**

Artigo 7.º

Planos de cibersegurança

1. Na sequência das conclusões extraídas da avaliação da maturidade e tendo em conta os ativos e riscos identificados nos termos do artigo 4.º, a direção ao mais alto nível de cada [...] **entidade** da União deve aprovar um plano de cibersegurança, sem demora injustificada, após o estabelecimento do quadro [...], [...] **a adoção de** [...] **medidas de gestão dos riscos** [...] de cibersegurança **e a realização da avaliação da maturidade, e, o mais tardar, 21 meses após a entrada em vigor do presente regulamento**. O plano **de cibersegurança** visa reforçar a cibersegurança global da entidade [...] **da União em causa** e, por conseguinte, contribuir para [...] o reforço de um elevado nível comum de cibersegurança em todas [...] **entidades** da União. [...] **O** plano **de cibersegurança** deve incluir pelo menos **as medidas de gestão dos riscos de cibersegurança referidas no artigo 5.º** [...]. O plano **de cibersegurança** é revisto pelo menos de **dois em dois** [...] anos, **ou** na sequência de [...] **cada** avaliação da maturidade [...] realizada nos termos do artigo 6.º **ou de cada revisão do quadro realizada nos termos do artigo 4.º.**

2. [...]

3. O plano de cibersegurança deve **ter em conta** [...] os eventuais documentos de orientação e recomendações aplicáveis emitidos **nos termos do artigo 13.º** [...].

4. **Uma vez concluído o plano de cibersegurança, a entidade da União transmite-o ao IICB**.

Artigo 7.º-A

Análise pelos pares

1. O IICB estabelece, mediante recomendação da CERT-UE e após consultar a ENISA, o mais tardar ... [24 meses após a entrada em vigor do presente regulamento], recorrendo à metodologia para análises pelos pares e à metodologia para autoavaliação nos termos do artigo 16.º da diretiva [proposta SRI 2], adaptadas, se for caso disso, às necessidades das entidades da União, a metodologia e os aspetos organizacionais de uma análise pelos pares tendo em vista aprender com base nas experiências comuns, reforçar a confiança mútua, alcançar um elevado nível comum de cibersegurança, bem como melhorar as capacidades e políticas das entidades da União em matéria de cibersegurança necessárias para aplicar o presente regulamento. A participação na análise pelos pares é voluntária. Os representantes dos Estados-Membros podem participar nas análises pelos pares na qualidade de observadores. As análises pelos pares são realizadas por peritos em cibersegurança designados por pelo menos duas entidades da União, que não sejam as entidades da União objeto da análise, e abrangem pelo menos um dos seguintes aspetos:

i) o nível de aplicação das medidas de gestão dos riscos de cibersegurança e das obrigações de comunicação de informações referidas no artigo 5.º e no artigo 20.º;

ii) o nível das capacidades, nomeadamente os recursos financeiros, técnicos e humanos disponíveis;

iii) o nível de aplicação do quadro de partilha de informações, referido no artigo 19.º;

iv) questões específicas de caráter transetorial.

2. As entidades da União podem identificar questões específicas mencionadas no n.º 1, subalínea iv), para serem analisadas. O âmbito da análise, incluindo as questões identificadas, é comunicado às entidades da União participantes antes do início da análise pelos pares.

3. Antes do início da análise pelos pares, as entidades da União podem proceder a uma autoavaliação dos aspetos analisados e facultar essa autoavaliação aos peritos designados.

4. As análises pelos pares incluem visitas virtuais ou físicas aos locais e discussões fora do local. Tendo em conta o princípio da boa cooperação, as entidades da União que sejam objeto da análise pelos pares facultam aos peritos designados as informações necessárias para a avaliação, sem prejuízo da legislação nacional ou da União relacionada com a proteção de informações sensíveis ou classificadas. As informações obtidas durante o processo de análise pelos pares são utilizadas exclusivamente para esse fim. Os peritos que participam na análise pelos pares não podem divulgar a terceiros quaisquer informações sensíveis ou classificadas obtidas no decurso da referida análise.

5. Quando são objeto de uma análise pelos pares, os aspetos analisados nas entidades da União não são objeto de novas análises pelos pares nessas entidades da União durante os dois anos seguintes à conclusão da análise pelos pares, salvo pedido em contrário das entidades da União ou se acordado na sequência de uma proposta do IICB.

6. As entidades da União asseguram que eventuais riscos de conflito de interesses relativos aos peritos designados sejam revelados às outras entidades da União e ao IICB antes do início da análise pelos pares. As entidades da União objeto da análise pelos pares podem opor-se à designação de peritos específicos por motivos devidamente justificados e comunicados às entidades da União responsáveis pela designação.

7. **Os peritos que participam nas análises pelos pares elaboram relatórios sobre as constatações e conclusões dessas análises. As entidades da União são autorizadas a apresentar observações sobre os respetivos projetos de relatório, que devem ser anexadas aos relatórios. Os relatórios incluem recomendações de melhorias relativas aos aspetos abrangidos pela análise pelos pares. Quando pertinente, os relatórios são apresentados ao IICB e à rede CSIRT. As entidades da União objeto da análise podem optar por disponibilizar os seus relatórios, ou uma versão expurgada do mesmo, ao público.**

Artigo 8.º

Implementação

1. [...]

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

3. **Mediante pedido do IICB, as entidades da União comunicam informações sobre aspetos específicos do presente capítulo.**

Capítulo III
CONSELHO INTERINSTITUCIONAL PARA A CIBERSEGURANÇA

Artigo 9.º

Conselho Interinstitucional para a Cibersegurança

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

2. Cabe ao IICB:

   a) Acompanhar a implementação do presente regulamento por parte das **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 Europeia;

      v) o Tribunal de Justiça da União Europeia;

      vi) o Banco Central Europeu;

vii) o Tribunal de Contas Europeu;

viii) o Serviço Europeu para a Ação Externa;

ix) 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; e

xiii) a Agência da União Europeia para a Cibersegurança;

b) Três representantes [...] **designados** pela Rede de Agências da União Europeia (EUAN), mediante proposta do seu Comité Consultivo para as TIC, para representar os interesses dos órgãos e organismos que administram os seus próprios ambientes informáticos. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3-A. Os membros podem ser assistidos por um suplente. O presidente pode convidar outros representantes das **entidades** [...] acima enumeradas ou de outras [...] **entidades** da União para participarem nas reuniões do IICB, sem direito de voto.

4. Cabe ao IICB aprovar o seu regulamento interno.

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

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

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

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

9. O diretor da CERT-UE**, o presidente do grupo de cooperação SRI**, **o presidente da EU-CyCLONe e o presidente da rede CSIRT,** ou **os seus** [...] suplentes, [...] **podem** participar nas reuniões do IICB, salvo decisão em contrário do IICB**, na qualidade de observadores**.

10. O secretariado do IICB é assegurado pela **ENISA** [...] **e responde perante o presidente do IICB**.

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

12. [...]

13. O IICB pode **estabelecer** [...] um Comité Executivo para o assistir nos seus trabalhos e delegar-lhe algumas das suas atribuições e competências**, em especial as referidas no artigo 10.º, alíneas c) e e)**. Cabe ao IICB estabelecer o regulamento interno do Comité Executivo, incluindo as respetivas atribuições e poderes e a duração do mandato dos seus membros.

14. O IICB apresenta ao Conselho, de doze em doze meses, um relatório que descreve pormenorizadamente os progressos realizados na execução do presente regulamento e que especifica, em especial, a amplitude da cooperação da CERT-UE com as suas contrapartes nacionais em cada Estado-Membro. Este relatório constitui um contributo para o relatório bienal sobre o estado da cibersegurança na União durante o mesmo período de tempo, em conformidade com o artigo 15.º da diretiva [proposta SRI 2].

Artigo 10.º

Atribuições do IICB

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

a) [...] **Acompanhar e supervisionar eficazmente a aplicação** do presente regulamento [...] **e apoiar** [...] **as entidades** da União **no reforço da respetiva cibersegurança**; **para o efeito, o IICB pode solicitar relatórios *ad-hoc* à CERT-UE e às entidades da União;**

a-A) Na sequência de um debate estratégico, adotar uma estratégia plurianual para o aumento do nível de cibersegurança nas entidades da União e avaliá-la periodicamente, e pelo menos de cinco em cinco anos, e, quando necessário, alterá-la;

b) Aprovar, com base numa proposta **apresentada pelo** [...] diretor da CERT-UE, o programa de trabalho anual do CERT-UE e acompanhar a sua execução;

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

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

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

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

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

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

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

j) **Adotar documentos de orientação e recomendações com base numa proposta da CERT-UE nos termos do artigo 13.º, e dar instruções à CERT-UE no sentido de que emita, retire ou modifique uma proposta de documento de orientação ou de recomendação, ou um apelo à ação;**

k) Receber e avaliar documentos e relatórios apresentados pelas entidades da União nos termos do presente regulamento;

l) Apoiar o estabelecimento de um grupo informal que reúna os responsáveis locais pela cibersegurança de todas as entidades e, por conseguinte, facilitar o intercâmbio de boas práticas e de informações em relação à aplicação do presente regulamento;

m) Desenvolver um plano de gestão de crises de cibersegurança para apoiar a gestão coordenada de incidentes de grande envergadura a nível operacional que afetem as entidades da União e para contribuir para o intercâmbio periódico de informações pertinentes, nomeadamente sobre os impactos e a gravidade de incidentes de grande envergadura e as possíveis formas de atenuação.

Artigo 11.º

Conformidade

1. Cabe ao IICB**, nos termos do artigo 9.º, n.º 2 e do artigo 10.º,** acompanhar **de forma eficaz** a implementação, por parte das [...] **entidades** da União, do presente regulamento e dos documentos de orientação, recomendações e apelos à ação adotados. **Para o efeito, o IICB pode solicitar as informações ou os documentos necessários para avaliar a aplicação adequada das disposições do regulamento por parte das entidades da União. Para efeitos da adoção das medidas de conformidade nos termos do presente artigo, a entidade da União em causa não tem direitos de voto.**

2. Quando concluir que as **entidades** [...] da União não aplicaram ou implementaram efetivamente o presente regulamento ou algum dos documentos de orientação, recomendações ou apelos à ação emitidos ao abrigo do presente regulamento, o IICB pode, sem prejuízo dos procedimentos internos da **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) Emitir um alerta **para colmatar as lacunas identificadas num prazo especificado, incluindo recomendações para alterar documentos de cibersegurança adotados pelas entidades da União com base no presente regulamento**; quando necessário à luz de um manifesto risco de cibersegurança, o alerta deverá ser reservado a um universo devidamente restrito;

a-A) Emitir uma notificação fundamentada a uma entidade da União, caso as lacunas identificadas no alerta emitido anteriormente não tenham sido suficientemente colmatadas num prazo especificado, e notificar formalmente o Conselho, o Parlamento Europeu e a Comissão desse parecer;

b) **Emitir, em especial:** [...]

i. Uma recomendação de realização de uma auditoria a uma entidade da União;

ii. Um pedido de realização de uma auditoria por um terceiro prestador de serviços de auditoria.

c) Exigir à entidade da União que diligencie no sentido de conformar a gestão, a governação e o controlo dos riscos de cibersegurança às disposições do presente regulamento, se necessário, de uma forma e num prazo específicos.

d) Emitir um aviso para todos os Estados-Membros e todas as entidades da União recomendando a suspensão temporária dos fluxos de dados para a entidade da União.

3. Se o IICB tiver adotado medidas nos termos do n.º 2, alíneas a) a d), a entidade da União em causa apresenta uma descrição pormenorizada das medidas e ações aplicadas para colmatar as alegadas lacunas identificadas pelo IICB. A entidade da União apresenta essa descrição dentro de um prazo razoável a ser acordado com o IICB.

4. Se considerar que existe uma violação continuada das disposições do presente regulamento por parte de uma entidade da União, diretamente resultante de ações ou omissões de um funcionário ou outro agente da União, incluindo a direção ao mais alto nível, o IICB exige à entidade em causa que tome as medidas necessárias, nomeadamente de caráter disciplinar, em conformidade, em especial, com as regras estabelecidas no Estatuto dos Funcionários da União Europeia e Regime Aplicável aos outros agentes da União Europeia. Para o efeito, o IICB transmite as informações necessárias à entidade em causa.

Capítulo IV
CERT-UE

Artigo 12.º

Missão e atribuições da CERT-UE

1. [...] [...] **A missão da CERT-UE** é contribuir para a segurança do ambiente informático não classificado de todas as [...] **entidades** da União, aconselhando-as em matéria de cibersegurança, ajudando-as a prevenir, detetar, atenuar e dar resposta a incidentes e agindo como plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes.

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

2. O CERT-UE desempenha as seguintes funções em relação às [...] **entidades** da União:

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

b) [...] **Disponibilizar serviços normalizados da CSIRT a todas as entidades da União por meio de** um pacote de serviços de cibersegurança descritos no seu catálogo de serviços ("serviços de base");

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

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

e) **Com base nas informações referidas no n.º 1-A,** [...] contribuir para o conhecimento da situação cibernética na UE**, em estreita cooperação com a ENISA. Estas informações são partilhadas com o IICB, bem como com a rede CSIRT e o UE-INTCEN;**

f) Exercer uma função equivalente à da coordenadora designada para as entidades da União, como referido no artigo 6.º da diretiva [proposta SRI 2].

[...]

[...]

[...]

[...]

[...]

4. **No quadro das competências,** a CERT-UE enceta uma cooperação estruturada com a [...] **ENISA** para efeitos de reforço das capacidades, cooperação operacional e análises estratégicas a longo prazo das ciberameaças, em conformidade com o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.

5. 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 informático das [...] **entidades** da União, distintos dos referidos no n.º 2, com base em acordos de nível de serviço e sob reserva dos recursos disponíveis;

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

   c) Serviços de apoio à cibersegurança do ambiente informático de organizações distintas das [...] **entidades** da União mas que colaborem estreitamente com **as mesmas**, por exemplo, por possuírem atribuições ou responsabilidades ao abrigo do direito da União, com base em acordos reduzidos a escrito e mediante aprovação prévia do IICB.

6. A CERT-UE pode organizar **ou participar em** exercícios de cibersegurança ou recomendar a participação em exercícios existentes, em estreita colaboração com a [...] **ENISA**, sempre que aplicável, de forma a testar o nível de cibersegurança das [...] **entidades** da União.

7. A CERT-UE pode, se as **entidades da União** [...] envolvidas o solicitarem explicitamente, prestar assistência às [...] **entidades** da União relativamente a incidentes em ambientes informáticos classificados**, em conformidade com os respetivos procedimentos. Neste caso, não se aplicam as disposições estabelecidas nos artigos 19.º a 21.º do presente regulamento. A prestação de assistência pela CERT-UE nos termos do presente número é efetuada sem prejuízo das regras aplicáveis dos Estados-Membros ou da União relacionadas com a proteção de informações sensíveis ou classificadas.**

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

9. A CERT-UE pode monitorizar o tráfego da rede de uma entidade da União com o consentimento desta.

10. Se os serviços temáticos das entidades da União o solicitarem expressamente, a CERT-UE pode facultar informações ou aconselhamento técnico sobre questões estratégicas pertinentes.

11. A CERT-UE apoia, em cooperação com a Autoridade Europeia para a Proteção de Dados, as entidades da União em causa na resolução de incidentes que resultem em violações de dados pessoais.

Artigo 13.º

Documentos de orientação, recomendações e apelos à ação

1. A CERT-UE apoia a implementação 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. Sem demora injustificada após receber o apelo à ação, a entidade da União em causa informa a CERT-UE sobre a forma como essas medidas foram aplicadas;

   b) Propostas ao IICB com vista à adoção de documentos de orientação dirigidos a todas ou a um conjunto de [...] **entidades** da União;

   c) Propostas ao IICB com vista à adoção de recomendações dirigidas a [...] **entidades** da União a título individual.

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

   a) Modalidades ou melhorias da gestão dos riscos de cibersegurança e **das medidas de gestão dos riscos de cibersegurança** [...];

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

   c) Se for caso disso, a utilização em comum de uma tecnologia, arquitetura e das 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** [...]**.**

[...]

[...]

Artigo 14.º

Diretor da CERT-UE

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

2. 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 é responsável pela execução da direção estratégica, das orientações, dos objetivos e das prioridades definidas pelo IICB, assim como pela gestão da CERT-UE, nomeadamente dos seus recursos financeiros e humanos. O diretor informa regularmente o presidente do IICB.

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 66.º, n.º 9, do Regulamento Financeiro, e informa-o regularmente sobre a aplicação das medidas para as quais lhes tenham sido subdelegadas competências.

4. O diretor da CERT-UE elabora anualmente um planeamento financeiro das receitas e despesas administrativas relacionadas com as suas atividades, a proposta de programa de trabalho anual, a proposta de catálogo de serviços da CERT-UE e a respetiva revisão, a proposta de modalidades dos acordos de nível de serviço e a proposta de indicadores-chave de desempenho para a CERT-UE com vista à sua aprovação pelo IICB nos termos do artigo 10.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.

5. O diretor do CERT-UE apresenta [...] relatórios **anuais** ao IICB [...] sobre o desempenho da CERT-UE, o planeamento financeiro, as receitas, a execução orçamental, os acordos de nível de serviço e os acordos escritos celebrados, a colaboração com as contrapartes e os parceiros, bem como as missões realizadas pelos membros do seu pessoal, incluindo os relatórios referidos no artigo 10.º, [...] **alínea a)**.

Artigo 15.º

Questões financeiras e de pessoal

[...]

1-A. Embora criada como prestadora de serviços interinstitucional autónoma para todas as entidades da União, a CERT-UE é integrada na estrutura administrativa de uma Direção-Geral da Comissão, a fim de beneficiar das estruturas de apoio da Comissão em matéria administrativa, financeira, de gestão e de contabilidade. A Comissão informa o IICB da sede administrativa da CERT-UE, bem como de qualquer alteração desta. Essa abordagem é avaliada regularmente, o mais tardar até ao final de todos os quadros financeiros plurianuais estabelecidos nos termos do artigo 312.º do TFUE para possibilitar a aplicação das medidas adequadas.

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

3. As atribuições e atividades da CERT-UE, incluindo os serviços que preste nos termos do artigo 12.º, n.ºs 2, [...] 4 e 6, e do artigo 13.º, n.º 1, às [...] **entidades** da União financiados a partir da rubrica do quadro financeiro plurianual dedicada à administração pública europeia, são financiados por uma rubrica orçamental distinta do orçamento da Comissão. Os postos afetados 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 devem prestar uma contribuição financeira anual à CERT-UE para cobrir os serviços prestados pela CERT-UE nos termos desse mesmo n.º 3. As respetivas contribuições baseiam-se nas orientações dadas pelo IICB e acordadas entre cada entidade e 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 como receitas afetadas, tal como previsto no artigo 21.º, n.º 3, alínea c), do Regulamento (UE, Euratom) 2018/1046 do Parlamento Europeu e do Conselho[13].

5. Os custos das atribuições definidas no artigo 12.º, n.º 5, serão recuperados junto das [...] **entidades** da União que beneficiem dos serviços da CERT-UE. As receitas são afetadas às rubricas orçamentais às quais são imputados os custos.

[13] 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).

Artigo 16.º

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

1. A CERT-UE deve colaborar e trocar informações**, sem demora injustificada,** com as suas contrapartes nos Estados-Membros, **nomeadamente** [...] [...] [...] as CSIRT **referidas no artigo 9.º da diretiva [proposta SRI 2]**, **e/ou, se for caso disso, as autoridades nacionais competentes** e os pontos de contacto únicos referidos no artigo 8.º da diretiva [proposta SRI 2], relativamente a ciberameaças, vulnerabilidades e incidentes, a possíveis contramedidas e a todas as questões pertinentes para melhorar a proteção do ambiente informático das [...] **entidades** da União, nomeadamente por meio da rede de CSIRT referida no artigo 13.º da diretiva [proposta SRI 2].

1-A. A CERT-UE notifica, sem demora, as suas contrapartes nacionais pertinentes, referidas no n.º 1, num determinado Estado-Membro quando tiver conhecimento de incidentes significativos que ocorram no território desse Estado-Membro, exceto se a CERT-UE tiver conhecimento de que a entidade da União afetada já comunicou o incidente em causa nos termos do artigo 20.º, n.º 2-A.

2. A CERT-UE **troca** informações específicas sobre incidentes**, sem demora injustificada,** [...] com as suas contrapartes nacionais nos Estados-Membros, para facilitar a deteção de ciberameaças ou incidentes semelhantes **ou para contribuir para a análise de um incidente** sem **precisar** do consentimento da **entidade da União** [...] afetada. A CERT-UE **não** [...] partilha informações específicas sobre um determinado incidente de cibersegurança que revelem a identidade do seu alvo, **exceto se** [...]:

a) A entidade da União afetada tiver dado o seu consentimento;

b) A entidade da União afetada já tiver divulgado publicamente ter sido afetada;

c) Na ausência de consentimento por parte da entidade da União afetada, a publicação da identidade da União afetada aumentaria a probabilidade de evitar ou atenuar incidentes noutros locais. Essas decisões requerem a aprovação do diretor da CERT-UE. A entidade da União afetada é informada antes da publicação.

Artigo 17.º

Colaboração da CERT-UE com [...] ***<u>outras</u> contrapartes***

1. A CERT-UE pode colaborar com contrapartes **da União Europeia distintas das mencionadas no artigo 16.º**, nomeadamente setoriais [...], em matéria de ferramentas e métodos, como técnicas, táticas, procedimentos e boas práticas, bem como em matéria de ameaças e vulnerabilidades informáticas. No que respeita à colaboração com tais contrapartes, [...] a CERT-UE deve obter a aprovação prévia do IICB **numa base casuística. A CERT-UE informa todas as contrapartes nacionais pertinentes referidas no artigo 16.º, n.º 1, num Estado-Membro onde a contraparte se encontre, do estabelecimento da cooperação com tais contrapartes.**

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

3. Mediante consentimento da **entidade da União** [...] afetada por um incidente, a CERT-UE pode, **desde que seja celebrado um acordo ou contrato de não divulgação com o parceiro pertinente,** transmitir informações relacionadas com o **incidente específico** a parceiros **mencionados nos n.º 1 e 2, exclusivamente com vista a contribuir** [...] para a sua análise. **A legalidade de tais acordos ou contratos de não divulgação é verificada em conformidade com os procedimentos internos aplicáveis da Comissão. Os acordos ou contratos de não divulgação não carecem da aprovação prévia do IICB mas são levados ao conhecimento do seu presidente.**

4. **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.**

Capítulo V
OBRIGAÇÕES DE COOPERAÇÃO E DE COMUNICAÇÃO DE INFORMAÇÕES

Artigo 18.º
Tratamento de informações

1. A CERT-UE e as [...] **entidades** da União devem respeitar as obrigações de sigilo profissional nos termos do artigo 339.º do Tratado sobre o Funcionamento da União Europeia ou dos quadros equivalentes aplicáveis.

2. As disposições do Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho[14] são aplicáveis 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 e, quando pertinente, os Estados-Membros,** sempre que um pedido diga respeito a documentos seus.

[...]

4. O tratamento das informações pela CERT-UE e pelas [...] **entidades** da União deve ser consentâneo com as regras **aplicáveis** [...] relativas à segurança da informação [...].

[...]

Artigo 19.º

[...] ***Partilha de informações sobre cibersegurança***

-1. As entidades da União podem fornecer voluntariamente à CERT-UE informações sobre ciberameaças, incidentes, quase incidentes e vulnerabilidades que as afetem. A CERT-UE garante a disponibilidade de meios de comunicação eficazes com o objetivo de facilitar a partilha de informações com as entidades da União. A CERT-UE pode dar prioridade ao tratamento das notificações obrigatórias em relação às notificações voluntárias.

[14] 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).

1. Com vista a [...] **cumprir a sua missão e as suas atribuições nos termos do artigo 12.º**, a CERT-UE [...] pode solicitar que as [...] **entidades** da União lhe transmitam informações dos respetivos inventários de sistemas informáticos, **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 para detetar incidentes de cibersegurança** [...]. A [...] **entidade da União** requerida deve transmitir sem demora injustificada as informações solicitadas, bem como eventuais atualizações subsequentes dessas informações.

2. 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 especificar os tipos de informação digital de que necessita para fins de conhecimento situacional e resposta a incidentes.

3. A CERT-UE só pode partilhar **com as entidades da União** informações que permitam identificar a [...] **entidade** da União afetada por um determinado incidente com o consentimento dessa entidade. **Caso não seja dado o consentimento, a entidade em causa apresenta razões devidamente justificadas à CERT-UE.** [...]

4. As obrigações de partilha não abrangem as informações classificadas da UE (ICUE) nem as informações **cuja divulgação a outras partes que não a entidade da União recetora tenha sido excluída pelo remetente das informações por meio de marcação visível, salvo se o remetente das informações** [...] **permitir explicitamente a partilha das informações em causa com a CERT-UE.** [...]

Artigo 20.º

[...] ***Obrigações de <u>comunicação de informações</u>***

-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.

1. Todas as [...] **entidades** da União devem **apresentar** [...] **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 for o caso, indica se o incidente significativo foi presumivelmente causado por um ato ilícito ou malicioso ou se teve ou poderia ter um impacto transfronteiriço;

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 for o caso, atualiza as informações a que se refere a alínea a) e inclui uma avaliação inicial do incidente significativo, 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 notificação de incidente significativo a que se refere a alínea b), um relatório final que contenha, no mínimo, os seguintes elementos:

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

ii) o tipo de ameaça ou provável causa primária do incidente significativo;

iii) medidas de atenuação aplicadas e em curso;

iv) se for caso disso, o impacto transfronteiriço do incidente significativo.

e) Nos casos de incidentes significativos em curso no momento da apresentação do relatório final a que se refere a alínea d), um relatório intercalar simultâneo e um relatório final no prazo de um mês após a resolução do incidente.

[...]

g) [...]

h) [...]

i) [...]

j) [...]

2-A. Todas as entidades da União partilham, dentro do mesmo prazo, as informações comunicadas nos termos do n.º 1 com as contrapartes nacionais pertinentes referidas no artigo 16.º, n.º 1, no local onde se encontrem.

3. A CERT-UE apresenta [...] **trimestralmente ao IICB, ao UE-INTCEN e à rede CSIRT** [...] um relatório de síntese que inclua dados anonimizados e agregados sobre as [...] ciberameaças, [...] vulnerabilidades **nos termos do artigo 19.º, as respostas das entidades da União a apelos à ação nos termos do artigo 13.º, n.º 1, alínea a),** e incidentes de caráter significativo notificados em conformidade com o n.º 1. **Esse relatório constitui um contributo para o relatório bienal sobre o estado da cibersegurança na União, em conformidade com o artigo 15.º da diretiva [proposta SRI 2].**

4. O IICB **emite,** [...] **até [6 meses após a data de entrada em vigor do presente regulamento],** documentos de orientação ou recomendações **no sentido de especificar melhor** [...] as modalidades, **o formato** e o conteúdo da **comunicação de informações** [...]. **Os documentos de orientação ou recomendações têm devidamente em conta as disposições aplicadas por quaisquer atos de execução nos termos do artigo 20.º, n.º 11, da diretiva [proposta SRI 2]**. 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.

5. As obrigações de **comunicação de informações** [...] não abrangem as ICUE nem as informações **cuja divulgação a outras partes que não a entidade da União recetora tenha sido excluída pelo remetente das informações por meio de marcação visível, salvo se o remetente das informações** [...] **permitir explicitamente a partilha das informações com a CERT-UE.** [...]

Artigo 21.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 ciberameaças, vulnerabilidades e incidentes entre:

    a) [...] **Entidades** da União;

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

2. A CERT-UE facilita**,** [...] **se for caso disso, em cooperação com a ENISA nos termos do artigo 7.º, n.º 7, alínea d), do Regulamento Cibersegurança[15],** a coordenação entre as [...] **entidades** da União na resposta a incidentes, incluindo os seguintes elementos:

    a) Contribuição para uma comunicação externa coerente;

    [...]

    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 deve apoiar**, em estreita cooperação com a ENISA,** as [...] **entidades** da União no que respeita ao conhecimento situacional das ciberameaças, vulnerabilidades e incidentes.

---

15 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)

4. O IICB **adota, até [12 meses após a data de entrada em vigor do presente regulamento], com base numa proposta da CERT-UE,** [...] **documentos de orientação 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 orientações sobre a forma como deverá ser notificado às autoridades judiciárias.

Artigo 22.º

Gestão de incidentes de grande envergadura [...]

-1. A fim de apoiar a gestão coordenada de incidentes de grande envergadura a nível operacional que afetem entidades da União e de contribuir para o intercâmbio regular de informações pertinentes entre as unidades da União e com os Estados-Membros, o IICB elabora um plano de gestão de crises de cibersegurança com base nas atividades descritas no artigo 21.º, n.º 2, em estreita cooperação com a CERT-UE e a ENISA, que inclua, no mínimo, os seguintes elementos:

a) Modalidades de coordenação e fluxo de informações entre as entidades da União para gestão de incidentes de grande envergadura a nível operacional;

b) Instruções permanentes normalizadas comuns;

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

d) Exercícios regulares;

e) Canais de comunicação segura a utilizar;

f) Um ponto de contacto para a EU-CyCLONe, que partilha informações pertinentes com a EU-CyCLONe a título de contributo para o conhecimento situacional comum.

1. A CERT-UE coordena a resposta das [...] **entidades** da União a **incidentes** [...] de grande envergadura. Deve manter um inventário dos conhecimentos técnicos especializados necessários para a resposta aos incidentes quando ocorram **incidentes de grande envergadura** [...].

2. 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.

3. Na sequência de um pedido específico de um Estado-Membro no qual a entidade da União afetada se encontra, e mediante [...] a aprovação da **entidade** [...] da União [...] **afetada** [...], a CERT-UE também pode solicitar que os peritos da lista a que se refere o n.º 2 contribuam para a resposta a um **incidente** [...] de grande envergadura [...] **nessa entidade da União** [...]**.**

Capítulo VI
DISPOSIÇÕES FINAIS

Artigo 23.º

Reafetação orçamental inicial

A Comissão propõe a reafetação do pessoal e dos recursos financeiros das [...] **entidades** da União no quadro do orçamento da Comissão. A reafetação será efetiva com a aprovação do primeiro orçamento após a entrada em vigor do presente regulamento.

Artigo 24.º

Reexame

1. O IICB, com a assistência do CERT-UE, deve comunicar periodicamente à Comissão informações sobre a implementação do presente regulamento. O IICB pode também formular recomendações dirigidas à Comissão para que esta **reexamine** [...] o presente regulamento.

2. A Comissão apresenta um relatório sobre a implementação do presente regulamento ao Parlamento Europeu e ao Conselho o mais tardar **36**[...] meses após a entrada em vigor do presente regulamento e, posteriormente, de três em três anos.

3. Passados**, no máximo,** [...] cinco anos da sua entrada em vigor, a Comissão avaliará o funcionamento do presente regulamento e apresentará ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões o correspondente relatório. **Se necessário, o relatório é acompanhado de uma proposta legislativa.**

Artigo 25.º

Entrada em vigor

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

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

Feito em Bruxelas, em

Pelo Parlamento Europeu
A Presidente

Pelo Conselho
O Presidente

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ANEXO II

[...]

[...]

[...]

[...]

[...]

[...]

[...]