Parlamento Europeu
2019-2024

Comissão dos Assuntos Constitucionais

2022/0085(COD)

31.1.2023

PARECER

da Comissão dos Assuntos Constitucionais

dirigido à Comissão da Indústria, da Investigação e da Energia

sobre a 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
(COM(2022)0122 – C9-0122/2022 – 2022/0085(COD))

Relatora de parecer: Markéta Gregorová

PA_Legam

JUSTIFICAÇÃO SUCINTA

As instituições, órgãos e organismos da União Europeia têm funcionado nos últimos anos num contexto cada vez mais digitalizado de constante evolução tecnológica e consequente evolução dos níveis de ameaça à cibersegurança. Essa situação foi agravada pelo início da crise sanitária da COVID-19 e, nomeadamente, pelo aumento das práticas de teletrabalho, durante o qual o número de ataques sofisticados provenientes de uma vasta gama de fontes continuou a aumentar.

Atualmente, o panorama da cibersegurança, incluindo a governação, a ciber-higiene, a capacidade global e a maturidade, difere consideravelmente entre as instituições, órgãos e organismos da União, o que cria um obstáculo adicional a uma administração europeia aberta, eficiente e independente.

Por conseguinte, a relatora concorda que seria necessária uma abordagem de base entre as instituições, órgãos e organismos da União para a criação de sistemas e requisitos comuns de cibersegurança, a fim de assegurar que a cibersegurança evolui na mesma direção, contribuindo assim para a eficiência e a independência da administração europeia.

A relatora considera ainda que é extremamente importante existir um quadro de segurança sólido e coerente para proteger todo o pessoal, dados, redes de comunicação, sistemas de informação e processos de tomada de decisão da UE, contribuindo assim também para o funcionamento democrático da União Europeia. Uma cultura de segurança reforçada das instituições, órgãos e organismos da União também faria com que a Europa estivesse preparada para a era digital e criaria uma economia preparada para o futuro ao serviço das pessoas.

ALTERAÇÕES

A Comissão dos Assuntos Constitucionais insta a Comissão da Indústria, da Investigação e da Energia, competente quanto à matéria de fundo, a ter em conta as seguintes alterações:

Alteração 1

Proposta de regulamento
Considerando 1

Texto da Comissão	*Alteração*
(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	(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.	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 ***e comunicação («TIC»)***, 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.

Justificação

A proposta da Comissão faz referência às «tecnologias da informação» apesar de o termo adequado ser «tecnologias da informação e comunicação» (TIC), visto ser este o termo padrão utilizado na Diretiva SRI 2 e no Regulamento Cibersegurança.

Alteração 2

Proposta de regulamento
Considerando 2

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

automatizadas que visam as partes mais expostas de sistemas cada vez mais alargados, explorando rapidamente qualquer vulnerabilidade.	***automatizados*** que visam as partes mais expostas de sistemas cada vez mais alargados, explorando rapidamente qualquer vulnerabilidade.

Alteração 3

Proposta de regulamento
Considerando 3

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

Alteração 4
Proposta de regulamento
Considerando 4

Texto da Comissão	*Alteração*
(4) As instituições, órgãos e organismos da União são alvos atrativos que enfrentam perpetradores com um elevado nível de competências e recursos, bem como outras ameaças. Ao mesmo tempo, o nível e a maturidade da ciber-resiliência e das capacidades de deteção e resposta a atividades informáticas maliciosas variam	(4) As instituições, órgãos e organismos da União são alvos atrativos que enfrentam perpetradores com um elevado nível de competências e recursos, bem como outras ameaças. Ao mesmo tempo, o nível e a maturidade da ciber-resiliência e das capacidades de deteção e resposta a atividades informáticas maliciosas variam

significativamente entre estas entidades. Para assegurar o correto funcionamento da administração europeia, é portanto necessário que as instituições, órgãos e organismos da União atinjam um elevado nível comum de cibersegurança por meio de uma base de referência na matéria (um conjunto mínimo de regras de cibersegurança que as redes e os sistemas de informação têm de cumprir, de modo a ***minimizar*** os riscos de cibersegurança), do intercâmbio de informações e da colaboração.	significativamente entre estas entidades. Para assegurar o correto funcionamento da administração europeia, é portanto necessário que as instituições, órgãos e organismos da União atinjam um elevado nível comum de cibersegurança por meio de uma base de referência na matéria (um conjunto mínimo ***comum*** de regras de cibersegurança que as redes e os sistemas de informação têm de cumprir, de modo a ***limitar*** os riscos de cibersegurança), do intercâmbio ***regular e eficaz*** de informações e da colaboração ***e educação em cibersegurança***.

Alteração 5

Proposta de regulamento
Considerando 7

Texto da Comissão	*Alteração*
(7) As diferenças existentes entre as instituições, órgãos e organismos da União exigem flexibilidade na aplicação, uma vez que uma única abordagem não se adequará a todos os casos. As medidas destinadas a garantir um elevado nível comum de cibersegurança ***não*** devem ***incluir nenhuma obrigação que interfira diretamente no*** exercício das missões das instituições, órgãos e organismos da União ***ou prejudique*** a sua autonomia institucional. Por conseguinte, essas instituições, órgãos e organismos devem estabelecer os seus próprios quadros de gestão, governação e controlo dos riscos de cibersegurança, bem como adotar os seus próprios planos de cibersegurança e bases de referência.	(7) As diferenças existentes entre as instituições, órgãos e organismos da União exigem flexibilidade na aplicação, uma vez que uma única abordagem não se adequará a todos os casos. As medidas destinadas a garantir um elevado nível comum de cibersegurança devem ***contribuir para o*** exercício das missões das instituições, órgãos e organismos da União ***e ter em conta*** a sua autonomia institucional. Por conseguinte, essas instituições, órgãos e organismos devem estabelecer os seus próprios quadros de gestão, governação e controlo dos riscos de cibersegurança, bem como adotar os seus próprios planos de cibersegurança e bases de referência***, tendo em conta a coerência e a interoperabilidade dos seus quadros respetivos e com base no quadro comum estabelecido pelo presente regulamento***.

Alteração 6
Proposta de regulamento
Considerando 8

Texto da Comissão	*Alteração*
(8) Para evitar impor encargos financeiros e administrativos desproporcionados às instituições, órgãos e organismos da União, os requisitos de gestão dos riscos de cibersegurança devem ***ser proporcionados em relação*** ao risco das redes e dos sistemas de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas. Cada instituição, órgão e organismo da União deve procurar afetar ***uma percentagem adequada*** do seu orçamento ***informático*** à melhoria do respetivo nível de cibersegurança***, devendo*** a ***mais longo*** prazo ***procurar alcançar uma meta da ordem dos 10 %***.	(8) Para evitar impor encargos financeiros e administrativos desproporcionados às instituições, órgãos e organismos da União, os requisitos de gestão dos riscos de cibersegurança devem ***corresponder*** ao risco das redes e dos sistemas de informação em causa, tendo em conta os progressos técnicos mais recentes no que respeita a tais medidas. Cada instituição, órgão e organismo da União deve procurar afetar***, pelo menos, 10 %*** do seu orçamento ***das TIC*** à melhoria do respetivo nível de cibersegurança a ***médio*** prazo***, aumentado essa percentagem a longo prazo, se necessário***.

Alteração 7

Proposta de regulamento
Considerando 9

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

Alteração 8

Proposta de regulamento
Considerando 10

Texto da Comissão	*Alteração*
(10) As instituições, órgãos e organismos da União devem avaliar os riscos ligados ao seu relacionamento com fornecedores e prestadores de serviços, incluindo prestadores de serviços de armazenamento e tratamento de dados ou de serviços de segurança sob gestão de terceiros, e tomar medidas adequadas para os acautelar. Estas medidas devem integrar a base de referência em matéria de cibersegurança e ser especificadas em documentos de orientação ou recomendações emitidos pelo CERT-UE. Na definição das medidas e orientações, devem ser tidas em devida conta a legislação e as políticas pertinentes da UE, incluindo as avaliações de risco e as recomendações emitidas pelo grupo de cooperação SRI, como a avaliação coordenada dos riscos a nível da UE e o conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G. Além disso, poderá ser exigida a certificação de produtos, serviços e processos de TIC pertinentes, ao abrigo de sistemas específicos de certificação da cibersegurança da UE adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881.	(10) As instituições, órgãos e organismos da União devem avaliar os riscos ligados ao seu relacionamento com fornecedores e prestadores de serviços, incluindo prestadores de serviços de armazenamento e tratamento de dados ou de serviços de segurança sob gestão de terceiros, e tomar medidas adequadas para os acautelar. ***Estes fornecedores e prestadores de serviços devem ser cuidadosamente controlados, tendo em conta toda a extensão da cadeia de abastecimento e o ambiente económico e político em que operam.*** Sempre que estas relações representem um risco para a integridade dos processos democráticos na UE, devem ser terminadas sem demora injustificada. Estas medidas devem integrar a base de referência em matéria de cibersegurança e ser especificadas em documentos de orientação ou recomendações emitidos pelo CERT-UE. Na definição das medidas e orientações, devem ser tidas em devida conta a legislação e as políticas pertinentes da UE, incluindo as avaliações de risco e as recomendações emitidas pelo grupo de cooperação SRI, como a avaliação coordenada dos riscos a nível da UE e o conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G. Além disso, tendo em conta o panorama das ameaças e a importância de reforçar a resiliência, poderá ser exigida a certificação de produtos, serviços e processos de TIC pertinentes utilizados nas instituições, órgãos e organismos da União, ao abrigo de sistemas específicos de certificação da cibersegurança da UE adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881.

Alteração 9

Proposta de regulamento
Considerando 13

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

Alteração 10

Proposta de regulamento
Considerando 14

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

Alteração 11

Proposta de regulamento
Considerando 16

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

Alteração 12

Proposta de regulamento
Considerando 17

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

Alteração 13

Proposta de regulamento
Considerando 18

Texto da Comissão	*Alteração*
(18) Em 2020, o Comité Diretor do CERT-UE estabeleceu um novo objetivo estratégico no sentido de que o CERT-UE garantisse um nível abrangente de ciberdefesa para todas as instituições, órgãos e organismos da União, com uma amplitude e profundidade adequadas e uma adaptação contínua às ameaças atuais ou iminentes, incluindo ataques contra dispositivos móveis, ambientes de computação em nuvem e dispositivos da Internet das Coisas. Esse objetivo estratégico inclui igualmente centros de operações de segurança de largo espetro responsáveis pela monitorização das redes e das ameaças de maior gravidade. O CERT-UE deve apoiar as equipas de segurança ***informática*** das instituições, órgãos e organismos de maior dimensão, nomeadamente na monitorização	(18) Em 2020, o Comité Diretor do CERT-UE estabeleceu um novo objetivo estratégico no sentido de que o CERT-UE garantisse um nível abrangente de ciberdefesa para todas as instituições, órgãos e organismos da União, com uma amplitude e profundidade adequadas e uma adaptação contínua às ameaças atuais ou iminentes, incluindo ataques contra dispositivos móveis, ambientes de computação em nuvem e dispositivos da Internet das Coisas. Esse objetivo estratégico inclui igualmente centros de operações de segurança de largo espetro responsáveis pela monitorização das redes e das ameaças de maior gravidade. O CERT-UE deve apoiar as equipas de segurança ***das TIC*** das instituições, órgãos e organismos de maior dimensão, nomeadamente na monitorização

permanente de primeira linha, prestando todos os serviços nesse contexto às instituições, órgãos e organismos de pequena dimensão, bem como a alguns de média dimensão.

permanente de primeira linha, prestando todos os serviços nesse contexto às instituições, órgãos e organismos de pequena dimensão, bem como a alguns de média dimensão.

Alteração 14

Proposta de regulamento
Considerando 19-A (novo)

Texto da Comissão

Alteração

(19-A) A fim de assegurar uma melhor implementação das medidas e orientações em matéria de cibersegurança para as instituições, órgãos e organismos da União e consolidar uma cultura de cibersegurança, o CERT-UE deve igualmente reforçar a cooperação com a Rede de Centros Nacionais de Coordenação e o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança.

Alteração 15

Proposta de regulamento
Considerando 20

Texto da Comissão

Alteração

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

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

das ameaças e partilhar periodicamente com a agência o seu relatório sobre o panorama das ameaças.

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

partilhar periodicamente com a agência o seu relatório sobre o panorama das ameaças.

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

Alteração 16
Proposta de regulamento
Considerando 24

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

Alteração 17

Proposta de regulamento
Considerando 25

Texto da Comissão	*Alteração*
(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	(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***, pelo menos de três em três anos, um*** relatório ao Parlamento Europeu, ao Conselho, ao

Europeu e ao Comité das Regiões.	Comité Económico e Social Europeu e ao Comité das Regiões.

Alteração 18

Proposta de regulamento
Artigo 1 – parágrafo 1 – alínea a)

Texto da Comissão	*Alteração*
(a) Obrigações no sentido de que as instituições, órgãos e organismos da União criem um quadro interno de gestão, governação e controlo dos riscos de cibersegurança;	(a) (Não se aplica à versão portuguesa.)

Alteração 19

Proposta de regulamento
Artigo 1 – parágrafo 1 – alínea c)

Texto da Comissão	*Alteração*
(c) Regras relativas à organização e ao funcionamento do Centro de Cibersegurança para as instituições, órgãos e organismos da União («CERT-UE») e relativas à organização e ao funcionamento do Conselho Interinstitucional para a Cibersegurança («IICB»).	(c) (Não se aplica à versão portuguesa.)

Alteração 20

Proposta de regulamento
Artigo 2-A (novo)

Texto da Comissão	*Alteração*
	Artigo 2.º-A
	Tratamento de dados pessoais
	O tratamento de dados pessoais realizado pelo CERT-UE, o IICB e todas as instituições, órgãos e organismos da União ao abrigo do presente regulamento deve ser executado em conformidade com

	o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho.

Alteração 21

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 2

Texto da Comissão	*Alteração*
(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];	(2) «Rede e sistema de informação», uma rede e sistema de informação ***conforme definidos no*** artigo ***6***.º, n.º 1, da diretiva [proposta SRI 2];

Alteração 22

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 4

Texto da Comissão	*Alteração*
(4) «Cibersegurança», a cibersegurança ***na aceção do*** artigo ***4***.º, n.º ***3***, ***da diretiva [proposta SRI 2]***;	(4) «Cibersegurança», a cibersegurança ***conforme definida no*** artigo ***2***.º, n.º ***1***, ***do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho***[1-A];
	[1-A] 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).

Alteração 23

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 5

Texto da Comissão	*Alteração*

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

Alteração 24

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 7

Texto da Comissão	*Alteração*
(7) «Incidente significativo», qualquer incidente***, a menos que tenha um impacto limitado e seja suscetível de já ser bem compreendido em termos de método ou tecnologia.***	(7) «Incidente significativo», qualquer incidente ***que tenha causado ou seja suscetível de causar perturbações operacionais graves ao funcionamento da entidade da União ou perdas financeiras para a entidade da União em causa, ou que tenha afetado ou seja suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis.***

Alteração 25

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 11

Texto da Comissão	*Alteração*
(11) «Ciberameaça significativa», uma ciberameaça ***com intenção, oportunidade e capacidade de causar um incidente significativo***;	(11) «Ciberameaça significativa», uma ciberameaça ***conforme definida no artigo 6.º, n.º 11, da diretiva [proposta SRI 2]***;

Alteração 26

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 14

Texto da Comissão	*Alteração*
(14) ***«Risco de cibersegurança»***,	(14) ***«Risco»***, qualquer ***risco conforme***

qualquer ***circunstância ou evento razoavelmente identificável com potenciais efeitos adversos para a segurança das redes e dos sistemas de informação***;	***definido no artigo 6.º, n.º 9, da diretiva [proposta SRI 2]***;

Alteração 27

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 14-A (novo)

Texto da Comissão	*Alteração*
	(14-A) «ambiente das TIC», todos os produtos, serviços e processos de TIC virtuais ou nas instalações, conforme definidos no artigo 2.º do Regulamento (UE) 2019/881 e todas as redes e sistemas de informação, quer sejam propriedade de uma instituição, órgão ou organismo da União ou geridos por tal instituição, órgão ou organismo, ou sejam alojados por terceiros, incluindo os dispositivos móveis, as redes institucionais, as redes institucionais não ligadas à Internet e todos os dispositivos ligados ao ambiente das TIC;

Justificação

O termo foi transferido do artigo 4.º, n.º 2 da presente proposta para o artigo que estabelece as definições, visto ser utilizado de forma consistente em todo o texto. A definição sugerida para este termo resulta das definições dos seus componentes estabelecidas no artigo 2.º do Regulamento Cibersegurança (Regulamento (UE) 2019/881).

Alteração 28

Proposta de regulamento
Artigo 3 – parágrafo 1 – ponto 15

Texto da Comissão	*Alteração*
(15) «Ciberunidade Conjunta», uma plataforma virtual e física de cooperação para as diversas comunidades de cibersegurança na União, centrada na	***Suprimido***

coordenação operacional e técnica contra ciberameaças e incidentes transnacionais de grande envergadura na aceção da Recomendação da Comissão de 23 de junho de 2021;

Alteração **29**
Proposta de regulamento
Artigo 4 – n.º 1

Texto da Comissão	*Alteração*
1. Cada instituição, órgão e organismo da União deve estabelecer o seu próprio quadro interno de gestão, governação e controlo dos riscos de cibersegurança («o quadro»), em apoio da missão da entidade e no exercício da sua autonomia institucional. Este trabalho deve ser supervisionado ao mais alto nível de direção da entidade, ***a fim de*** assegurar uma gestão eficaz e prudente de todos os riscos de cibersegurança. O quadro deve ser posto em prática o mais tardar até ... [15 meses após a entrada em vigor do presente regulamento].	1. ***Com base numa auditoria exaustiva da segurança,*** cada instituição, órgão e organismo da União deve estabelecer o seu próprio quadro interno de gestão, governação e controlo dos riscos de cibersegurança («o quadro»), em apoio da missão da entidade e no exercício da sua autonomia institucional***, tendo igualmente em conta a coerência e interoperabilidade do seu quadro com os de outras instituições, órgãos e organismos relevantes***. Este trabalho deve ser supervisionado ao mais alto nível de direção da entidade, ***que deve ser responsável por*** 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 ***data de*** entrada em vigor do presente regulamento].

Alteração 30

Proposta de regulamento
Artigo 4 – n.º 2

Texto da Comissão	*Alteração*
2. O quadro deve abranger a totalidade do ambiente ***informático*** da instituição, órgão ou organismo em causa, incluindo todos os ambientes ***informáticos*** nas instalações, os ativos e serviços	2. O quadro deve abranger a totalidade do ambiente ***das TIC*** da instituição, órgão ou organismo em causa, incluindo todos os ambientes ***das TIC*** nas instalações, os ativos e serviços

contratados externamente em ambientes de computação em nuvem ou alojados por terceiros, os dispositivos móveis, as redes institucionais, as redes institucionais não ligadas à Internet e todos os dispositivos ligados ao ambiente ***informático***. O quadro deve ter em conta as questões da continuidade das atividades e da gestão das crises e abranger a segurança da cadeia de abastecimento, bem como a gestão dos riscos humanos suscetíveis de afetar a cibersegurança da instituição, órgão ou organismo da União em causa.	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 ***das TIC***. O quadro deve ter em conta as questões da continuidade das atividades e da gestão das crises e abranger a segurança da cadeia de abastecimento, bem como a gestão dos riscos humanos suscetíveis de afetar a cibersegurança da instituição, órgão ou organismo da União em causa.
Alteração 31 **Proposta de regulamento** **Artigo 4 – n.º 4**	
Texto da Comissão	*Alteração*
4. Cada instituição, órgão e organismo da União deve dispor de mecanismos eficazes para assegurar que ***uma percentagem adequada*** do orçamento para as ***tecnologias da informação*** seja ***aplicada*** em cibersegurança.	4. Cada instituição, órgão e organismo da União deve dispor de mecanismos eficazes para assegurar que***, pelo menos, 10 %*** do orçamento ***agregado*** para as ***TIC*** seja ***aplicado*** em cibersegurança ***a médio prazo***.
Alteração 32 **Proposta de regulamento** **Artigo 4 – n.º 5-A (novo)**	
Texto da Comissão	*Alteração*
	5-A. O responsável local pela cibersegurança deve cooperar com o encarregado da proteção de dados a que se refere o artigo 43.º do Regulamento (UE) 2018/1725, ao lidar com a sobreposição de atividades que aplicam a proteção de dados desde a conceção e por defeito a medidas de cibersegurança, selecionando medidas de cibersegurança que envolvam a proteção de dados pessoais, a gestão integrada dos riscos e o tratamento integrado de incidentes de segurança.

Alteração 33

Proposta de regulamento
Artigo 5 – n.º 1

Texto da Comissão	*Alteração*
1. Cabe à direção ao mais alto nível de cada instituição, órgão e organismo da União aprovar a sua própria base de referência em matéria de cibersegurança para fazer face aos riscos identificados no quadro referido no artigo 4.º, n.º 1, em apoio da sua missão e no exercício da sua autonomia institucional. A referida base de referência em matéria de cibersegurança deve ser criada o mais tardar até ... [18 meses após a entrada em vigor do presente regulamento] e abranger os domínios enumerados no anexo I e as medidas enumeradas no anexo II.	1. Cabe à direção ao mais alto nível de cada instituição, órgão e organismo da União aprovar a sua própria base de referência em matéria de cibersegurança para fazer face aos riscos identificados no quadro referido no artigo 4.º, n.º 1, em apoio da sua missão e no exercício da sua autonomia institucional***, em plena conformidade com os requisitos do presente regulamento e tendo em conta a coerência e a interoperabilidade dos seus quadros com os das outras instituições, órgãos e organismos relevantes, bem como com os documentos de orientação e as recomendações adotados pelo IICB sob proposta do CERT-EU e os regimes aplicáveis de certificação da cibersegurança da UE***. A referida base de referência em matéria de cibersegurança deve ser criada o mais tardar até ... [18 meses após a ***data de*** entrada em vigor do presente regulamento] e abranger os domínios enumerados no anexo I e as medidas enumeradas no anexo II.

Alteração 34

Proposta de regulamento
Artigo 5 – n.º 2

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

organização.	***adequados. Para além dessas formações específicas e para efeitos de criação e consolidação de uma cultura de cibersegurança, a formação regular dos membros do pessoal em matéria de cibersegurança deve ser incluída no plano de cibersegurança e atualizada pelo menos de dois em dois anos. Há que assegurar recursos suficientes para proporcionar uma formação de qualidade.***

Alteração 35

Proposta de regulamento
Artigo 6 – parágrafo 1

Texto da Comissão	*Alteração*
Cada instituição, órgão e organismo da União efetua uma avaliação da maturidade em matéria de cibersegurança, pelo menos de ***três*** em ***três*** anos, incorporando todos os elementos do seu ambiente ***informático***, tal como descrito no artigo 4.º, e tendo em conta os documentos de orientação e as recomendações pertinentes adotados em conformidade com o artigo 13.º.	Cada instituição, órgão e organismo da União efetua uma avaliação da maturidade em matéria de cibersegurança ***até... [6 meses após a entrada em vigor do presente regulamento] e, posteriormente***, pelo menos de ***dois*** em ***dois*** anos, incorporando todos os elementos do seu ambiente ***das TIC***, 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. ***A avaliação da maturidade deve basear-se em auditorias independentes de cibersegurança por prestadores confirmados.***

Alteração 36

Proposta de regulamento
Artigo 7 – n.º 1

Texto da Comissão	*Alteração*
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	1. Na sequência das conclusões extraídas da avaliação da maturidade e tendo em conta os ativos e riscos identificados nos termos do artigo 4.º, a direção ao mais alto nível de cada

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

Alteração 37

Proposta de regulamento
Artigo 7 – n.º 2

Texto da Comissão	*Alteração*
2. O plano de cibersegurança deve incluir as funções e responsabilidades dos diferentes membros do pessoal necessárias à sua execução.	2. O plano de cibersegurança deve incluir as funções***, preparação*** e responsabilidades dos diferentes membros do pessoal necessárias à sua execução.

Alteração 38

Proposta de regulamento
Artigo 7 – n.º 3

Texto da Comissão	*Alteração*
3. O plano de cibersegurança deve ***considerar os eventuais*** documentos de orientação e recomendações aplicáveis emitidos pelo CERT-UE.	3. O plano de cibersegurança deve ***incluir todas as medidas propostas expressas nos*** documentos de orientação e recomendações aplicáveis emitidos pelo CERT-UE.

Alteração 39

Proposta de regulamento
Artigo 7 – n.º 3-A (novo)

Texto da Comissão	*Alteração*
	3-A. As instituições, órgãos e organismos da União devem apresentar os seus planos de cibersegurança ao Conselho Interinstitucional para a Cibersegurança (IICB). Esses planos devem ser partilhados, na medida do possível, sem correr o risco de revelar ou divulgar informações sensíveis ou confidenciais sobre a arquitetura e as capacidades técnicas específicas de cibersegurança da entidade da União a terceiros não autorizados.

Alteração 40

Proposta de regulamento
Artigo 9 – n.º 2 – alínea a)

Texto da Comissão	*Alteração*
(a) Acompanhar a implementação do presente regulamento por parte das instituições, órgãos e organismos da União***;*** e	(a) Acompanhar a implementação do presente regulamento por parte das instituições, órgãos e organismos da União e ***formular recomendações para alcançar um elevado nível comum de cibersegurança;***

Alteração 41

Proposta de regulamento
Artigo 9 – n.º 3 – parágrafo 1 – parte introdutória

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

Alteração 42

Proposta de regulamento
Artigo 9 – n.º 3 – parágrafo 1 – alínea k-A) (nova)

Texto da Comissão	*Alteração*
	(k-A) A Autoridade Europeia para a Proteção de Dados.

Alteração 43

Proposta de regulamento
Artigo 10 – parágrafo 1 – alínea a-A) (nova)

Texto da Comissão	*Alteração*
	(a-A) Aprovar, com base numa proposta do chefe do CERT-UE, recomendações para alcançar um elevado nível comum de cibersegurança, dirigidas a uma ou a todas as instituições, órgãos e organismos da União;

Alteração 44

Proposta de regulamento
Artigo 11 – parágrafo 1 – alínea a)

Texto da Comissão	*Alteração*

(a) Emitir um alerta que, quando necessário à luz de um manifesto risco de cibersegurança, deverá ser reservado a um universo devidamente restrito;	(a) Emitir um alerta que, quando necessário à luz de um manifesto risco de cibersegurança, deverá ser reservado a um universo devidamente restrito***, com base numa metodologia acordada em comum***;

Alteração 45

Proposta de regulamento
Artigo 11 – parágrafo 1 – alínea b)

Texto da Comissão	*Alteração*
(b) ***Recomendar que*** um serviço de auditoria pertinente ***realize*** uma auditoria.	(b) ***Encarregar*** um serviço de auditoria pertinente ***de realizar*** uma auditoria.

Alteração 46

Proposta de regulamento
Artigo 12 – n.º 1

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

Alteração 47
Proposta de regulamento
Artigo 12 – n.º 2 – alínea d)

Texto da Comissão	*Alteração*
(d) Chamar a atenção do IICB para qualquer questão relacionada com a implementação do presente regulamento e dos documentos de orientação,	(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;	recomendações e apelos à ação ***e apresentar propostas de reparação***;

Alteração 48
Proposta de regulamento
Artigo 12 – n.º 4

Texto da Comissão	*Alteração*
4. O CERT-UE enceta uma cooperação estruturada com a Agência da União Europeia para a Cibersegurança para efeitos de reforço das capacidades, cooperação operacional e análises estratégicas a longo prazo das ciberameaças, em conformidade com o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.	4. O CERT-UE enceta uma cooperação estruturada com a Agência da União Europeia para a Cibersegurança para efeitos de reforço das capacidades, cooperação operacional e análises estratégicas a longo prazo das ciberameaças, em conformidade com o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho. ***Além disso, o CERT-UE pode cooperar e trocar informações com o Centro Europeu da Cibercriminalidade.***

Alteração 49
Proposta de regulamento
Artigo 12 – n.º 5 – parte introdutória

Texto da Comissão	*Alteração*
5. O CERT-UE pode prestar os seguintes serviços não descritos no seu catálogo de serviços («serviços sujeitos a cobrança»):	5. O CERT-UE pode prestar ***às instituições, órgãos e organismos da União*** os seguintes serviços não descritos no seu catálogo de serviços («serviços sujeitos a cobrança»):

Alteração 50

Proposta de regulamento
Artigo 12 – n.º 5 – alínea a)

Texto da Comissão	*Alteração*
(a) Serviços de apoio à cibersegurança	(a) Serviços de apoio à cibersegurança

do ambiente ***informático*** das instituições, órgãos e organismos da União, distintos dos referidos no n.º 2, com base em acordos de nível de serviço e sob reserva dos recursos disponíveis;	do ambiente ***das TIC*** das instituições, órgãos e organismos da União, distintos dos referidos no n.º 2, com base em acordos de nível de serviço e sob reserva dos recursos disponíveis;

Alteração 51

Proposta de regulamento
Artigo 12 – n.º 5 – alínea b)

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

Alteração 52
Proposta de regulamento
Artigo 12 – n.º 5 – alínea c)

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

Alteração 53

Proposta de regulamento
Artigo 12 – n.º 6

Texto da Comissão	*Alteração*
6. O CERT-UE pode organizar exercícios de cibersegurança ou recomendar a participação em exercícios existentes, em estreita colaboração com a Agência da União Europeia para a Cibersegurança, sempre que aplicável, de forma a testar o nível de cibersegurança das instituições, órgãos e organismos da União.	6. O CERT-UE pode organizar exercícios de cibersegurança ou recomendar a participação em exercícios existentes, ***de forma regular e*** em estreita colaboração com a Agência da União Europeia para a Cibersegurança, sempre que aplicável, de forma a testar o nível de cibersegurança das instituições, órgãos e organismos da União. ***Além disso, através de uma cooperação reforçada e de programas conjuntos com o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação, o CERT-UE pode apoiar a investigação e a inovação e ajudar a reforçar as capacidades de cibersegurança das instituições, órgãos e organismos da União.***

Alteração 54

Proposta de regulamento
Artigo 12 – n.º 7

Texto da Comissão	*Alteração*
7. O CERT-UE ***pode***, se ***o constituinte*** envolvido o solicitar explicitamente, prestar assistência às instituições, órgãos e organismos da União relativamente a incidentes em ambientes ***informáticos classificados***.	7. O CERT-UE ***deve***, se ***a instituição, órgão ou organismo da União*** envolvido o solicitar explicitamente, prestar assistência às instituições, órgãos e organismos da União relativamente a incidentes em ambientes ***classificados das TIC e se o CERT-UE dispuser dos recursos adequados para o fazer ou os obtenha da entidade em questão***.

Alteração 55

Proposta de regulamento
Artigo 14 – parágrafo 1

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

Alteração 56

Proposta de regulamento
Artigo 16 – n.º 1

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

Alteração 57

Proposta de regulamento
Artigo 16 – n.º 2

Texto da Comissão	*Alteração*
2. O CERT-UE pode trocar informações específicas sobre incidentes com as suas contrapartes nacionais nos	2. O CERT-UE pode trocar informações específicas sobre incidentes com as suas contrapartes nacionais nos

Estados-Membros, para facilitar a deteção de ciberameaças ou incidentes semelhantes, sem o consentimento do ***constituinte afetado***. O CERT-UE só pode partilhar informações específicas sobre um determinado incidente de cibersegurança que revelem a identidade do seu alvo com o consentimento ***do constituinte*** afetado.	Estados-Membros, para facilitar a deteção de ciberameaças ou incidentes semelhantes, sem o consentimento ***da instituição, órgão ou organismo da União afetado, desde que o tratamento de dados pessoais cumpra as disposições aplicáveis*** do ***Regulamento (UE) 2018/1725***. O CERT-UE só pode partilhar informações específicas sobre um determinado incidente de cibersegurança que revelem a identidade do seu alvo com o consentimento ***da instituição, órgão ou organismo da União*** afetado.

Alteração 58

Proposta de regulamento
Artigo 17 – n.º 1

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

Alteração 59

Proposta de regulamento
Artigo 17 – n.º 2

Texto da Comissão	*Alteração*
2. O CERT-UE pode colaborar com outros parceiros, como entidades comerciais, organizações internacionais,	2. O CERT-UE pode colaborar com outros parceiros, como entidades comerciais, organizações internacionais,

entidades nacionais de países terceiros ou determinados peritos, de forma a recolher informações sobre as ciberameaças, vulnerabilidades e contramedidas possíveis, em termos gerais e específicos. Para uma colaboração mais alargada com tais parceiros, o CERT-UE deve obter a aprovação prévia do IICB.	entidades nacionais de países terceiros ou determinados peritos, de forma a recolher informações sobre as ciberameaças, vulnerabilidades e contramedidas possíveis, em termos gerais e específicos. Para uma colaboração mais alargada com tais parceiros, o CERT-UE deve obter a aprovação prévia do IICB. ***Qualquer cooperação deste tipo deve respeitar a integridade democrática da UE.***

Alteração 60

Proposta de regulamento
Artigo 17 – n.º 3

Texto da Comissão	*Alteração*
3. Mediante consentimento ***do constituinte*** afetado por um incidente, o CERT-UE pode transmitir informações relacionadas com o mesmo a parceiros que possam contribuir para a sua análise.	3. Mediante consentimento ***da instituição, órgão ou organismo da União*** afetado por um incidente, o CERT-UE pode transmitir informações relacionadas com o mesmo a parceiros que possam contribuir para a sua análise.

Alteração 61

Proposta de regulamento
Artigo 19 – n.º -1 (novo)

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

Alteração 62

Proposta de regulamento
Artigo 19 – n.º 1

Texto da Comissão	*Alteração*
1. Com vista a ***permitir ao CERT-UE coordenar a gestão das vulnerabilidades e a resposta a incidentes***, o CERT-UE pode solicitar que as ***instituições, órgãos e organismos*** da União lhe transmitam informações dos respetivos inventários de sistemas ***informáticos que sejam relevantes para fins do apoio a prestar pelo CERT-UE.*** A ***instituição***, ***órgão ou organismo requerido*** deve transmitir sem demora injustificada as informações solicitadas, bem como eventuais atualizações subsequentes dessas informações.	1. Com vista a ***cumprir a sua missão e as suas atribuições nos termos do artigo 12.º***, o CERT-UE pode solicitar que as ***entidades*** da União lhe transmitam informações dos respetivos inventários de sistemas ***das TIC, incluindo informações relacionadas com ciberameaças, quase incidentes, vulnerabilidades, indicadores de exposição*** a ***riscos***, ***alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança destinadas a detetar incidentes de cibersegurança. A entidade requerida*** deve transmitir sem demora injustificada as informações solicitadas, bem como eventuais atualizações subsequentes dessas informações.

Alteração 63

Proposta de regulamento
Artigo 19 – n.º 2

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

Alteração 64
Proposta de regulamento
Artigo 20 – título

Texto da Comissão	*Alteração*
Obrigações de ***notificação***	Obrigações de ***comunicação de informações***

Alteração 65

Proposta de regulamento
Artigo 20 – n.º 1 – parágrafo 1

Texto da Comissão	*Alteração*
Todas as instituições, órgãos e organismos da União devem ***proceder a uma notificação inicial*** ao CERT-UE ***das*** ciberameaças, vulnerabilidades e incidentes de caráter significativo sem demora injustificada e, em todo o caso, o mais tardar no prazo de 24 horas após terem tomado conhecimento dos mesmos.	Todas as instituições, órgãos e organismos da União devem ***fazer chegar um alerta rápido*** ao CERT-UE ***sobre as*** ciberameaças, vulnerabilidades e incidentes de caráter significativo sem demora injustificada e, em todo o caso, o mais tardar no prazo de 24 horas após terem tomado conhecimento dos mesmos. ***O alerta rápido deve, se for caso disso, indicar se presumivelmente o incidente significativo foi causado por atos ilícitos ou maliciosos e se é suscetível de ter um impacto transfronteiriço;***

Alteração 66

Proposta de regulamento
Artigo 20 – n.º 1 – parágrafo 2

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

Alteração 67

Proposta de regulamento
Artigo 20 – n.º 2 – parte introdutória

Texto da Comissão	*Alteração*
2. As instituições, órgãos e organismos da União devem igualmente ***notificar*** ao CERT-UE, sem demora injustificada, pormenores técnicos sobre as ciberameaças, vulnerabilidades e incidentes que permitam a adoção de medidas para a deteção, resposta ou atenuação dos efeitos desses mesmos incidentes. A notificação deve incluir, se disponível:	2. As instituições, órgãos e organismos da União devem igualmente ***enviar uma notificação*** ao CERT-UE, sem demora injustificada ***e***, ***em qualquer caso, no prazo de 72 horas após terem tomado conhecimento do incidente significativo, atualizar o alerta rápido e fornecer uma avaliação inicial do incidente, da sua gravidade e do seu impacto, com os*** pormenores técnicos sobre as ciberameaças, vulnerabilidades e incidentes que permitam a adoção de medidas para a deteção, resposta ou atenuação dos efeitos desses mesmos incidentes. A notificação deve incluir, se disponível:

Alteração 68
Proposta de regulamento
Artigo 20 – n.º 2 – parágrafo 1 (novo)

Texto da Comissão	*Alteração*
	Nos casos devidamente justificados e com o acordo do CERT-UE, a instituição, órgão ou organismo da União em causa pode não cumprir esse prazo.

Alteração 69

Proposta de regulamento
Artigo 20 – n.º 2-A (novo)

Texto da Comissão	*Alteração*
	2-A. No prazo de um mês após a apresentação da notificação do incidente significativo, as instituições, órgãos e organismos da União devem apresentar um relatório final ao CERT-UE, incluindo, pelo menos, o seguinte:
	(a) uma descrição pormenorizada do incidente significativo, da sua gravidade e

	do seu impacto,
	(b) o tipo de ameaça ou provável causa primária do incidente significativo, (c) as medidas de atenuação aplicadas e em curso;
	(c) as medidas de atenuação aplicadas e em curso;
	(d) se for caso disso, o impacto transfronteiriço do incidente significativo;
	Nos casos de incidentes significativos em curso no momento da apresentação do relatório final a que se refere o presente número, deve ser apresentado relatório intercalar nesse momento e um relatório final um mês após a resolução do incidente.

Alteração 70

Proposta de regulamento
Artigo 20 – n.º 2-B (novo)

Texto da Comissão	*Alteração*
	2-B. Em determinados casos devidamente justificados e com o acordo do CERT-UE, a instituição, órgão ou organismo da União em causa poderá não cumprir o prazo previsto no n.º 2-A.

Alteração 71

Proposta de regulamento
Artigo 20 – n.º 3

Texto da Comissão	*Alteração*
3. O CERT-UE apresenta mensalmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre as ciberameaças, vulnerabilidades e incidentes de caráter significativo notificados em conformidade com o n.º 1.	3. O CERT-UE apresenta mensalmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre as ciberameaças, vulnerabilidades e incidentes de caráter significativo notificados em conformidade com o n.º 1. ***Esse relatório constitui um contributo para o relatório bienal sobre o***

	estado da cibersegurança na União, em conformidade com o artigo 18.º da diretiva [proposta SRI 2].

Alteração 72

Proposta de regulamento
Artigo 20 – n.º 4

Texto da Comissão	*Alteração*
4. O IICB ***pode*** emitir documentos de orientação ou recomendações sobre as modalidades e o conteúdo da notificação. O CERT-UE divulga os pormenores técnicos necessários para permitir uma deteção proativa, a resposta a incidentes ou a tomada de medidas de atenuação por parte das instituições, órgãos e organismos da União.	4. O IICB ***deve*** emitir documentos de orientação ou recomendações sobre as modalidades e o conteúdo da notificação. O CERT-UE divulga os pormenores técnicos necessários para permitir uma deteção proativa, a resposta a incidentes ou a tomada de medidas de atenuação por parte das instituições, órgãos e organismos da União.

Alteração 73

Proposta de regulamento
Artigo 20 – n.º 5

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

Alteração 74

Proposta de regulamento
Artigo 24 – n.º 2

Texto da Comissão	*Alteração*
2. A Comissão apresenta um relatório	2. A Comissão apresenta um relatório

sobre a implementação do presente regulamento ao Parlamento Europeu e ao Conselho o mais tardar ***48*** meses após a entrada em vigor do presente regulamento e, posteriormente, de ***três*** em ***três*** anos.	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 ***dois*** em ***dois*** anos.

Alteração 75

Proposta de regulamento
Artigo 24 – n.º 3

Texto da Comissão	*Alteração*
3. Passados pelo menos ***cinco*** anos da sua entrada em vigor, a Comissão avaliará o funcionamento do presente regulamento e apresentará ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões o correspondente relatório.	3. Passados pelo menos ***três*** anos da sua entrada em vigor***, dado o panorama das ciberameaças em rápida evolução***, a Comissão avaliará o funcionamento do presente regulamento e apresentará ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões o correspondente relatório.

Alteração 76

Proposta de regulamento
Anexo I — parágrafo 1 — parte introdutória

Texto da Comissão	*Alteração*
A base de referência em matéria de cibersegurança abordará os seguintes domínios:	A base de referência em matéria de cibersegurança abordará***, pelo menos,*** os seguintes domínios:

Alteração 77

Proposta de regulamento
Anexo I – parágrafo 1 – ponto 1-A (novo)

Texto da Comissão	*Alteração*
	(1-A) formação do pessoal em matéria de cibersegurança;

Alteração 78

Proposta de regulamento

Anexo I – parágrafo 1 – ponto 3

Texto da Comissão	*Alteração*
(3) gestão de ativos, incluindo o inventário dos ativos ***informáticos*** e o mapeamento da rede ***informática***;	(3) ***aquisição e*** gestão de ativos, incluindo o inventário dos ativos ***das TIC*** e o mapeamento da rede ***das TIC***;

Alteração 79

Proposta de regulamento
Anexo I – parágrafo 1 – ponto 7

Texto da Comissão	*Alteração*
(7) aquisição, desenvolvimento e manutenção dos sistemas;	(7) aquisição, desenvolvimento e manutenção dos sistemas***, incluindo o desenvolvimento interno de software de código aberto***;

Alteração 80

Proposta de regulamento
Anexo I – parágrafo 1 – ponto 7-A (novo)

Texto da Comissão	*Alteração*
	(7-A) auditorias de cibersegurança;

Alteração 81

Proposta de regulamento
Anexo I – parágrafo 1 – ponto 9

Texto da Comissão	*Alteração*
(9) gestão de incidentes, incluindo abordagens para melhorar a preparação, a resposta e a recuperação de incidentes e a cooperação com o CERT-UE, por exemplo no quadro da conservação de registos e da monitorização da segurança;	(9) gestão de incidentes, incluindo abordagens para melhorar a preparação, a resposta***, o cumprimento e redução dos prazos para as obrigações de comunicação de informações*** e a recuperação de incidentes e a cooperação com o CERT-UE, por exemplo no quadro da conservação de registos e da monitorização da segurança;

Alteração 82

Proposta de regulamento
Anexo II – parágrafo 1 – ponto 3-A) (novo)

Texto da Comissão	*Alteração*
	(3-A) formação regular do pessoal em matéria de cibersegurança;

Alteração 83

Proposta de regulamento
Anexo II – parágrafo 1 – ponto 4 – alínea a)

Texto da Comissão	*Alteração*
(a) da remoção dos obstáculos contratuais que limitam a partilha de informações com o CERT-UE por parte dos prestadores de serviços ***informáticos*** sobre os incidentes, vulnerabilidades e as ciberameaças;	(a) da remoção dos obstáculos contratuais que limitam a partilha de informações com o CERT-UE por parte dos prestadores de serviços ***de TIC*** sobre os incidentes, vulnerabilidades e as ciberameaças;

PROCESSO DA COMISSÃO ENCARREGADA DE EMITIR PARECER

Título	Estabelecimento de medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União
Referências	COM(2022)0122 – C9-0122/2022 – 2022/0085(COD)
Comissão competente quanto ao fundo Data de comunicação em sessão	ITRE 4.4.2022
Parecer emitido por Data de comunicação em sessão	AFCO 4.4.2022
Relator(a) de parecer Data de designação	Markéta Gregorová 20.6.2022
Exame em comissão	26.10.2022 1.12.2022
Data de aprovação	25.1.2023
Resultado da votação final	+: 24 –: 0 0: 0
Deputados presentes no momento da votação final	Gerolf Annemans, Gabriele Bischoff, Damian Boeselager, Gwendoline Delbos-Corfield, Salvatore De Meo, Daniel Freund, Charles Goerens, Esteban González Pons, Laura Huhtasaari, Victor Negrescu, Max Orville, Domènec Ruiz Devesa, Helmut Scholz, Pedro Silva Pereira, Sven Simon, Guy Verhofstadt, Loránt Vincze, Rainer Wieland
Suplentes presentes no momento da votação final	Nathalie Colin-Oesterlé, Pascal Durand, Seán Kelly, Jaak Madison, Maite Pagazaurtundúa
Suplentes (art. 209.º, n.º 7) presentes no momento da votação final	Leszek Miller

VOTAÇÃO NOMINAL FINAL
NA COMISSÃO ENCARREGADA DE EMITIR PARECER

24	+
ID	Gerolf Annemans, Laura Huhtasaari, Jaak Madison
PPE	Nathalie Colin-Oesterlé, Salvatore De Meo, Esteban González Pons, Seán Kelly, Sven Simon, Loránt Vincze, Rainer Wieland
Renew	Charles Goerens, Max Orville, Maite Pagazaurtundúa, Guy Verhofstadt
S&D	Gabriele Bischoff, Pascal Durand, Leszek Miller, Victor Negrescu, Domènec Ruiz Devesa, Pedro Silva Pereira
The Left	Helmut Scholz
Verts/ALE	Damian Boeselager, Gwendoline Delbos-Corfield, Daniel Freund

0	-

0	0

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções