C/2024/1049

9.2.2024

Parecer do Comité das Regiões Europeu — Regulamento Cibersolidariedade e Resiliência Digital da UE

(C/2024/1049)

Relator:	Pehr GRANFALK (SE-PPE), membro da Assembleia Municipal de Solna
Texto de referência:	Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades na União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança COM(2023) 209 final

I. RECOMENDAÇÕES DE ALTERAÇÃO

COM(2023) 209

Alteração 1

Considerando 1

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
A utilização e a dependência de tecnologias da informação e comunicação tornaram-se características fundamentais de todos os setores de atividade económica, uma vez que as nossas administrações públicas, as nossas empresas e os nossos cidadãos nunca estiveram tão interligados e dependentes de outros setores e países.	A utilização e a dependência de tecnologias da informação e comunicação tornaram-se características fundamentais***, mas também expuseram as vulnerabilidades*** de todos os setores de atividade económica, uma vez que as nossas administrações públicas, as nossas empresas e os nossos cidadãos nunca estiveram tão interligados e dependentes de outros setores e países.

Justificação

Evidente.

Alteração 2

Considerando 3

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
É necessário reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Tal como recomendado em três propostas diferentes da Conferência sobre o Futuro da Europa, é necessário aumentar a resiliência dos cidadãos, das empresas e das entidades que operam infraestruturas críticas contra as ameaças crescentes à cibersegurança, que podem ter impactos societais e económicos devastadores. […]	É necessário reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Tal como recomendado em três propostas diferentes da Conferência sobre o Futuro da Europa, é necessário aumentar a resiliência dos cidadãos, das empresas***, da administração pública a nível local, regional e nacional*** e das entidades que operam infraestruturas críticas contra as ameaças crescentes à cibersegurança, que podem ter impactos societais e económicos devastadores. […]

Justificação

Os órgãos de poder local e regional prestam serviços próximos dos cidadãos e críticos para a sociedade e constituem um dos elementos mais essenciais de um mercado europeu dinâmico.

Alteração 3

Considerando 29

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
No âmbito das ações de preparação, a fim de promover uma abordagem coerente e de reforçar a segurança em toda a União e o seu mercado interno, deve ser prestado apoio para testar e avaliar de forma coordenada a cibersegurança das entidades que operam nos setores altamente críticos identificados nos termos da Diretiva (UE) 2022/2555. Para o efeito, a Comissão, com o apoio da ENISA e em colaboração com o grupo de cooperação SRI criado pela Diretiva (UE) 2022/2555, deve identificar regularmente os setores ou subsetores pertinentes que devem ser elegíveis para receber apoio financeiro para a realização de testes coordenados a nível da União. Os setores ou subsetores devem ser selecionados do anexo I da Diretiva (UE) 2022/2555 («setores de importância crítica»). Os exercícios de teste coordenados […]	No âmbito das ações de preparação, a fim de promover uma abordagem coerente e de reforçar a segurança em toda a União e o seu mercado interno, deve ser prestado apoio para testar e avaliar de forma coordenada a cibersegurança das entidades que operam nos setores altamente críticos identificados nos termos da Diretiva (UE) 2022/2555. Para o efeito, a Comissão, com o apoio da ENISA e em colaboração com o grupo de cooperação SRI criado pela Diretiva (UE) 2022/2555, deve identificar regularmente os setores ou subsetores pertinentes que devem ser elegíveis para receber apoio financeiro para a realização de testes coordenados a nível da União. Os setores ou subsetores***, bem como as entidades da administração pública a nível regional e local, independentemente de serem ou não consideradas de importância crítica nos termos da legislação nacional,*** devem ser selecionados do anexo I da Diretiva (UE) 2022/2555 («setores de importância crítica»). Os exercícios de teste coordenados […]

Justificação

Uma vez que os Estados-Membros têm a possibilidade de excluir os órgãos de poder local e regional da aplicação da Diretiva SRI 2 ([1]), cabe garantir que, em compensação, são tidos em conta no Regulamento Cibersolidariedade.

Alteração 4

Considerando 30

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
Além disso, o mecanismo de ciberemergência deve prestar apoio a outras ações de preparação e apoiar a preparação noutros setores não abrangidos pelos testes coordenados de entidades que operam em setores ***altamente*** críticos. Essas ações poderão incluir vários tipos de atividades de preparação nacionais.	Além disso, o mecanismo de ciberemergência deve prestar apoio a outras ações de preparação e apoiar a preparação noutros setores não abrangidos pelos testes coordenados de entidades que operam em setores críticos. ***O mesmo se deve aplicar à administração pública, independentemente de ser ou não considerada um setor crítico nos termos da legislação nacional.*** Essas ações poderão incluir vários tipos de atividades de preparação nacionais.

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

Justificação

Os órgãos de poder local e regional devem ter a possibilidade de recorrer ao apoio do mecanismo de ciberemergência.

Alteração 5

Considerando 33

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
Deve ser criada progressivamente uma reserva de cibersegurança a nível da União, composta por prestadores privados de serviços de segurança geridos para apoiar ações de resposta e recuperação imediata em caso de incidentes de cibersegurança significativos ou em grande escala. A Reserva de Cibersegurança da UE deve assegurar a disponibilidade e prontidão dos serviços. Os serviços da Reserva de Cibersegurança da UE devem servir para apoiar as autoridades nacionais na prestação de assistência às entidades afetadas ***que operam em setores críticos ou altamente críticos*** em complemento das suas próprias ações a nível nacional. Ao solicitarem o apoio da Reserva de Cibersegurança da UE, os Estados-Membros devem especificar o apoio prestado à entidade afetada a nível nacional, que deve ser tido em conta na avaliação do pedido do Estado-Membro. Os serviços da Reserva de Cibersegurança da UE podem também servir para apoiar as instituições, órgãos e organismos da União em condições semelhantes.	Deve ser criada progressivamente uma reserva de cibersegurança a nível da União, composta por prestadores privados de serviços de segurança geridos para apoiar ações de resposta e recuperação imediata em caso de incidentes de cibersegurança significativos ou em grande escala. A Reserva de Cibersegurança da UE deve assegurar a disponibilidade e prontidão dos serviços. Os serviços da Reserva de Cibersegurança da UE devem servir para apoiar as autoridades nacionais na prestação de assistência às entidades afetadas em complemento das suas próprias ações a nível nacional. Ao solicitarem o apoio da Reserva de Cibersegurança da UE, os Estados-Membros devem especificar o apoio prestado à entidade afetada a nível nacional, que deve ser tido em conta na avaliação do pedido do Estado-Membro. Os serviços da Reserva de Cibersegurança da UE podem também servir para apoiar as instituições, órgãos e organismos da União em condições semelhantes.

Justificação

As entidades afetadas devem receber apoio da Reserva de Cibersegurança da UE e não apenas quando operem em setores críticos ou altamente críticos.

Alteração 6

Artigo 1.º, n.º 2, alínea b)

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
Aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos na União e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente mediante a disponibilização de apoio da União para resposta a incidentes de cibersegurança a países terceiros associados ao Programa Europa Digital;	Aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos***, bem como da administração pública a nível nacional e infranacional,*** na União e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente mediante a disponibilização de apoio da União para resposta a incidentes de cibersegurança a países terceiros associados ao Programa Europa Digital;

Justificação

O regulamento em apreço também deve abranger as administrações públicas a nível infranacional.

Alteração 7

Artigo 4.º, n.º 1, segundo parágrafo

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
Tem capacidade para atuar como ponto de referência e de acesso a outras organizações públicas e privadas a nível nacional para recolher e analisar informações sobre ameaças e incidentes de cibersegurança e contribuir para um SOC transfronteiriço. […]	Tem capacidade para atuar como ponto de referência e de acesso a outras organizações públicas e privadas a nível nacional ***e infranacional*** para recolher e analisar informações sobre ameaças e incidentes de cibersegurança e contribuir para um SOC transfronteiriço. […]

Justificação

Os centros de operações de segurança (SOC) nacionais também devem recolher e analisar informações de entidades do nível local e regional.

Alteração 8

Artigo 5.º, n.º 2

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
Na sequência de um convite à manifestação de interesse, o ECCC seleciona um consórcio de acolhimento para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder ao consórcio de acolhimento uma subvenção para financiar o funcionamento das ferramentas e infraestruturas. A contribuição financeira da União cobre até 75 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo consórcio de acolhimento. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o consórcio de acolhimento devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.	Na sequência de um convite à manifestação de interesse, o ECCC seleciona um consórcio de acolhimento para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder ao consórcio de acolhimento uma subvenção para financiar o funcionamento das ferramentas e infraestruturas. A contribuição financeira da União cobre até 75 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo consórcio de acolhimento ***com fundos que não os previstos no Regulamento (UE) 2021/1060 (Regulamento Disposições Comuns)***. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o consórcio de acolhimento devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.

Justificação

As medidas no quadro do Regulamento Cibersolidariedade não devem ser financiadas pelos programas no âmbito da política de coesão.

Alteração 9

Artigo 9.º, n.º 1

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
É criado um mecanismo de ciberemergência para melhorar a resiliência da União a ameaças ***graves*** à cibersegurança e para preparar e atenuar, num espírito de solidariedade, o impacto a curto prazo de incidentes de cibersegurança significativos e em grande escala («mecanismo»).	É criado um mecanismo de ciberemergência para melhorar a resiliência da União a ameaças à cibersegurança e para preparar e atenuar, num espírito de solidariedade, o impacto a curto prazo de incidentes de cibersegurança significativos e em grande escala («mecanismo»).

Justificação

O mecanismo de ciberemergência deve servir para preparar e atenuar o impacto a curto prazo de todos os tipos de incidentes de cibersegurança.

Alteração 10

Artigo 10.º, n.º 2 (novo)

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
	2. A Comissão elabora um relatório anual de avaliação do funcionamento do mecanismo e da eventual necessidade de requisitos adicionais em matéria de cooperação ou formação.

Justificação

A Comissão deve apresentar relatórios periódicos, uma vez que a cibersegurança está sempre em evolução e os requisitos têm de ser adaptados à realidade em tempo útil.

Alteração 11

Artigo 11.º, n.º 1

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
A fim de apoiar os testes coordenados de preparação das entidades a que se refere o artigo 10.º, n.º 1, alínea a), na União, a Comissão, após consulta do grupo de cooperação SRI e da ENISA, deve identificar os setores ou subsetores em causa com base nos setores de importância crítica enumerados no anexo I da Diretiva (UE) 2022/2555, consoante os quais as entidades podem ser sujeitas aos testes coordenados de preparação, tendo em conta as avaliações coordenadas dos riscos e os testes de resiliência existentes e planeados a nível da União.	A fim de apoiar os testes coordenados de preparação das entidades a que se refere o artigo 10.º, n.º 1, alínea a), na União, a Comissão, após consulta do grupo de cooperação SRI e da ENISA, deve identificar os setores ou subsetores em causa com base nos setores de importância crítica enumerados no anexo I da Diretiva (UE) 2022/2555***, incluindo as administrações públicas ao nível local,*** consoante os quais as entidades podem ser sujeitas aos testes coordenados de preparação, tendo em conta as avaliações coordenadas dos riscos e os testes de resiliência existentes e planeados a nível da União.

Justificação

Os órgãos de poder local e regional devem ter a oportunidade de beneficiar do mecanismo de ciberemergência. A proposta de alteração integra nos artigos da proposta de regulamento o pedido do relator expresso na alteração 3 (considerando 30).

Alteração 12

Artigo 14.º, n.º 2, alínea b)

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
O tipo de entidade afetada, dando maior prioridade aos incidentes que afetem entidades essenciais na aceção do artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555;	O tipo de entidade afetada, ***incluindo as entidades da administração pública a nível local e regional,*** dando maior prioridade aos incidentes que afetem entidades essenciais na aceção do artigo 3.º, n.º 1, da Diretiva (UE) 2022/2555;

Justificação

Clarificação do âmbito de aplicação com a inclusão das entidades infranacionais.

Alteração 13

Artigo 18.º, n.º 1

Texto da proposta da Comissão Europeia	Alteração proposta pelo CR
A pedido da Comissão, da UE-CyCLONe ou da rede de CSIRT, a ENISA analisa e avalia as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA apresenta um relatório de análise do incidente à rede de CSIRT, à UE-CyCLONe e à Comissão, a fim de as apoiar no desempenho das suas funções, em especial tendo em conta as enunciadas nos artigos 15.º e 16.º da Diretiva (UE) 2022/2555. Se for caso disso, a Comissão partilha o relatório com o alto representante.	A pedido da Comissão, da UE-CyCLONe ou da rede de CSIRT, a ENISA analisa e avalia as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA apresenta um relatório de análise do incidente à rede de CSIRT, à UE-CyCLONe e à Comissão, a fim de as apoiar no desempenho das suas funções, em especial tendo em conta as enunciadas nos artigos 15.º e 16.º da Diretiva (UE) 2022/2555. ***Se for possível, a rede de CSIRT partilha o relatório com a administração pública infranacional.*** Se for caso disso, a Comissão partilha o relatório com o alto representante.

Justificação

Clarificação do âmbito de aplicação com a inclusão das entidades infranacionais.

II. **RECOMENDAÇÕES POLÍTICAS**

POSIÇÃO DO COMITÉ DAS REGIÕES EUROPEU

O Comité das Regiões Europeu (CR) acolhe favoravelmente a proposta de regulamento da Comissão, que visa reforçar a solidariedade europeia em matéria de cibersegurança. Atualmente, os Estados-Membros da União Europeia (UE) estão estreitamente conectados e digitalmente interligados, o que só aumentará nos próximos anos. Por conseguinte, o Comité congratula-se com a iniciativa da Comissão de abordar conjuntamente as ciberameaças geradas pela crescente digitalização. A proposta aborda o número crescente de ciberincidentes — nomeadamente nos domínios de competência dos municípios e das regiões — e destaca a importância da preparação para os incidentes em domínios críticos da sociedade, de lhes dar resposta e de aprender com os mesmos. O CR considera que as propostas da Comissão podem contribuir para aumentar a resiliência digital na União.

O COMITÉ DAS REGIÕES EUROPEU

1. estima que, para alcançar o objetivo de uma Europa resiliente do ponto de vista digital, é essencial que tanto os representantes políticos como os cidadãos reconheçam a importância de se mobilizarem em torno da cibersegurança; insta, portanto, os Estados-Membros, a Comissão e todos os órgãos de poder local a agirem em conjunto para sensibilizar para a necessidade de ações, nomeadamente de aumentar os investimentos em resiliência digital, em particular nos níveis local e regional, e de ponderar o desenvolvimento de instrumentos de proteção contra ataques de *software* de sequestro. Tal requererá medidas adequadas no domínio financeiro, técnico e de melhoria de competências;

2. observa que a proposta faz referência e se baseia na Diretiva SRI 2 em muitos aspetos. Na transposição para o nível nacional da Diretiva SRI 2, cada Estado-Membro determina se os órgãos de poder local são abrangidos pelo âmbito de aplicação da diretiva ([2]). Uma vez que cada Estado-Membro pode decidir se os municípios são definidos como entidades essenciais ou importantes na aplicação da Diretiva SRI 2, serão as diferenças entre países a determinar a abordagem de cada país em relação ao Regulamento Cibersolidariedade tal como agora proposto. A fim de evitar que os órgãos de poder local responsáveis por serviços essenciais de alguns Estados-Membros sejam excluídos do âmbito de aplicação do Regulamento Cibersolidariedade, o texto jurídico deve determinar claramente que aqueles devem ser considerados abrangidos, independentemente de estarem ou não abrangidos pela Diretiva SRI 2;

3. assinala que, na medida em que a cibersegurança é um pilar da interoperabilidade digital, é imperativo que os esforços para reforçar a interoperabilidade entre regiões sejam apoiados por medidas de cibersegurança sólidas, a fim de assegurar que as ciberameaças não prejudicam a interoperabilidade das regiões em toda a Europa;

4. tem para si que os municípios e as regiões necessitam do apoio concreto das estruturas que vão ser criadas, e não devem ter apenas a obrigação de lhes comunicar informações; solicita, por conseguinte, uma maior clareza sobre a forma como este apoio será prestado às regiões, nomeadamente para aumentar o nível de cibersegurança nos municípios de pequena dimensão;

Observações sobre os domínios de ação da proposta

O ciberescudo europeu

Implantação de uma infraestrutura pan-europeia de centros de operações de segurança (SOC) para criar e reforçar capacidades comuns de deteção, análise e tratamento de dados sobre ciberameaças e ciberincidentes.

5. nota que, a fim de obter uma visão global do estado atual da cibersegurança na UE, é necessário agregar informações, avaliações de risco, ameaças e incidentes, também dos fornecedores de sistemas locais e nacionais; considera problemático que não existam incentivos e processos claros para a forma como os municípios e as regiões podem contribuir ativamente para reforçar a resiliência digital. A participação do nível local e regional é fundamental, uma vez que possui soluções digitais que estão expostas a ataques. Por conseguinte, é importante criar um enquadramento em que os municípios e as regiões possam e devam participar enquanto parceiros nos esforços para aumentar a cibersegurança da União;

6. assinala que uma série de estudos constaram que existem grandes diferenças no grau de maturidade entre os países no que diz respeito às medidas de proteção e de segurança adotadas. Mesmo no interior de cada país há diferenças significativas entre, por exemplo, os poderes públicos nacionais e os órgãos de poder local, de menor dimensão, tanto no que diz respeito às capacidades como aos objetivos de cibersegurança; considera, por isso, importante que o regulamento contribua para reduzir estas diferenças e assegurar que todas as partes interessadas tenham capacidades e objetivos relativamente equivalentes;

7. observa que se corre o risco de as tarefas da nova rede de SOC nacionais e transfronteiriços se sobreporem às da rede de equipas de resposta a incidentes de segurança informática (CSIRT) ([3]). Quando se criarem centros de segurança nacionais juntamente com as CSIRT, é importante definir claramente o funcionamento da cooperação e as responsabilidades do SOC nacional e das CSIRT em caso de incidente;

([2]) Artigo 2.º, n.º 5, da Diretiva SRI 2: «Os Estados-Membros podem prever que a presente diretiva se aplique [às] entidades da administração pública a nível local.»

([3]) Segundo o artigo 11.º, n.º 3, da Diretiva SRI 2, as «funções das CSIRT são as seguintes:
a) Monitorizar e analisar ciberameaças, vulnerabilidades e incidentes a nível nacional e, mediante pedido, prestar assistência a entidades essenciais e importantes em causa relativamente à monitorização em tempo real ou quase real dos seus sistemas de rede e informação;
b) Ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às entidades essenciais e importantes, bem como a autoridades competentes e a outras partes interessadas, sobre ciberameaças, vulnerabilidades e incidentes, se possível em tempo quase real;
c) Intervir em caso de incidentes e prestar assistência às entidades essenciais e importantes envolvidas, se aplicável;
d) Recolher e analisar dados forenses, proceder à análise dinâmica dos riscos e dos incidentes e desenvolver o conhecimento situacional em matéria de cibersegurança;
e) Realizar, a pedido de uma entidade essencial ou importante, uma análise proativa dos sistemas de rede e informação da entidade em causa, a fim de detetar vulnerabilidades com um potencial impacto significativo;
f) Participar na rede de CSIRT e prestar assistência mútua, em conformidade com as suas capacidades e competências, a outros membros da rede de CSIRT, a pedido destes;
g) Se aplicável, atuar como coordenador para efeitos do processo de divulgação coordenada de vulnerabilidades a que se refere o artigo 12.º, n.º 1;
h) Contribuir para a implantação de ferramentas seguras de partilha de informações nos termos do artigo 10.º, n.º 3».

8. congratula-se com os objetivos específicos da proposta de regulamento e com as medidas propostas; lamenta, ao mesmo tempo, que, apesar do aumento dos ciberataques, os órgãos de poder local e regional não sejam suficientemente abrangidos pela proposta em apreço e, por conseguinte, propõe uma série de alterações legislativas para colmatar tais lacunas;

9. estima que, atualmente, faltam dados e pontos de medição claros sobre os incidentes, ameaças e riscos para os municípios e as regiões. No âmbito do ciberescudo europeu, devem ser desenvolvidos indicadores para avaliar o eventual aumento do desenvolvimento e do grau de maturidade no contexto da aplicação do regulamento. A longo prazo, os indicadores podem contribuir para um mapa de riscos assente em dados, mostrando onde são necessárias mais medidas;

Mecanismo de ciberemergência

O objetivo é reforçar a preparação, testar o grau de preparação dos setores considerados críticos, reforçar as capacidades de recuperação de incidentes e criar uma reserva de cibersegurança.

10. chama a atenção para o facto de os incidentes em grande escala poderem resultar de acontecimentos locais e que a proposta deve indicar de que forma os SOC e a Reserva de Cibersegurança podem detetar perturbações locais graves, e não apenas incidentes significativos e em grande escala que já tenham ocorrido. A partilha de informações não se deve limitar a incidentes em grande escala, mas antes incluir igualmente os riscos potenciais;

11. assinala que as informações relacionadas com incidentes de cibersegurança são, na sua maioria, altamente sensíveis, podendo conter pormenores técnicos ou mesmo dados pessoais, que atualmente não podem ser partilhados sem contratos e acordos entre as partes. Presentemente, existem dificuldades na partilha de informações a nível nacional, pelo que a questão da partilha transfronteiriça é muito complexa. Para que o mecanismo de ciberemergência funcione, a Comissão deve assegurar que todas as partes interessadas, públicas e privadas, no âmbito da Reserva de Cibersegurança da UE cumprem as condições jurídicas e técnicas necessárias para partilhar e receber informações; considera que a divulgação de informações é especialmente necessária para a resolução de incidentes, ou seja, qual é a melhor forma de as entidades afetadas lidarem com um incidente grave;

12. congratula-se com o elevado nível de requisitos impostos aos prestadores de serviços do setor privado que participam na Reserva de Cibersegurança proposta. No entanto, a formulação destes requisitos não deve resultar na exclusão de determinadas competências ou conhecimentos do sistema, uma vez que apenas alguns operadores de muito grande dimensão são capazes de satisfazer os requisitos impostos aos prestadores de soluções de segurança. A UE deve abarcar uma ampla gama de atividades de segurança para ser tão resiliente quanto possível;

13. nota que, segundo a proposta de regulamento, a Reserva de Cibersegurança consistirá numa lista de serviços prestados por prestadores de confiança, que devem ser certificados em conformidade com o Regulamento Cibersegurança ([4]). A Agência da União Europeia para a Cibersegurança (ENISA) é responsável por assegurar que os produtos e serviços cumprem os requisitos de cibersegurança estipulados; salienta a importância de a ENISA criar rapidamente sistemas de certificação para que os prestadores se possam certificar com base em tecnologias modernas ([5]);

14. considera que, quando da criação da Reserva de Cibersegurança, é importante que não se criem obstáculos à concorrência ou se excluam intervenientes que operam apenas em partes da União. A criação da Reserva de Cibersegurança e a certificação requerem procedimentos rápidos e claros para determinar os intervenientes mais competentes e pertinentes neste contexto;

([4]) 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).

([5]) A ENISA está a desenvolver três sistemas de certificação, que ainda não estão concluídos, designadamente para TIC, 5G e computação em nuvem (https://www.enisa.europa.eu/topics/standards/certification/eu-cybersecurity-certification-faq).

15. considera que se deve identificar os fornecedores nacionais de tecnologias e serviços para sistemas críticos e registá-los numa base de dados. Tais dados podem ser muito valiosos no contexto de medidas que exijam a mobilização dos intervenientes locais. Podem também ser utilizados no contexto do trabalho da Academia de Competências de Cibersegurança;

16. sublinha que, em caso de incidente, o impacto da resposta depende da rapidez das medidas adotadas. As informações complexas partilhadas sobre incidentes e riscos deve chegar aos grupos-alvo adequados num curto espaço de tempo. A proposta tem por objetivo criar uma nova organização e estrutura para a partilha de informações; salienta, no entanto, a necessidade de utilizar e aperfeiçoar os canais de informação existentes, como a UE-CyCLONe ([6]) e a rede de CSIRT, aquando da criação de centros de segurança nacionais e transfronteiriços;

Mecanismo de análise de incidentes de cibersegurança

Uma função de análise de incidentes de cibersegurança, especificamente dos incidentes com impacto significativo.

17. sublinha que a necessidade de capacidades no domínio da cibersegurança e do seu financiamento se explica pelo forte desenvolvimento da digitalização; congratula-se com a criação pela Comissão de uma Academia de Competências de Cibersegurança e defende uma estratégia clara para reforçar especificamente os municípios e as regiões de menor dimensão e com menos recursos, dada a escassez de competências na UE;

18. sublinha que uma forte resiliência digital exige a cooperação de diferentes intervenientes, contribuindo as entidades públicas e privadas com conhecimentos especializados, experiência e recursos humanos; destaca o papel dos órgãos de poder local e regional no reforço da resiliência digital, uma vez que podem apoiar-se mutuamente através de campanhas de sensibilização, do intercâmbio de exemplos de boas práticas e de conhecimentos especializados; salienta que, quanto mais as empresas investirem na sua resiliência digital, maior será o custo dos ataques para os seus opositores, o que pode também servir de elemento dissuasor;

19. observa que, hoje em dia, os municípios e as regiões da Europa suportam os custos para manter um elevado nível de cibersegurança, bem como os custos decorrentes de incidentes; considera que existe o risco de o regulamento exercer uma pressão adicional sobre recursos que já são escassos. Por conseguinte, o regulamento não deve criar encargos, mas antes reforçar a capacidade de todas as entidades através de instrumentos, métodos e apoio concretos;

20. interroga-se sobre a razão pela qual os relatórios de auditoria não podem ser partilhados no âmbito da rede de SOC nacionais e transfronteiriços. Segundo a proposta, os centros de segurança nacionais só podem aceder a informação pública. As lições aprendidas com os incidentes são essenciais para que os intervenientes possam melhorar e desenvolver a sua cibersegurança. Por conseguinte, as informações detalhadas devem ser disponibilizadas a todos os participantes na rede;

21. estima que a proposta descreve o financiamento de forma demasiado geral; solicita uma descrição muito mais detalhada da forma como os fundos serão utilizados e qual a percentagem que será diretamente afetada às regiões e aos municípios;

([6]) Artigo 16.º, n.os 1 e 3, da Diretiva SRI 2:
Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe)
1. «É criada a UE-CyCLONe para apoiar a gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível operacional e para assegurar o intercâmbio regular de informações pertinentes entre os Estados-Membros e as instituições, órgãos e organismos da União.
3. As funções da UE-CyCLONe são as seguintes:
   a) Aumentar o nível de preparação para a gestão de crises e de incidentes de cibersegurança em grande escala;
   b) Desenvolver um conhecimento situacional comum relativo a crises e incidentes de cibersegurança em grande escala;
   c) Avaliar as consequências e o impacto de crises e incidentes de cibersegurança em grande escala relevantes e propor eventuais medidas de atenuação;
   d) Coordenar a gestão de crises e de incidentes de cibersegurança em grande escala e apoiar a tomada de decisões a nível político em relação a tais incidentes e crises;
   e) Discutir, a pedido do Estado-Membro em causa, os planos nacionais de resposta a crises e incidentes de cibersegurança em grande escala a que se refere o artigo 9.º, n.º 4.»

22. sublinha, por último, que a proposta é consentânea com os princípios da subsidiariedade e da proporcionalidade.

Bruxelas, 30 de novembro de 2023.

O Presidente
do Comité das Regiões Europeu

Vasco ALVES CORDEIRO