Conselho da
União Europeia

Bruxelas, 7 de setembro de 2023
(OR. en)

12485/23

Dossiê interinstitucional:
2023/0318(NLE)

PROCIV 57	**ATO 48**
ENV 925	**CSC 408**
JAI 1084	**ECOFIN 839**
SAN 494	**CSCI 149**
COSI 140	**DATAPROTECT 216**
CHIMIE 85	**MI 698**
ENFOPOL 356	**CODEC 1500**
RECH 380	**COPS 418**
CT 133	**JAIEX 46**
DENLEG 38	**COPEN 292**
COTER 153	**IND 441**
RELEX 987	**POLMIL 221**
ENER 467	**IPCR 55**
HYBRID 53	**DIGIT 160**
TRANS 329	**DISINFO 62**
CYBER 203	**CSDP/PSDC 608**
TELECOM 251	**MARE 18**
ESPACE 45	**POLMAR 47**

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	6 de setembro de 2023
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2023) 526 final
Assunto:	Proposta de RECOMENDAÇÃO DO CONSELHO sobre um plano de ação para a coordenação da resposta a nível da UE a perturbações em infraestruturas críticas com importante relevância transfronteiriça

Envia-se em anexo, à atenção das delegações, o documento COM(2023) 526 final.

Anexo: COM(2023) 526 final

COMISSÃO
EUROPEIA

Bruxelas, 6.9.2023
COM(2023) 526 final

2023/0318 (NLE)

Proposta de

RECOMENDAÇÃO DO CONSELHO

sobre um plano de ação para a coordenação da resposta a nível da UE a perturbações em infraestruturas críticas com importante relevância transfronteiriça

(Texto relevante para efeitos do EEE)

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Razões e objetivos da proposta

No atual contexto geopolítico, caracterizado por uma instabilidade crescente, nomeadamente devido à guerra de agressão da Rússia contra a Ucrânia e à maior complexidade das ameaças à segurança, bem como pelos efeitos das alterações climáticas, como o aumento de fenómenos climáticos invulgares ou a escassez de água, a União tem de permanecer vigilante e adaptar-se constantemente. Os cidadãos, as empresas e as autoridades da União dependem de infraestruturas críticas[1] devido aos serviços essenciais prestados pelas entidades que as exploram. Estes serviços são indispensáveis à manutenção de funções societais ou atividades económicas vitais, da saúde e segurança pública ou do ambiente e têm de ser prestados sem entraves no mercado interno. Por conseguinte, dada a importância destes serviços essenciais para o mercado interno e, consequentemente, a necessidade de tornar as infraestruturas críticas mais resilientes e, de um modo mais geral, de assegurar a resiliência das entidades críticas que prestam esses serviços, a União tem de tomar medidas para reforçar essa resiliência e atenuar quaisquer perturbações na prestação destes serviços essenciais. Se não o fizer, tais perturbações podem ter consequências graves para os cidadãos da União, as nossas economias e a confiança nos nossos sistemas democráticos, podendo ainda afetar o bom funcionamento do mercado interno, em especial num contexto de interdependências crescentes entre setores e além-fronteiras.

A União já tomou uma série de medidas destinadas a reforçar a proteção das infraestruturas críticas, nomeadamente no que respeita a infraestruturas transfronteiriças, bem como a resiliência das entidades críticas, a fim de evitar ou atenuar os efeitos de perturbações nos serviços essenciais que estas prestam no mercado interno.

A Diretiva 2008/114/CE relativa à identificação e designação das infraestruturas críticas europeias[2] (Diretiva ICE) foi o primeiro instrumento jurídico a estabelecer um procedimento à escala da UE para identificar e designar as infraestruturas críticas europeias e uma abordagem comum da União para avaliar a necessidade de melhorar a proteção dessas infraestruturas contra ameaças humanas – intencionais e acidentais – bem como catástrofes naturais. No entanto, concentrou-se apenas nos setores da energia e dos transportes e na proteção das infraestruturas críticas e não previu medidas mais alargadas para reforçar a resiliência das entidades que exploram essas infraestruturas.

Devido à natureza cada vez mais interligada e transfronteiriça das operações no mercado interno, impunha-se abranger mais do que dois setores e ir além das medidas de proteção de ativos individuais. Foi por esta razão que, em 2022, foi adotada a Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas[3] (Diretiva REC), juntamente com a Diretiva (UE) 2022/2555 relativa a medidas destinadas a garantir um elevado nível comum de

---

[1] Entende-se por «infraestrutura crítica», um ativo, uma instalação, um equipamento, uma rede ou um sistema, no seu todo ou uma parte de um ativo, uma instalação, um equipamento, uma rede ou um sistema, que seja necessário para a prestação de um serviço essencial [artigo 2.º, n.º 4, da Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas].

[2] Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75).

[3] Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho (JO L 333 de 27.12.2022, p. 164).

cibersegurança na União[4] (Diretiva SRI 2). O objetivo é assegurar um nível abrangente de resiliência física e digital das entidades críticas. A Diretiva REC entrou em vigor em 16 de janeiro de 2023 e visa ajudar os Estados-Membros a reforçar a resiliência global das entidades críticas, aumentando simultaneamente a coordenação a nível da União. Substituirá a Diretiva ICE a partir de 18 de outubro de 2024, data até à qual os Estados-Membros terão de tomar as medidas necessárias para dar cumprimento à Diretiva REC. A Diretiva REC é aplicável a 11 setores[5]. Transfere a tónica da proteção das infraestruturas críticas para o conceito mais amplo de resiliência das entidades críticas que exploram essas infraestruturas críticas, abrangendo o antes, o durante e o depois de um incidente. A Diretiva SRI 2 também entrou em vigor em 16 de janeiro de 2023 e moderniza o quadro jurídico em vigor para se adaptar a uma digitalização crescente e à evolução do panorama das ameaças à cibersegurança. A Diretiva SRI 2 também alarga o âmbito de aplicação das regras em matéria de cibersegurança a novos setores e entidades e melhora a resiliência e as capacidades de resposta a incidentes das entidades públicas e privadas, das autoridades competentes e da União no seu conjunto.

A Diretiva REC inclui disposições relativas à notificação de incidentes pela entidade crítica à autoridade nacional competente, à notificação de outros Estados-Membros (potencialmente) afetados pela autoridade nacional competente e à notificação da Comissão no caso de o incidente afetar seis ou mais Estados-Membros. A Diretiva REC estipula determinadas obrigações de notificação de incidentes no caso de o incidente ter ou poder ter um impacto significativo nas entidades críticas e na continuidade da prestação de serviços essenciais para ou em um ou mais Estados-Membros[6].

Conforme ilustrado pela sabotagem dos gasodutos Nord Stream em setembro de 2022, o contexto de segurança em que as infraestruturas críticas operam mudou significativamente e são necessárias medidas urgentes adicionais a nível da União a fim de reforçar a resiliência das infraestruturas críticas, não só no que respeita à preparação, mas também a uma resposta coordenada.

Neste contexto, foi adotada, em 8 de dezembro de 2022, na sequência de uma proposta da Comissão, uma recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas[7] (Recomendação sobre a resiliência das infraestruturas críticas). A referida recomendação salienta, nomeadamente, a necessidade de assegurar, a nível da União, uma resposta coordenada e eficaz aos riscos atuais e futuros que se colocam à prestação de serviços essenciais. Mais especificamente, o Conselho convidou a Comissão a elaborar «um plano de resposta coordenada a perturbações das infraestruturas críticas com importante relevância transfronteiriça». A recomendação refere que o plano deve ser coerente com o Protocolo da UE para a luta contra as ameaças híbridas[8], ter em conta a Recomendação 2017/1584 da Comissão sobre a resposta coordenada

---

4 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 (JO L 333 de 27.12.2022, p. 80).

5 Setores da energia, dos transportes, dos serviços bancários, das infraestruturas do mercado financeiro, das infraestruturas digitais, da administração pública, espacial, da saúde, da água potável, das águas residuais, da produção, transformação e distribuição de produtos alimentares.

6 Em conformidade com o artigo 15.º, n.os 1 e 3, da Diretiva REC.

7 Recomendação do Conselho, de 8 de dezembro de 2022, relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas (2023/C 20/01) (JO C 20 de 20.1.2023, p. 1).

8 Documento de trabalho conjunto dos serviços da Comissão - *EU Protocol for countering hybrid threats* , SWD(2023) 116 final.

a incidentes e crises de cibersegurança em grande escala[9] [Plano de Ação para a Cibersegurança («Cyber Blueprint»)] e respeitar o Mecanismo Integrado de Resposta Política a Situações de Crise[10] (IPCR).

Neste contexto, a presente proposta dá seguimento ao convite do Conselho constante da recomendação no sentido de elaborar um plano de ação. A proposta visa complementar o atual quadro jurídico descrevendo a resposta coordenada a nível da União no que se refere a perturbações em infraestruturas críticas com importante relevância transfronteiriça, utilizando simultaneamente os mecanismos existentes a nível da União. Concretamente, a proposta descreve o âmbito de aplicação, os objetivos, os intervenientes, os processos e os instrumentos existentes que poderão ser utilizados para responder, de forma coordenada a nível da União, a um incidente perturbador em infraestruturas críticas com um efeito transfronteiriço significativo e para apresentar as modalidades de cooperação entre os Estados-Membros, as instituições, órgãos e organismos da União nessas situações.

- **Coerência com as disposições existentes da mesma política setorial**

A presente proposta de recomendação do Conselho está em consonância e complementa o atual quadro jurídico relativo à proteção das infraestruturas críticas e à resiliência das entidades críticas - a Diretiva ICE e a Diretiva REC, respetivamente, bem como a Recomendação sobre a resiliência das infraestruturas críticas -, uma vez que visa assegurar, de forma complementar, a coordenação entre os Estados-Membros e entre estes e as instituições, órgãos e organismos da União na resposta a incidentes que causam perturbações em infraestruturas críticas com importante relevância transfronteiriça e na prestação de serviços essenciais. A proposta utiliza as estruturas e mecanismos existentes a nível da União, incluindo os estabelecidos pela Diretiva REC, nomeadamente a cooperação entre as autoridades competentes e o Grupo para a Resiliência das Entidades Críticas, um grupo criado pela Diretiva REC para apoiar a Comissão e facilitar a cooperação entre os Estados-Membros e o intercâmbio de informações sobre questões relacionadas com a Diretiva REC.

A presente proposta de recomendação do Conselho está igualmente em consonância com o quadro da União em matéria de cibersegurança, tal como estabelecido na Diretiva SRI 2, e é complementar do mesmo.

A atual proposta visa apresentar, no domínio da resiliência das entidades críticas e da proteção das infraestruturas críticas, um Plano de Ação para as Infraestruturas Críticas semelhante ao Plano de Ação para a Cibersegurança.

A parte I, ponto 4, alínea b), do anexo também explica as interligações com o Plano de Ação para a Cibersegurança, que se aplica a incidentes de cibersegurança de grande escala que causem perturbações demasiado extensas para que um Estado-Membro seja capaz de as resolver sozinho ou que afetem dois ou mais Estados-Membros ou instituições da UE, causando um impacto de tão grande alcance e com repercussões a nível técnico e político que exija uma coordenação e uma resposta a nível político da União. Um incidente é definido na Diretiva SRI 2 como «um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por sistemas de rede e informação ou acessíveis por intermédio destes» (incidente de cibersegurança).

---

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

[10] Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (JO L 320 de 17.12.2018, p. 28).

As autoridades competentes ao abrigo da Diretiva REC e da Diretiva SRI 2 têm a obrigação de cooperar e trocar informações sobre incidentes de cibersegurança e incidentes que afetem entidades críticas, nomeadamente no que respeita às medidas tomadas. Numa situação em que um incidente significativo em infraestruturas críticas e um incidente de cibersegurança de grande escala afetem a mesma entidade, deve haver coordenação das possíveis respostas entre os intervenientes relevantes.

A proposta é coerente com o Protocolo da UE para a luta contra as ameaças híbridas, sendo este último aplicável em caso de incidentes híbridos. A parte I, ponto 4, alínea a), do anexo explica as interligações com o Protocolo da UE, nomeadamente qual o instrumento aplicável no caso de um incidente significativo em infraestruturas críticas com uma dimensão híbrida.

A proposta é igualmente coerente com outros mecanismos de gestão de crises existentes a nível da União, tais como o mecanismo IPCR do Conselho, o processo interno de coordenação de crises da Comissão ARGUS[11] e o Mecanismo de Proteção Civil da União Europeia[12] (MPCUE), apoiado pelo seu Centro de Coordenação de Resposta de Emergência (CCRE), e o Mecanismo de Resposta a Situações de Crise do Serviço Europeu para a Ação Externa.

A proposta é igualmente coerente com outra legislação setorial pertinente e, nomeadamente, com medidas específicas nela contidas que regulam determinados aspetos da resposta a perturbações por parte de entidades que operam nos setores em causa.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

A proposta baseia-se no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE),que se prende com a aproximação das legislações destinadas a melhorar o mercado interno, juntamente com o artigo 292.º do TFUE, que estabelece as regras para a adoção de recomendações.

A escolha do artigo 114.º do TFUE como base jurídica substantiva justifica-se pelo facto de a recomendação do Conselho proposta visar assegurar uma resposta coordenada em caso de perturbações em infraestruturas críticas com importante relevância transfronteiriça. Tais perturbações afetam vários Estados-Membros e correm o risco de ter um impacto no funcionamento do mercado interno devido às crescentes interdependências entre infraestruturas e setores numa economia da União cada vez mais interdependente. Uma melhor resposta às perturbações evitará, por sua vez, perturbações no funcionamento do mercado interno, uma vez que essas infraestruturas críticas e os serviços essenciais que prestam são indispensáveis à manutenção de funções societais ou atividades económicas vitais, da saúde e segurança pública ou do ambiente.

A proposta complementará as Diretivas ICE e REC, que também se baseiam no artigo 114.º do TFUE. Tal como a recomendação agora proposta, a Recomendação sobre a resiliência das infraestruturas críticas tem igualmente por base os artigos 114.º e 292.º do TFUE.

---

[11] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Disposições da Comissão que criam o sistema geral de alerta rápido «ARGUS», COM(2005) 662 final.

[12] Regulamento (UE) 2021/836 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que altera que altera a Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 185 de 26.5.2021, p. 1).

- **Subsidiariedade (no caso de competência não exclusiva)**

Embora a resposta a perturbações em infraestruturas críticas ou nos serviços prestados pelas entidades críticas que exploram essas infraestruturas críticas seja, sobretudo, da responsabilidade dos Estados-Membros, a União desempenha um papel importante em caso de perturbações em infraestruturas críticas com importante relevância transfronteiriça, uma vez que essas perturbações podem afetar vários ou mesmo todos os setores da atividade económica no mercado único, a segurança e as relações internacionais da União. Com o objetivo de garantir o funcionamento do mercado interno, a coordenação, a nível da União, em caso de perturbações em infraestruturas críticas com um efeito transfronteiriço significativo não só é adequada como também necessária, uma vez que essa resposta coordenada a nível da União apoiará a resposta dos Estados-Membros à perturbação através de um conhecimento partilhado da situação, de uma comunicação pública coordenada e da atenuação das consequências da perturbação no mercado interno.

- **Proporcionalidade**

A presente proposta está em conformidade com o princípio da proporcionalidade, tal como previsto no artigo 5.º, n.º 4, do Tratado da União Europeia.

Nem o conteúdo nem a forma da presente proposta de recomendação do Conselho excedem o necessário para alcançar os seus objetivos. As ações propostas são proporcionais aos objetivos visados, que se centram em assegurar uma resposta coordenada a nível da União em caso de perturbações em infraestruturas críticas ou nos serviços prestados pelas entidades críticas que exploram essas infraestruturas críticas e que tenham uma importante relevância transfronteiriça. Esta proposta no sentido de uma resposta coordenada é proporcional às prerrogativas e obrigações dos Estados-Membros ao abrigo do direito nacional. Muitas vezes, os incidentes que perturbam infraestruturas críticas ou a prestação de serviços essenciais por parte de entidades críticas não atingem o limiar de um incidente significativo em infraestruturas críticas e podem ser objeto de uma resposta eficaz a nível nacional. Por conseguinte, a utilização do mecanismo previsto na presente proposta limita-se a perturbações graves que tenham uma importante relevância transfronteiriça e afetem vários Estados-Membros.

- **Escolha do instrumento**

A fim de alcançar os objetivos acima referidos, o TFUE prevê a adoção pelo Conselho de recomendações, nomeadamente no seu artigo 292.º, com base numa proposta da Comissão. Nos termos do artigo 288.º do TFUE, as recomendações não são vinculativas. Uma recomendação do Conselho é um instrumento adequado neste caso, uma vez que indica o compromisso dos Estados-Membros relativamente às medidas nela incluídas e proporciona uma base sólida para a cooperação no domínio da resposta coordenada em caso de perturbações significativas em infraestruturas críticas. Desta forma, a recomendação proposta complementará o quadro jurídico vinculativo (em especial, a Diretiva REC) e também a Recomendação sobre a resiliência das infraestruturas críticas anteriormente adotada, que insta à adoção dessas medidas complementares, respeitando simultaneamente na íntegra as responsabilidades dos Estados-Membros no domínio em causa.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- **Consultas das partes interessadas**

Na elaboração da presente proposta, foram consultados os Estados-Membros, bem como instituições e agências da União. Além disso, foram tidas em consideração as opiniões dos peritos dos Estados-Membros expressas no seminário de 24 de abril de 2023 e enviadas por escrito após esse seminário.

Verificou-se um consenso geral quanto à utilidade de uma maior coordenação na resposta, a nível da União, a perturbações em infraestruturas críticas com importante relevância transfronteiriça no atual contexto de ameaças, respeitando simultaneamente a competência dos Estados-Membros neste domínio e a confidencialidade das informações sensíveis. Verificou-se igualmente consenso quanto à necessidade de evitar a duplicação de instrumentos e de tirar partido dos mecanismos existentes a nível da União para a coordenação, a partilha de informações e a resposta.

Embora alguns Estados-Membros tivessem uma opinião favorável ao âmbito mais alargado do Plano de Ação para as Infraestruturas Críticas, outros consideraram que o limiar de seis ou mais Estados-Membros previsto na Diretiva REC no que se refere à identificação de entidades críticas de especial relevância europeia era suficiente e não se justificava incluir um segundo tipo de incidente no âmbito de aplicação. Alguns Estados-Membros observaram a importância de envolver, se for o caso, os operadores de infraestruturas críticas que prestam serviços essenciais, devido aos seus conhecimentos especializados e à importância de ter em conta a dimensão cibernética.

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

A proposta de recomendação do Conselho é constituída por uma parte principal e um anexo.

A parte principal é composta por 11 pontos, da seguinte forma:

O ponto 1 estabelece a necessidade de uma cooperação reforçada no que diz respeito à resposta a incidentes significativos em infraestruturas críticas, em conformidade com o plano de ação para as infraestruturas críticas constante da presente proposta de recomendação, incluindo as partes pertinentes do respetivo anexo.

O ponto 2 explica o âmbito de aplicação do Plano de Ação para as Infraestruturas Críticas, que se refere a dois tipos de situações de incidentes perturbadores que desencadeiam o recurso ao referido plano: o incidente tem um efeito perturbador significativo na prestação de serviços essenciais a, ou em, seis ou mais Estados-Membros; ou tem um efeito perturbador significativo em dois ou mais Estados-Membros e existe acordo entre os intervenientes relevantes nele mencionados quanto à necessidade de coordenação a nível da União devido ao impacto significativo do incidente.

O ponto 3 refere-se à identificação dos intervenientes relevantes que deverão participar no Plano de Ação para as Infraestruturas Críticas e aos níveis em que esse plano funcionará (operacional, estratégico/político). Estes aspetos são explicados mais em pormenor no anexo da recomendação.

O ponto 4 recomenda a aplicação do Plano de Ação para as Infraestruturas Críticas em coerência com outros instrumentos mencionados no anexo.

O ponto 5 recomenda aos Estados-Membros que respondam eficazmente, a nível nacional, a perturbações significativas em infraestruturas críticas.

O ponto 6 recomenda a criação ou designação de pontos de contacto pelos intervenientes relevantes que devem apoiar a utilização do Plano de Ação para as Infraestruturas Críticas. Sempre que possível, estes pontos de contacto devem ser os mesmos que os pontos de contacto únicos previstos na Diretiva REC.

O ponto 7 refere-se ao fluxo de informações em caso de incidente significativo em infraestruturas críticas.

O ponto 8 explica de que forma se deve proceder ao intercâmbio de informações.

O ponto 9 recomenda que se teste o funcionamento do Plano de Ação para as Infraestruturas Críticas através de exercícios.

O ponto 10 recomenda que os ensinamentos identificados sejam debatidos no Grupo para a Resiliência das Entidades Críticas, que deve elaborar um relatório, incluindo recomendações, que será adotado pela Comissão.

O ponto 11 recomenda aos Estados-Membros que debatam o relatório no Conselho.

O anexo descreve os objetivos, os princípios, os principais intervenientes, a interação com os mecanismos de resposta a situações de crise existentes e o funcionamento do Plano de Ação para as Infraestruturas Críticas, com as suas duas modalidades de cooperação: o intercâmbio de informações e a resposta.

2023/0318 (NLE)

Proposta de

RECOMENDAÇÃO DO CONSELHO

sobre um plano de ação para a coordenação da resposta a nível da UE a perturbações em infraestruturas críticas com importante relevância transfronteiriça

(Texto relevante para efeitos do EEE)

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente os artigos 114.º e 292.º,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

(1) É fundamental para o bom funcionamento do mercado interno e da sociedade no seu conjunto contar com infraestruturas críticas resilientes e entidades críticas resilientes que prestam serviços indispensáveis à manutenção de funções societais ou atividades económicas vitais, da saúde e segurança pública ou do ambiente.

(2) No atual panorama de riscos em evolução e à luz das crescentes interdependências entre infraestruturas e setores e, de um modo mais geral, das interligações entre setores e fronteiras, impõe-se garantir e reforçar, de forma abrangente e coordenada, a proteção das infraestruturas críticas e a resiliência das entidades críticas que exploram essas infraestruturas.

(3) Um incidente que perturbe infraestruturas críticas e, por conseguinte, incapacite ou dificulte gravemente a prestação de serviços essenciais pode ter efeitos transfronteiriços significativos, bem como um impacto negativo no mercado interno. A fim de assegurar uma abordagem orientada, proporcionada e eficaz, devem ser tomadas medidas para fazer face, em especial, a incidentes significativos em infraestruturas críticas, tal como especificado na presente recomendação, que abranjam, por exemplo, situações em que a perturbação causada pelo incidente é de longa duração ou pode ter efeitos em cascata consideráveis no mesmo setor ou noutros setores ou Estados-Membros.

(4) É essencial uma resposta coordenada a incidentes significativos em infraestruturas críticas para evitar perturbações graves no mercado interno e assegurar o restabelecimento da prestação desses serviços essenciais o mais rapidamente possível, uma vez que tais incidentes podem ter consequências graves para a economia e os cidadãos da União. Uma resposta atempada e eficaz a este tipo de incidentes a nível da União exige uma cooperação célere e eficaz entre todos os intervenientes relevantes e uma ação coordenada, apoiada a nível da União. Esta resposta depende, por conseguinte, da existência de procedimentos e mecanismos de cooperação previamente estabelecidos e, na medida do possível, bem ensaiados, com a definição

das funções e responsabilidades específicas dos principais intervenientes a nível nacional e da União.

(5) Embora a responsabilidade principal de assegurar a resposta a incidentes significativos em infraestruturas críticas incumba aos Estados-Membros e às entidades que exploram infraestruturas críticas e prestam serviços essenciais, justifica-se uma maior coordenação a nível da União em caso de perturbações com importante relevância transfronteiriça. Uma resposta atempada e eficaz depende não só da implantação de mecanismos nacionais pelos Estados-Membros, mas também de uma ação coordenada apoiada a nível da União, nomeadamente uma cooperação efetiva, conduzida de forma célere e eficaz.

(6) A proteção das infraestruturas críticas europeias é atualmente regulada pela Diretiva 2008/114/CE do Conselho[1], que abrange apenas dois setores, os transportes e a energia. A referida diretiva estabelece um procedimento de identificação e designação das infraestruturas críticas europeias e uma abordagem comum para a avaliação da necessidade de melhorar a proteção de tais infraestruturas. Constitui o pilar central do Programa Europeu de Proteção das Infraestruturas Críticas[2] (PEPIC), adotado pela Comissão em 2006, que definiu um enquadramento europeu baseado numa abordagem de todos os riscos para a proteção das infraestruturas críticas.

(7) A fim de ir além da proteção das infraestruturas críticas e de assegurar, de um modo mais geral, a resiliência das entidades críticas que exploram essas infraestruturas que prestam serviços essenciais no mercado interno, a Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho[3] substituirá a Diretiva 2008/114/CE a partir de 18 de outubro de 2024. A Diretiva (UE) 2022/2557 abrange 11 setores e prevê obrigações de reforço da resiliência para os Estados-Membros e as entidades críticas, a cooperação entre os Estados-Membros e com a Comissão, bem como o apoio da Comissão às autoridades nacionais e entidades críticas e o apoio dos Estados-Membros às entidades críticas.

(8) Na sequência da sabotagem dos gasodutos Nord Stream, é necessário adotar, a nível da União, mais medidas de reforço da resiliência das infraestruturas críticas. Por conseguinte, com base numa proposta da Comissão, o Conselho adotou a Recomendação relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas (Recomendação 2023/C 20/01)[4], que visa o reforço do grau de preparação, a melhoria da resposta e a cooperação internacional neste domínio. A recomendação salienta, nomeadamente, a necessidade de assegurar, a nível da União, uma resposta coordenada e eficaz aos riscos atuais e futuros que se colocam à prestação de serviços essenciais.

(9) Por conseguinte, impõe-se complementar o quadro jurídico em vigor com uma recomendação adicional do Conselho que estabeleça um plano de ação para uma

---

[1] Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75).

[2] COM(2006) 786 final de 12 de dezembro de 2006 — Comunicação da Comissão relativa a um Programa Europeu de Proteção das Infraestruturas Críticas.

[3] Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho (JO L 333 de 27.12.2022, p. 164).

[4] Recomendação do Conselho, de 8 de dezembro de 2022, relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas (2023/C 20/01) (JO C 20 de 20.1.2023, p. 1).

resposta coordenada a perturbações em infraestruturas críticas com importante relevância transfronteiriça (Plano de Ação para as Infraestruturas Críticas), utilizando simultaneamente os mecanismos existentes a nível da União.

(10) A presente recomendação deve ser alinhada com a Recomendação 2023/C 20/01, a fim de assegurar a coerência e evitar duplicações. Por conseguinte, a presente recomendação não deve, enquanto tal, abranger os outros elementos do ciclo de vida da gestão de crises, nomeadamente a prevenção, a preparação e a recuperação.

(11) A presente recomendação deve complementar a Diretiva (UE) 2022/2557, em especial no que se refere à resposta coordenada, e deve ser aplicada assegurando simultaneamente a coerência com a referida diretiva e com quaisquer outras regras aplicáveis do direito da União. Assim sendo, a presente recomendação deve também basear-se e utilizar, na medida do possível, os conceitos, instrumentos e processos da dita diretiva, tais como o Grupo para a Resiliência das Entidades Críticas, atuando dentro dos limites das suas atribuições conforme definidas na diretiva, e os pontos de contacto. Além disso, o conceito de «infraestrutura crítica» utilizado na presente recomendação deve ser entendido da mesma forma que o estabelecido no considerando 7 da Recomendação 2023/C 20/01, ou seja, no sentido de incluir as infraestruturas críticas identificadas por um Estado-Membro a nível nacional ou designadas como infraestruturas críticas europeias nos termos da Diretiva 2008/114/CE, bem como as entidades críticas a identificar nos termos da Diretiva (UE) 2022/2557. A fim de assegurar a coerência com a Diretiva (UE) 2022/2557, os conceitos utilizados na presente recomendação devem, por conseguinte, ser interpretados como tendo o mesmo significado que na referida diretiva. Por exemplo, o conceito de resiliência, conforme definido no artigo 2.º, ponto 2, da referida diretiva, deve também ser entendido como referindo-se à capacidade de uma infraestrutura crítica para prevenir, proteger, reagir, resistir, atenuar, absorver, adaptar ou recuperar em caso de eventos que perturbem significativamente ou tenham potencial para perturbar significativamente a prestação de serviços essenciais no mercado interno, ou seja, serviços indispensáveis à manutenção de funções societais e económicas vitais, da segurança pública, da saúde da população ou do ambiente.

(12) Além disso, o conceito de «efeito perturbador significativo» deve ser entendido à luz dos critérios previstos no artigo 7.º, n.º 1, da Diretiva (UE) 2022/2557, a saber: i) o número de utilizadores que dependem do serviço essencial prestado pela entidade em questão; ii) o grau em que outros setores e subsetores estabelecidos no anexo da diretiva dependem do serviço essencial em questão; iii) o possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais, o ambiente, a segurança pública ou a saúde da população; iv) a quota de mercado da entidade no mercado do serviço essencial ou serviços essenciais em questão; v) a zona geográfica suscetível de ser afetada por um incidente, incluindo um eventual impacto transfronteiriço, tendo em conta a vulnerabilidade associada ao grau de isolamento de determinados tipos de zonas geográficas, como sejam as regiões insulares, as regiões remotas ou as zonas montanhosas; vi) a importância da entidade na manutenção de um nível de serviço essencial suficiente, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço essencial.

(13) A bem da eficiência e eficácia, importa que o Plano de Ação para as Infraestruturas Críticas seja totalmente coerente e interoperável com o protocolo operacional revisto

da União para a luta contra as ameaças híbridas[5] e tenha em conta o atual plano de ação para a resposta coordenada a incidentes e crises de cibersegurança transfronteiriços em larga escala estabelecido pela Recomendação (UE) 2017/1584 da Comissão[6](Plano de Ação para a Cibersegurança) e o mandato da Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe) estabelecido na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[7] e evite a duplicação de estruturas e atividades. Deve também respeitar plenamente o Mecanismo Integrado da UE de Resposta Política a Situações de Crise[8] (IPCR) do Conselho para a coordenação da resposta.

(14) A presente recomendação baseia-se e é, de um modo mais geral, coerente com os mecanismos de gestão de crises estabelecidos pela União, e complementar dos mesmos, nomeadamente o mecanismo IPCR do Conselho, o processo interno de coordenação de crises da Comissão ARGUS[9] e o Mecanismo de Proteção Civil da União (MPCUE)[10], apoiado pelo Centro de Coordenação de Resposta de Emergência (CCRE)[11], o Mecanismo de Resposta a Situações de Crise do Serviço Europeu para a Ação Externa (SEAE), bem como o Instrumento de Emergência do Mercado Único[12], que podem, todos eles, desempenhar um papel na resposta a uma perturbação grave das operações em infraestruturas críticas.

(15) Na resposta a um incidente significativo em infraestruturas críticas, os supramencionados instrumentos ou mecanismos a nível da União podem ser utilizados, em conformidade com as regras e procedimentos aplicáveis aos mesmos, que a presente recomendação deve complementar, mas não afetar. Por exemplo, o mecanismo IPCR do Conselho continua a ser o principal instrumento de coordenação da resposta a nível político da União entre os Estados-Membros. A coordenação interna no seio da Comissão tem lugar no âmbito do processo de coordenação transetorial de crises ARGUS. Se a crise implicar uma dimensão externa ou a nível da política comum de segurança e defesa (PCSD), pode ser ativado o Mecanismo de Resposta a Situações de Crise do Serviço Europeu para a Ação Externa (SEAE). Em conformidade com a Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União Europeia (MPCUE), as respostas operacionais no âmbito do MPCUE a catástrofes naturais e de origem humana, reais ou iminentes, dentro e fora da União

---

5 Documento de trabalho conjunto dos serviços da Comissão — *EU Protocol for countering hybrid threats*, SWD(2023) 116 final.

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

7 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 (JO L 333 de 27.12.2022, p. 80).

8 Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (JO L 320 de 17.12.2018, p. 28).

9 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões - Disposições da Comissão que criam o sistema geral de alerta rápido «ARGUS», COM(2005) 662 final.

10 Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 347 de 20.12.2013, p. 924).

11 A Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União (MPCUE) cria um quadro para todos os riscos que define modalidades de prevenção, preparação e resposta a nível da União para gerir todos os tipos de catástrofes naturais e de origem humana ou de catástrofes iminentes dentro e fora da UE.

12 Regulamento …/… do Parlamento Europeu e do Conselho que cria um Instrumento de Emergência do Mercado Único e que revoga o Regulamento (CE) n.º 2679/98 do Conselho, COM(2022) 459 final.

(incluindo as que afetam infraestruturas críticas) são organizadas pelo CCRE, o centro operacional permanente único da Comissão que gere as respostas a situações de crise. Nesses casos, o CCRE pode assegurar o alerta rápido, a notificação, a análise, o apoio à partilha de informações e, em caso de ativação do MPCUE por um Estado-Membro, o destacamento de assistência operacional e de peritos para as zonas afetadas. Além disso, o CCRE pode facilitar a coordenação setorial e transetorial tanto a nível da UE como entre a UE e as autoridades nacionais competentes, incluindo as responsáveis pela proteção civil e pela resiliência das infraestruturas críticas.

(16) Embora os processos estabelecidos na presente recomendação devam ser tidos em conta, se for caso disso, em ligação com esses outros instrumentos ou mecanismos quando são utilizados, a presente recomendação deve também descrever as ações que poderão ser empreendidas a nível da União no que respeita ao conhecimento partilhado da situação, à comunicação pública coordenada e à resposta eficaz fora do quadro desses mecanismos de coordenação de crises da União, caso não sejam utilizados.

(17) A fim de coordenar melhor a resposta em caso de incidentes significativos em infraestruturas críticas, cumpre reforçar a cooperação entre os Estados-Membros e as instituições da União, órgãos e organismos competentes da União, através dos dispositivos existentes, no quadro do Plano de Ação para as Infraestruturas Críticas. O Plano de Ação para as Infraestruturas Críticas deve, por conseguinte, aplicar-se quando se atingir o limiar de seis ou mais Estados-Membros previsto na Diretiva (UE) 2022/2557 no que respeita à identificação de entidades críticas de especial relevância europeia, ou quando ocorram incidentes que afetem um número mais reduzido de Estados-Membros com um vasto impacto potencial, devido a efeitos em cascata transfronteiriços, pelo que a coordenação da resposta a nível da União será benéfica.

(18) Embora se considere necessário um quadro de cooperação a nível da União para uma resposta coordenada a incidentes significativos em infraestruturas críticas, este não deve desviar os recursos das entidades críticas e das autoridades competentes afetos ao tratamento de incidentes, que deve ser a prioridade.

(19) Os intervenientes relevantes que participam na execução do Plano de Ação para as Infraestruturas Críticas devem ser claramente identificados, de modo a proporcionar uma visão clara e completa das instituições, órgãos e organismos e das autoridades que possam estar a dar resposta a incidentes significativos em infraestruturas críticas.

(20) A resposta a incidentes em infraestruturas críticas, incluindo incidentes significativos, é primeiramente da responsabilidade das autoridades competentes dos Estados-Membros. A presente recomendação não deve afetar a responsabilidade dos Estados-Membros na salvaguarda da segurança ou defesa nacionais, nem a sua competência para salvaguardar outras funções essenciais do Estado, em especial no que se refere à segurança pública, integridade territorial e manutenção da ordem pública, em conformidade com o direito da União. Além disso, a presente recomendação não deve afetar os processos nacionais, tais como a comunicação e a ligação dos operadores de infraestruturas críticas com as autoridades nacionais competentes. A presente recomendação deve aplicar-se sem afetar acordos bilaterais ou multilaterais pertinentes celebrados entre Estados-Membros.

(21) A designação ou o estabelecimento de pontos de contacto por parte dos intervenientes relevantes é essencial para uma cooperação eficaz e atempada no quadro do Plano de Ação para as Infraestruturas Críticas. A fim de assegurar a coerência, os Estados-Membros devem ponderar a possibilidade de os pontos de contacto designados ou

estabelecidos neste quadro serem os mesmos que os pontos de contacto únicos a designar ou estabelecer no âmbito da Diretiva (UE) 2022/2557.

(22) No interesse da eficácia, o teste e a prática do Plano de Ação para as Infraestruturas Críticas, bem como a comunicação de informações e o debate dos ensinamentos retirados após a sua aplicação, devem ser um elemento essencial para manter um elevado nível de preparação em caso de incidentes significativos em infraestruturas críticas e para assegurar a capacidade de dar uma resposta célere e bem coordenada, com a participação dos intervenientes relevantes.

(23) Considerando a estrutura do mecanismo de coordenação de crises do Conselho (IPCR) e tendo em conta, de um modo mais geral, a potencial ativação dos mecanismos de coordenação de crises já existentes a nível da União, o Plano de Ação para as Infraestruturas Críticas deve abranger duas modalidades de cooperação para dar resposta a um incidente significativo em infraestruturas críticas. A primeira deve consistir no intercâmbio de informações com a participação de todos os intervenientes relevantes, na coordenação da comunicação pública e, quando utilizada, na coordenação através de mecanismos já existentes, como o mecanismo IPCR no Conselho, ou a coordenação ARGUS a nível da Comissão, com o apoio do CCRE como ponto de contacto operacional permanente, e o Mecanismo de Resposta a Situações de Crise do SEAE. A segunda deve incluir outras medidas de intervenção devido à dimensão do incidente. Esta cooperação deve implicar um compromisso a nível operacional, estratégico/político, que reflita os níveis previstos na Recomendação 2017/1584 e no Protocolo da UE para a luta contra as ameaças híbridas, a fim de coordenar as ações e responder de forma eficaz e eficiente ao incidente significativo em infraestruturas críticas. Com base nos princípios da proporcionalidade, da subsidiariedade, da confidencialidade da informação e da complementaridade, e a fim de assegurar uma cooperação eficaz, o Plano de Ação para as Infraestruturas Críticas deve descrever de que forma se processa a partilha do conhecimento da situação pelos intervenientes relevantes, bem como a comunicação pública coordenada e uma resposta eficaz.

(24) O intercâmbio de informações nos termos da presente recomendação deve ser efetuado sem pôr em causa a segurança nacional ou a segurança e os interesses comerciais das entidades que exploram infraestruturas críticas. Por conseguinte, as informações sensíveis devem ser consultadas, trocadas e tratadas com prudência, em conformidade com as regras aplicáveis e dedicando especial atenção aos canais de transmissão e às capacidades de armazenamento utilizadas,

ADOTOU A PRESENTE RECOMENDAÇÃO:

(1) Os Estados-Membros, o Conselho, a Comissão e, se for o caso, o Serviço Europeu para a Ação Externa (SEAE) e os órgãos, e organismos competentes da União devem cooperar entre si no quadro de um Plano de Ação para as Infraestruturas Críticas estabelecido na presente recomendação, a fim de alcançar os objetivos estabelecidos na parte I, secção 1, do anexo e, tendo em conta os princípios enunciados na parte I, secção 2, do anexo, dar uma resposta coordenada a incidentes significativos em infraestruturas críticas.

(2) Os Estados-Membros, o Conselho, a Comissão e, se for o caso, o SEAE e os órgãos e organismos competentes da União devem aplicar o Plano de Ação para as Infraestruturas Críticas, sem demora injustificada, sempre que ocorra um incidente

significativo em infraestruturas críticas, ou seja, um incidente que envolva infraestruturas críticas com um dos seguintes efeitos:

(a) Um efeito perturbador significativo na prestação de serviços essenciais a, ou em, seis ou mais Estados-Membros, nomeadamente quando afeta uma entidade crítica de especial relevância europeia na aceção do artigo 17.º da Diretiva (UE) 2022/2557 relativa à resiliência das entidades críticas[13]; ou

(b) Um efeito perturbador significativo na prestação de serviços essenciais em dois ou mais Estados-Membros, sempre que o Estado-Membro que exerce a Presidência rotativa do Conselho, em concertação com esses outros Estados-Membros e em consulta com a Comissão, considere que é necessária uma coordenação atempada da resposta a nível da União, devido ao impacto de grande alcance e com repercussões a nível técnico ou político do incidente.

(3) Os intervenientes relevantes do Plano de Ação para as Infraestruturas Críticas, identificados a nível operacional, estratégico/político em conformidade com a parte I, secção 3, do anexo, devem esforçar-se por interagir e cooperar em complementaridade. Devem assegurar o intercâmbio adequado e atempado de informações, incluindo a coordenação da comunicação pública, e a resposta coordenada, tal como estabelecido na parte II do anexo.

(4) O Plano de Ação para as Infraestruturas Críticas deve ser aplicado tendo em conta e em coerência com outros instrumentos pertinentes, em conformidade com a parte I, secção 4, do anexo. Caso um incidente afete tanto os aspetos físicos como a cibersegurança das infraestruturas críticas, devem ser asseguradas sinergias com os processos estabelecidos no plano cibernético.

(5) Os Estados-Membros devem assegurar que respondem eficazmente, a nível nacional e em conformidade com o direito da União, a perturbações em infraestruturas críticas na sequência de incidentes significativos em infraestruturas críticas.

(6) Os Estados-Membros, o Conselho, o SEAE, a Agência da União Europeia para a Cooperação Policial (Europol) e outras agências competentes da União devem, bem como a Comissão, designar ou estabelecer um ponto de contacto para questões relacionadas com o Plano de Ação para as Infraestruturas Críticas. Os pontos de contacto devem apoiar a aplicação do Plano de Ação para as Infraestruturas Críticas, facultando as informações necessárias e facilitando medidas de coordenação em resposta a um incidente significativo em infraestruturas críticas. No que se refere aos Estados-Membros, sempre que possível, esses pontos de contacto devem ser os mesmos que os pontos de contacto únicos a designar ou a estabelecer nos termos do artigo 9.º, n.º 2, da Diretiva (UE) 2022/2557. Para a Comissão, o CCRE assegura o contacto e a capacidade operacional permanente e coordena, acompanha e apoia, em tempo real, a resposta a emergências a nível da União, servindo simultaneamente os Estados-Membros e a Comissão como plataforma operacional de resposta a situações de crise, promovendo uma abordagem transetorial da gestão de catástrofes.

(7) O Estado-Membro que exerce a Presidência rotativa do Conselho, com o acordo dos Estados-Membros afetados, deve informar todos os intervenientes relevantes, através

[13] Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho (JO L 333 de 27.12.2022, p. 164).

dos pontos de contacto referidos no ponto 6, do incidente significativo em infraestruturas críticas e da aplicação do Plano de Ação para as Infraestruturas Críticas. O intercâmbio de informações sobre um incidente significativo em infraestruturas críticas deve ocorrer através de canais de comunicação adequados, incluindo, se for aplicável e apropriado, a plataforma do Mecanismo Integrado de Resposta Política a Situações de Crise[14] (IPCR) e o CCRE através do Sistema Comum de Comunicação e de Informação de Emergência (CECIS), uma aplicação baseada na Web de alerta e notificação que permite o intercâmbio de informação em tempo real.

(8) Se necessário, os canais de transmissão devem incluir canais seguros, a fim de não comprometer a segurança nacional ou a segurança e os interesses comerciais das entidades em causa. O intercâmbio de informações descrito na parte II, secção 1, do anexo da presente recomendação deve também ser efetuado sem pôr em causa a segurança nacional ou a segurança e os interesses comerciais das entidades críticas e em conformidade com o Direito da União, nomeadamente o Regulamento (UE) .../... do Parlamento Europeu e do Conselho[15]. Em especial, as informações sensíveis devem ser consultadas, trocadas e tratadas com prudência. Devem ser utilizados instrumentos acreditados disponíveis, bem como medidas de segurança adequadas, para o tratamento e o intercâmbio de informações classificadas.

(9) Os intervenientes relevantes devem praticar e testar regularmente o funcionamento do Plano de Ação para as Infraestruturas Críticas e a sua resposta coordenada a um incidente significativo em infraestruturas críticas a nível nacional, regional e da União, por exemplo no quadro de exercícios. Tais práticas e testes podem, quando se justificar, incluir entidades do setor privado. Deverá ser realizado um exercício a nível da União que incorpore os aspetos físicos e cibernéticos até [*data de adoção da presente recomendação +12 meses*].

(10) Na sequência da aplicação do Plano de Ação para as Infraestruturas Críticas a um incidente significativo em infraestruturas críticas, o Grupo para a Resiliência das Entidades Críticas, a que se refere o artigo 19.º da Diretiva (UE) 2022/2557, deve debater com os intervenientes relevantes, em tempo útil, os ensinamentos identificados que possam indicar lacunas e domínios em que são necessárias melhorias e, subsequentemente, elaborar um relatório, incluindo recomendações para alcançar tais melhorias. A elaboração do referido relatório deve ser apoiada pelos intervenientes relevantes que participam na aplicação do Plano de Ação para as Infraestruturas Críticas. O relatório será adotado pela Comissão.

(11) Os Estados-Membros devem debater o relatório mencionado no ponto 10 nas instâncias preparatórias competentes do Conselho ou no Conselho.

---

[14] Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise, ST/13422/2018/INIT (JO L 320 de 17.12.2018, p. 28).

[15] Regulamento (UE) …/… relativo à segurança da informação nas instituições, órgãos e organismos da União, COM(2022) 119 final.

Feito em Bruxelas, em

Pelo Conselho
O Presidente