Conselho da
União Europeia

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

12485/23
ADD 1

Dossiê interinstitucional:
2023/0318(NLE)

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

Anexo: COM(2023) 526 final - ANEXO

COMISSÃO
EUROPEIA

Bruxelas, 6.9.2023
COM(2023) 526 final

ANNEX

ANEXO

da

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

ANEXO

O presente anexo descreve os princípios, os objetivos, os principais intervenientes, a interação com os mecanismos de resposta a situações de crise existentes, bem como o funcionamento de um plano de ação para coordenar a resposta a incidentes significativos em infraestruturas críticas (Plano de Ação para as Infraestruturas Críticas) e melhorar a cooperação entre os Estados-Membros e as instituições, órgãos e organismos competentes da União no que respeita a esses incidentes, em conformidade com as regras e os procedimentos aplicáveis. O presente plano não afeta de forma alguma o papel e o funcionamento de outros dispositivos.

PARTE I: OBJETIVOS, PRINCÍPIOS, INTERVENIENTES E OUTROS INSTRUMENTOS

1. Objetivos

O Plano de Ação para as Infraestruturas Críticas visa alcançar os seguintes três objetivos principais em resposta a um incidente significativo em infraestruturas críticas:

(a) **O conhecimento partilhado da situação**, uma vez que uma boa compreensão do incidente significativo em infraestruturas críticas nos Estados-Membros, da sua origem e das suas potenciais consequências para todas as partes interessadas a nível operacional e estratégico/político é essencial para uma resposta coordenada adequada;

(b) **Uma comunicação pública coordenada**, uma vez que contribui para atenuar os efeitos negativos de um incidente significativo em infraestruturas críticas e minimizar as discrepâncias nas mensagens transmitidas ao público nos Estados-Membros e entre Estados-Membros. Uma comunicação pública clara é igualmente importante para atenuar as consequências da desinformação;

(c) **Uma resposta eficaz**, uma vez que o reforço da resposta dos Estados-Membros e da cooperação entre os Estados-Membros e com as instituições, órgãos e organismos competentes da União contribui para atenuar os efeitos de um incidente significativo em infraestruturas críticas e viabilizar o rápido restabelecimento dos serviços essenciais de uma forma que minimize a vulnerabilidade a novos incidentes significativos.

2. Princípios

Proporcionalidade

Muitas vezes, os incidentes que perturbam infraestruturas críticas e/ou a prestação de serviços essenciais não atingem o limiar de um incidente significativo em infraestruturas críticas, conforme especificado no ponto 2 da presente recomendação. Assim, podem, em princípio, ser tratados de forma eficaz a nível nacional. Por conseguinte, a aplicação do Plano de Ação para as Infraestruturas Críticas limita-se a incidentes significativos em infraestruturas críticas.

Subsidiariedade

Os Estados-Membros são os principais responsáveis pela resposta a perturbações numa infraestrutura crítica ou em serviços essenciais prestados por entidades críticas, em conformidade com o direito da União. No entanto, as instituições, órgãos e organismos competentes da União e o Serviço Europeu para a Ação Externa (SEAE) desempenham um importante papel complementar em caso de um incidente significativo em infraestruturas críticas com grande relevância transfronteiriça, uma vez que esse incidente pode afetar vários

ou mesmo todos os setores da atividade económica no mercado interno, a vida dos cidadãos que vivem na União, a segurança e as relações internacionais da União.

Complementaridade

O Plano para as Infraestruturas Críticas tem em conta e reflete o funcionamento dos mecanismos de gestão de crises existentes a nível da União, nomeadamente o Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) do Conselho, o processo interno de coordenação de crises da Comissão ARGUS, o Mecanismo de Proteção Civil da União (MPCUE), apoiado pelo Centro de Coordenação de Resposta de Emergência (CCRE) e o Mecanismo de Resposta a Situações de Crise do SEAE. Tem igualmente por base acordos setoriais, incluindo as disposições para a gestão coordenada de incidentes de cibersegurança em grande escala previstas na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[1] e o quadro estabelecido no Plano de ação para a resposta coordenada a incidentes e crises de cibersegurança transfronteiriços em larga escala (Plano de Ação para a Cibersegurança)[2], a Rede de Pontos de Contacto para os Transportes[3] e a Célula de Coordenação de Crises da Aviação Europeia[4].

Além disso, baseia-se e deve ser aplicado em conformidade com as estruturas e mecanismos estabelecidos pela Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho[5], em especial no que respeita à cooperação entre as autoridades competentes e com a Comissão e no Grupo para a Resiliência das Entidades Críticas. Tem igualmente em conta as responsabilidades das instituições, órgãos e organismos competentes da União ao abrigo do quadro jurídico que lhes é aplicável. As atividades de resposta a situações de crise que afetam infraestruturas críticas são complementares de outros mecanismos de gestão de crises a nível da União, nacional e setorial que apoiam a coordenação multissetorial.

Confidencialidade da informação

O Plano de Ação para as Infraestruturas Críticas tem em conta a importância de salvaguardar a confidencialidade das informações classificadas e sensíveis não classificadas relacionadas com infraestruturas críticas e entidades críticas.

3. Intervenientes relevantes

Cada Estado-Membro e as instituições, órgãos e organismos competentes da União a que se referem as alíneas a) a e) *infra* decidirão, em conformidade com as regras e o procedimento que lhes são aplicáveis, sobre o(s) interveniente(s) relevante(s) para cada incidente significativo em infraestruturas críticas, em função do(s) setor(es) afetado(s) e do tipo de incidente.

---

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

2 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).

3 Comunicação da Comissão - Plano de emergência para os transportes, COM(2022) 211 final.

4 Criada nos termos do artigo 19.º do Regulamento de Execução (UE) 2019/123 da Comissão, de 24 de janeiro de 2019, que estabelece as regras de execução para a implementação das funções de rede na gestão do tráfego aéreo (ATM).

5 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).

a) Estados-Membros

- Autoridades competentes [por exemplo, autoridades responsáveis por infraestruturas críticas, autoridades setoriais competentes, pontos de contacto únicos designados ou estabelecidos nos termos do artigo 9.º, n.º 2, da Diretiva (UE) 2022/2557, autoridades designadas ou estabelecidas nos termos do artigo 9.º, n.º 1, da Diretiva (UE) 2022/2557];

- Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe) a que se refere o artigo 16.º da Diretiva (UE) 2022/2555;

- O grupo de cooperação a que se refere o artigo 14.º da Diretiva (UE) 2022/2555;

- Se for o caso, outras partes interessadas, nomeadamente entidades ou pessoas do setor privado, como os operadores de infraestruturas críticas, incluindo os identificados como entidades críticas;

- Ministros responsáveis pela resiliência das infraestruturas críticas e/ou o(s) ministro(s) responsável(eis) pelo setor ou setores mais afetados pelo incidente significativo em infraestruturas críticas em questão.

b) O Conselho

- A Presidência rotativa;

- Os grupos de trabalho pertinentes, como o Grupo da Proteção Civil, incluindo o subgrupo para a resiliência das entidades críticas PROCIV-CER e o(s) presidente(s) do(s) grupo(s) de trabalho pertinente(s), consoante o(s) setor(es) afetado(s) e a natureza do incidente, tais como o Grupo Horizontal das Questões do Ciberespaço e o Grupo Horizontal para o Reforço da Resiliência e a Luta contra as Ameaças Híbridas;

- O COREPER, o Comité Político e de Segurança e o IPCR, todos apoiados pelo Secretariado-Geral do Conselho.

c) A Comissão, incluindo os grupos de peritos da Comissão

- Serviço responsável designado (consoante o setor afetado) apoiado pelo CCRE enquanto centro operacional permanente para gerir as respostas a situações de crise e pela Direção-Geral da Migração e dos Assuntos Internos enquanto serviço competente na zona e, em caso de incidente transetorial, pela Direção-Geral da Migração e dos Assuntos Internos e outros serviços competentes da Comissão;

- A Direção-Geral da Comunicação e o Serviço do Porta-Voz;

- Direção-Geral HERA,-Autoridade de Preparação e Resposta a Emergências Sanitárias;

- O Grupo para a Resiliência das Entidades Críticas, presidido por um representante da Comissão (Direção-Geral da Migração e dos Assuntos Internos), criado pela Diretiva (UE) 2022/2557, e, se for o caso, outros grupos de peritos e comités pertinentes;

- O CCRE criado ao abrigo do MPCUE pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho[6] (centro operacional permanente de gestão de emergências no quadro

[6] 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).

do MPCUE localizado na Direção-Geral da Proteção Civil e das Operações de Ajuda Humanitária Europeias);

- O grupo de cooperação a que se refere o artigo 14.º da Diretiva (UE) 2022/2555;

- O Centro de Conhecimento Situacional e de Análise Cibernética;

- O Comité de Segurança da Saúde, a que se refere o artigo 4.º do Regulamento (UE) 2022/2371[7];

- O Secretariado-Geral da Comissão (secretariado ARGUS) e o secretário-geral (adjunto) (processo ARGUS), Direção-Geral dos Recursos Humanos (Direção de Segurança);

- Outros grupos de peritos relevantes da Comissão que a assistem na coordenação de medidas em situações de emergência ou de crise;

- Outras redes de gestão de crises, nomeadamente setoriais (por exemplo, Rede de Pontos de Contacto para os Transportes gerida pela Direção-Geral da Mobilidade e dos Transportes, o Grupo de Trabalho Interinstitucional para Cibercrises[8], a Célula de Coordenação de Crises da Aviação Europeia);

- O presidente e/ou o vice-presidente/comissário competente.

d) SEAE

- Capacidade Única de Análise de Informações (SIAC) composta pelo Centro de Situação e de Informações (INTCEN) e pela Direção de Informações do Estado-Maior da UE (EUME Int);

- Centro de Resposta a Crises (CRC);

- O alto representante da União para os Negócios Estrangeiros e a Política de Segurança/vice-presidente da Comissão.

e) Órgãos e organismos competentes da União e agências competentes da União, como a Europol, em função do(s) setor(es) afetado(s)[9].

[7] Regulamento (UE) 2022/2371 do Parlamento Europeu e do Conselho, de 23 de novembro de 2022, relativo às ameaças transfronteiriças graves para a saúde e que revoga a Decisão n.º 1082/2013/UE (JO L 314 de 6.12.2022, p. 26).

[8] Um grupo informal que inclui os serviços competentes da Comissão, o SEAE, a Agência da União Europeia para a Cibersegurança (ENISA), a CERT-UE e a Europol, copresidido pela Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias e pelo SEAE.

[9] Tais como a Europol; para os transportes: a Agência da União Europeia para a Segurança da Aviação (AESA), a Agência Europeia da Segurança Marítima (EMSA), a Agência Ferroviária da União Europeia (AFE); para a saúde o Centro Europeu de Prevenção e Controlo das Doenças (ECDC) e a Agência Europeia de Medicamentos (EMA); para a energia: a Agência de Cooperação dos Reguladores da Energia (ACER); para o espaço: a Agência da União Europeia para o Programa Espacial (EUSPA); para o setor alimentar: a Autoridade Europeia para a Segurança dos Alimentos (EFSA); para o setor marítimo: a Agência Europeia de Controlo das Pescas (AECP); para os ciberincidentes: a Agência da União Europeia para a Cibersegurança (ENISA), as Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) e a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE).

4. Interação com outros mecanismos e instrumentos de gestão de crises relevantes

O Plano de Ação para as Infraestruturas Críticas é uma ferramenta flexível que define várias ações que podem ser realizadas parcial ou totalmente com recurso a diferentes dispositivos existentes, em função da natureza e gravidade do incidente significativo em infraestruturas críticas e da necessidade de coordenação operacional, estratégica/política.

a) Protocolo da UE para a luta contra as ameaças híbridas[10] (Protocolo da UE)

O Protocolo da UE aplica-se em situação de ameaças híbridas[11], apresentando uma descrição dos processos e instrumentos aplicáveis em caso de ameaças ou campanhas desse tipo.

No caso de um incidente significativo em infraestruturas críticas com uma dimensão híbrida, o Protocolo da UE aplica-se em complementaridade com o Plano de Ação para as Infraestruturas Críticas, se for caso disso, por exemplo, no que se refere a informações, análises ou comunicações específicas sobre aspetos híbridos do incidente significativo em infraestruturas críticas e no que respeita à cooperação com parceiros externos.

b) Plano de ação para a resposta coordenada a incidentes e crises de cibersegurança transfronteiriços em larga escala

O Plano de Ação para a Cibersegurança aplica-se a incidentes transfronteiriços em larga escala que causem perturbações demasiado extensas para que um Estado-Membro afetado 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.

No caso de um incidente significativo em infraestruturas críticas que coincida ou aparente estar relacionado com um incidente de cibersegurança em larga escala, os grupos de trabalho competentes do Conselho determinam a coordenação adequada a nível operacional, incluindo a UE-CyCLONe ou através de uma reunião conjunta do Grupo para a Resiliência das Entidades Críticas com o grupo de cooperação. O objetivo da coordenação é determinar quais os intervenientes, instrumentos ou mecanismos que podem contribuir de forma mais eficaz para dar resposta ao incidente significativo em infraestruturas críticas, evitando simultaneamente duplicações e vertentes de trabalho paralelas.

c) Mecanismo de Proteção Civil da União e Centro de Coordenação de Resposta de Emergência

Em conformidade com a Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União, as respostas operacionais no âmbito do MPCUE a catástrofes naturais e de origem humana, reais ou iminentes (incluindo as que envolvem perturbações em infraestruturas críticas), dentro e fora da União, são lideradas 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 e 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 União como entre a União e as

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

[11] As ameaças híbridas podem ser caracterizadas como uma mistura de atividades coercivas e subversivas, métodos convencionais e não convencionais, que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para alcançar objetivos específicos, mantendo-se ao mesmo tempo abaixo do limiar da guerra formalmente declarada, cf. o Protocolo da UE relativo às ameaças híbridas.

autoridades nacionais competentes, incluindo as responsáveis pela proteção civil e pela resiliência das infraestruturas críticas.

d) Outros mecanismos e instrumentos setoriais ou transetoriais

O presente Plano de Ação para as Infraestruturas Críticas não duplica outros instrumentos de gestão de crises ou mecanismos de coordenação setoriais ou transetoriais. Sempre que tais instrumentos ou mecanismos já existam no setor afetado, o presente Plano de Ação para as Infraestruturas Críticas, dentro do seu âmbito de aplicação, pode ser utilizado como instrumento complementar aos instrumentos ou mecanismos setoriais ou transetoriais, mas não os substitui. Haverá que assegurar a necessária coordenação entre os vários intervenientes, de modo a evitar essa duplicação, o que poderá ser conseguido, por exemplo, no âmbito do processo interno de coordenação de crises da Comissão ARGUS, apoiado pelo CCRE, e/ou em reuniões de coordenação no quadro do IPCR.

PARTE II: INTERCÂMBIO DE INFORMAÇÕES E RESPOSTA COORDENADA

As ações a seguir descritas consistem em modalidades de cooperação, a saber, o intercâmbio de informações, a comunicação e a resposta coordenada. Esta estrutura corresponde às modalidades do mecanismo de coordenação de crises IPCR do Conselho e tem em conta, de um modo mais geral, a potencial utilização dos mecanismos de coordenação de crises já existentes a nível da UE. Esta estrutura mostra como estas modalidades de cooperação se integrarão nesses mecanismos, se utilizadas. No entanto, a maioria destas ações também podem ser desenvolvidas de forma autónoma: não dependem da utilização desse mecanismo, mas sim complementam-no. As ações são apresentadas por ordem cronológica, tendo simultaneamente em conta que, em caso de crise em grande escala que constitua um incidente significativo em infraestruturas críticas, podem ser levadas a cabo várias ações em simultâneo e continuamente.

1. TROCA DE INFORMAÇÕES

(a) A nível operacional

Os Estados-Membros afetados pelo incidente significativo em infraestruturas críticas aplicam as suas próprias medidas de contingência, asseguram a coordenação com os mecanismos nacionais de gestão de crises pertinentes e a participação de todos os intervenientes nacionais, regionais e locais relevantes, conforme adequado.

Se for o caso, no que diz respeito à assistência de proteção civil, a coordenação entre os Estados-Membros e com a Comissão é assegurada através do CCRE ao abrigo do MPCUE.

i) Partilha de informações e notificação pelas autoridades nacionais competentes

Para além das obrigações de notificação e de informação previstas no artigo 15.º da Diretiva (UE) 2022/2557, as autoridades nacionais competentes responsáveis pelas infraestruturas críticas nos Estados-Membros afetados pelo incidente significativo em infraestruturas críticas partilham com a Presidência rotativa do Conselho e a Comissão, através dos seus pontos de contacto únicos e sem demora injustificada, informações relevantes recebidas do(s) operador(es) de infraestruturas críticas, entidades críticas ou de outras fontes, bem como informações sobre os mecanismos de gestão de crises que foram ativados. 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.

A partilha de informações diz respeito à natureza do incidente significativo na infraestrutura crítica, à sua causa, ao impacto observado ou estimado da perturbação na infraestrutura crítica e na prestação de serviços essenciais, às consequências do incidente a nível setorial e transfronteiriço e às medidas de atenuação, já tomadas ou previstas, a nível nacional ou com outros Estados-Membros pertinentes e a Comissão, através dos dispositivos existentes, por exemplo, os mecanismos de partilha de informações nos termos dos artigos 9.º e 15.º da Diretiva (UE) 2022/2557. Esta notificação é enviada sem desviar os recursos da infraestrutura crítica ou, em alguns casos, da entidade crítica ou do Estado-Membro afetos a atividades relacionadas com o tratamento de incidentes, às quais deverá ser atribuída prioridade.

A fim de assegurar o acompanhamento, o CCRE ou os serviços notificados da Comissão responsáveis pelo(s) setor(es) em que ocorreu o incidente significativo na infraestrutura crítica informam o ponto de contacto na Direção-Geral da Migração e dos Assuntos Internos e o Secretariado-Geral da Comissão. Entretanto, se ainda não o tiver feito, o CCRE começa a acompanhar os acontecimentos, especialmente em caso de ativação do MPCUE por um ou mais dos Estados-Membros afetados.

Se as informações puderem ser relevantes para responder a uma dimensão de cibersegurança ou estiverem relacionadas com um incidente de cibersegurança, a Comissão partilha as informações relevantes com a UE-CyCLONe.

As autoridades nacionais competentes nos termos da Diretiva (UE) 2022/2557 cooperam e trocam informações com as autoridades competentes nos termos da Diretiva (UE) 2022/2555, sem demora injustificada, em relação a ciberincidentes e incidentes que afetem entidades críticas, incluindo as medidas físicas e de cibersegurança tomadas por entidades críticas.

No domínio marítimo, as autoridades nacionais competentes devem ponderar a possibilidade de utilizar o ambiente comum de partilha da informação (CISE) para partilhar informações sem demora injustificada.

ii) Organização de reuniões de peritos

A Comissão convoca o mais rapidamente possível o Grupo para a Resiliência das Entidades Críticas a fim de facilitar o intercâmbio de informações entre as autoridades nacionais competentes responsáveis pelas infraestruturas críticas e as instituições, órgãos e organismos competentes da União sobre o incidente (natureza, causa, impacto e consequências a nível setorial e transfronteiriço) e sobre medidas de resposta, incluindo medidas de atenuação e apoio técnico aos Estados-Membros afetados. Dependendo do centro de gravidade do incidente, os serviços competentes da Comissão estarão estreitamente associados à reunião do Grupo para a Resiliência das Entidades Críticas, a fim de partilhar as informações recolhidas através dos instrumentos setoriais existentes. Em caso de incidentes com uma combinação de aspetos de cibersegurança e aspetos físicos não cibernéticos, os serviços competentes da Comissão, a CERT-UE e o SEAE, se for caso disso, notificam e consultam o mais rapidamente possível o Grupo de Trabalho para Cibercrises, bem como os respetivos presidentes do grupo de cooperação a que se refere o artigo 14.º da Diretiva (UE) 2022/2555, e a UE-CyCLONe, consoante o caso, sobre a necessidade de atividades de coordenação. Com o acordo dos respetivos presidentes, a Comissão (Direção-Geral da Migração e dos Assuntos Internos e Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias) pode propor uma reunião conjunta do Grupo para a Resiliência das Entidades Críticas com o grupo de cooperação com vista a um conhecimento partilhado da situação e à coordenação das respetivas respostas.

No caso de um incidente significativo transetorial em infraestruturas críticas que exija ou seja suscetível de exigir uma gestão das consequências a nível da União, a Comissão pode

convocar reuniões de coordenação transetorial com a participação de todas as partes interessadas.

Caso um incidente significativo em infraestruturas críticas afete também um país terceiro, a Comissão consulta a autoridade competente do país terceiro afetado e pode convidá-la para uma reunião do Grupo para a Resiliência das Entidades Críticas.

iii) Apoio da Comissão e das agências da União

Se for caso disso, e atuando em conformidade com o seu mandato, a Europol apresenta um relatório sobre a situação dos incidentes a nível da União. Outras agências da União, se pertinente e atuando em conformidade com os respetivos mandatos, comunicam informações que contribuam para o conhecimento da situação ou para a resposta coordenada ao incidente significativo em infraestruturas críticas às respetivas direções-gerais de tutela que, por sua vez, informam a Comissão (Direção-Geral da Migração e dos Assuntos Internos, na qualidade de presidente do Grupo para a Resiliência das Entidades Críticas).

A Comissão pode contribuir para o conhecimento da situação utilizando os recursos do Programa Espacial da União[12], como o Copernicus, o Galileo e o EGNOS, sempre que adequado e em conformidade com o quadro jurídico aplicável.

(b) A nível estratégico

i) Elaboração de relatórios de conhecimento da situação

Com base em informações partilhadas pelas autoridades nacionais competentes numa reunião do Grupo para a Resiliência das Entidades Críticas ou em reuniões conjuntas com os serviços, grupos de peritos ou redes pertinentes, a Comissão elabora um relatório de conhecimento da situação com base nos contributos das autoridades nacionais competentes e noutras informações disponíveis.

O relatório deve, se for o caso, ter em conta os resultados das avaliações de risco, análises e cenários relevantes a nível da UE numa perspetiva de cibersegurança, incluindo os realizados pela Comissão, pelo alto representante da União para os Negócios Estrangeiros e a Política de Segurança e pelo grupo de cooperação.

Em caso de ativação do IPCR, este relatório pode contribuir para o relatório de conhecimento e análise integrados da situação (ISAA) elaborado pelos serviços da Comissão e pelo SEAE.

A SIAC, se pertinente, apresenta uma avaliação atualizada do incidente, com base em informações.

ii) Ativação dos mecanismos de coordenação de crises da União e utilização dos instrumentos da União

O CCRE começa a prestar apoio com vista ao conhecimento da situação em torno do incidente, se for caso disso, em especial se o acontecimento desencadear a ativação do MPCUE[13]. Além disso, os Estados-Membros afetados podem solicitar imagens de satélite do seu território através do Serviço de Gestão de Emergências do Copernicus.

---

[12] Regulamento (UE) 2021/696 do Parlamento Europeu e do Conselho, de 28 de abril de 2021, que cria o Programa Espacial da União e a Agência da União Europeia para o Programa Espacial e que revoga os Regulamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 e (UE) n.º 377/2014 e a Decisão n.º 541/2014/UE (JO L 170 de 12.5.2021, p. 69).

[13] Como, por exemplo, a publicação de produtos de acompanhamento dos meios de comunicação social, mensagens de proteção civil, notas analíticas, mapas diários ECHO, resumos diários ECHO e outros produtos personalizados.

Sempre que se considerar adequado partilhar informações entre a Comissão e o SEAE e as agências competentes da União, a direção-geral responsável ou a Direção-Geral da Migração e dos Assuntos Internos, em coordenação com o Secretariado-Geral, ativa o processo interno de coordenação de crises da Comissão ARGUS Fase I, abrindo um evento na ferramenta informática Argus.

A Presidência rotativa do Conselho da União pode ativar o mecanismo IPCR em modo de partilha de informações, o que implica a elaboração de relatórios ISAA pela Comissão e pelo SEAE com contribuições das autoridades nacionais competentes e de outras fontes, se for o caso. Mesmo sem ativar o IPCR, a Presidência rotativa do Conselho ou a Comissão podem lançar, sob determinadas condições, uma página de acompanhamento na plataforma Web do IPCR.

Podem ser ativados outros mecanismos e instrumentos (setoriais) de gestão de crises da União, de acordo com os respetivos procedimentos, conforme adequado. A Comissão assegurará a coordenação entre estes mecanismos e instrumentos.

Se o incidente físico coincidir ou aparentar estar relacionado com um incidente de cibersegurança em grande escala, na aceção do artigo 6.º, n.º 7, da Diretiva (UE) 2022/2555, a Presidência rotativa do Conselho pode utilizar o Plano de Ação para a Cibersegurança para determinar uma coordenação adequada a nível operacional que envolva, entre outros, a UE-CyCLONe e o Grupo para a Resiliência das Entidades Críticas.

iii) Coordenação da comunicação pública

Os Estados-Membros afetados por incidentes significativos em infraestruturas críticas coordenam, na medida do possível, a sua comunicação pública sobre a crise, respeitando as competências nacionais nesta matéria. A Rede de Comunicação de Crises do IPCR pode participar nesta coordenação, se adequado.

Com base no conhecimento partilhado da situação, o Grupo para a Resiliência das Entidades Críticas e os Estados-Membros afetados apoiam a formulação de linhas de comunicação públicas acordadas, quando adequado.

A Europol e outras agências competentes da União coordenam as suas atividades de comunicação pública com o Serviço do Porta-voz da Comissão, com base no conhecimento partilhado da situação.

Se o incidente significativo em infraestruturas críticas implicar uma dimensão externa, híbrida ou de política comum de segurança e defesa, a comunicação pública é coordenada com o SEAE e o Serviço do Porta-voz da Comissão, em conformidade com o Protocolo da UE para a luta contra as ameaças híbridas[14].

2. RESPOSTA (QUE PREVÊ AÇÕES CONTÍNUAS DESCRITAS NO ÂMBITO DO INTERCÂMBIO DE INFORMAÇÕES E AÇÕES ADICIONAIS A NÍVEL ESTRATÉGICO/POLÍTICO)

(a) A nível estratégico

i) Elaboração contínua de relatórios de situação

O Grupo da Proteção Civil – Resiliência das Entidades Críticas (PROCIV-CER) do Conselho é informado da elaboração de um relatório sobre a situação a nível político/estratégico (por

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

exemplo, o ISAA em caso de ativação do IPCR ou o relatório de conhecimento partilhado da situação elaborado pela Comissão) e prepara o COREPER, caso este ainda não tenha sido convocado, ou a reunião do Comité Político e de Segurança, conforme adequado.

A SIAC intensifica o seu contacto com os serviços de informações dos Estados-Membros, agrega as informações provenientes de todas as fontes e prepara uma análise e avaliação do incidente, bem como atualizações regulares, se necessário.

ii) Plena ativação dos mecanismos de coordenação de crises da União e utilização dos instrumentos da União

Caso a presidente da Comissão ative o processo interno de coordenação de crises da Comissão ARGUS Fase II, são convocadas, a curto prazo, reuniões do Comité de Coordenação de Crises com a participação dos serviços competentes da Comissão, de agências e do SEAE, se for caso disso, a fim de assegurar a coordenação no que respeita a todos os aspetos do incidente significativo em infraestruturas críticas.

Caso se verifique a plena ativação do IPCR pela Presidência do Conselho:

- A Presidência rotativa do Conselho solicita a realização oportuna de uma mesa redonda informal, reunindo os intervenientes nacionais, europeus e internacionais relevantes, em que o representante da Comissão, na qualidade de presidente do Grupo para a Resiliência das Entidades Críticas (Direção-Geral da Migração e dos Assuntos Internos), pode apresentar um relatório sobre a(s) reunião(ões) do grupo previamente convocada(s), com a assistência de outros serviços da Comissão e do SEAE, conforme adequado.

- A SIAC e as agências competentes da União podem ser convidadas a apresentar, nesta reunião, uma atualização da situação no que se refere ao incidente significativo em infraestruturas críticas.

O serviço responsável pelo ISAA (o serviço responsável da Comissão ou o SEAE) elabora o relatório ISAA com contributos dos serviços competentes da Comissão, dos gabinetes, organismos e agências competentes da União e das autoridades nacionais competentes. Os Estados-Membros são convidados a fornecer contributos, através da plataforma Web do IPCR, para a elaboração dos relatórios ISAA.

No caso de um incidente significativo em infraestruturas críticas com relevância para a segurança internacional, os serviços da Comissão e o SEAE podem convocar uma reunião no âmbito do diálogo estruturado UE-OTAN sobre a resiliência, a fim de contribuir para o conhecimento partilhado da situação e para o intercâmbio de informações sobre as medidas tomadas pela União e pela OTAN, respetivamente.

iii) Comunicação pública

O Conselho prepara mensagens comuns de comunicação pública. A rede informal de comunicadores de crise criada através do IPCR pode apoiar este trabalho. O Serviço do Porta-voz da Comissão também prepara mensagens de comunicação pública, se for caso disso.

Se o incidente significativo em infraestruturas críticas implicar uma dimensão externa, híbrida ou de política comum de segurança e defesa, a comunicação pública é coordenada com o SEAE e o Serviço do Porta-voz da Comissão.

iv) Apoio aos Estados-Membros e resposta eficaz

A Presidência rotativa pode convocar uma reunião do PROCIV-CER para apoiar as atividades no quadro do IPCR, caso seja ativado.

Os Estados-Membros afetados pelo incidente significativo em infraestruturas críticas podem solicitar o apoio técnico de outros Estados-Membros ou das instituições, órgãos e organismos competentes da União através do Grupo para a Resiliência das Entidades Críticas, por exemplo, conhecimentos especializados específicos para atenuar os impactos adversos do incidente significativo em infraestruturas críticas.

Os Estados-Membros afetados pelo incidente significativo em infraestruturas críticas podem igualmente solicitar o apoio técnico e/ou financeiro da Comissão ou das agências competentes da União. A Comissão, em coordenação com as agências competentes da União, avalia o seu eventual apoio e ativa, se for caso disso, medidas técnicas de atenuação a nível da União, em conformidade com os respetivos procedimentos, e coordena as capacidades técnicas necessárias para pôr termo ao incidente significativo em infraestruturas críticas ou para reduzir o seu impacto.

Especificamente no contexto do MPCUE, os países afetados podem solicitar assistência através do Sistema Comum de Comunicação e de Informação de Emergência (CECIS), após o que o CCRE trabalhará para coordenar a assistência prestada pelos Estados-Membros e Estados participantes no MPCUE, bem como através da rescEU.

No âmbito dos respetivos mandatos e mediante pedido, a Europol e outras agências competentes da União apoiam os Estados-Membros afetados por um incidente significativo em infraestruturas críticas na investigação do incidente.

(b) A nível político

A Presidência do Conselho poderá considerar a necessidade de convocar mesas redondas no âmbito do IPCR, reuniões dos grupos de trabalho do Conselho, COREPER, Conselho de Ministros e/ou cimeiras para trocar informações sobre a possível origem e as consequências esperadas do incidente significativo em infraestruturas críticas para os Estados-Membros e para a União, chegar a acordo sobre orientações comuns, e adotar as medidas necessárias para apoiar os Estados-Membros afetados pelo incidente significativo em infraestruturas críticas e atenuar os seus efeitos.

Gráfico 1: Síntese esquemática do Plano de Ação para as Infraestruturas Críticas

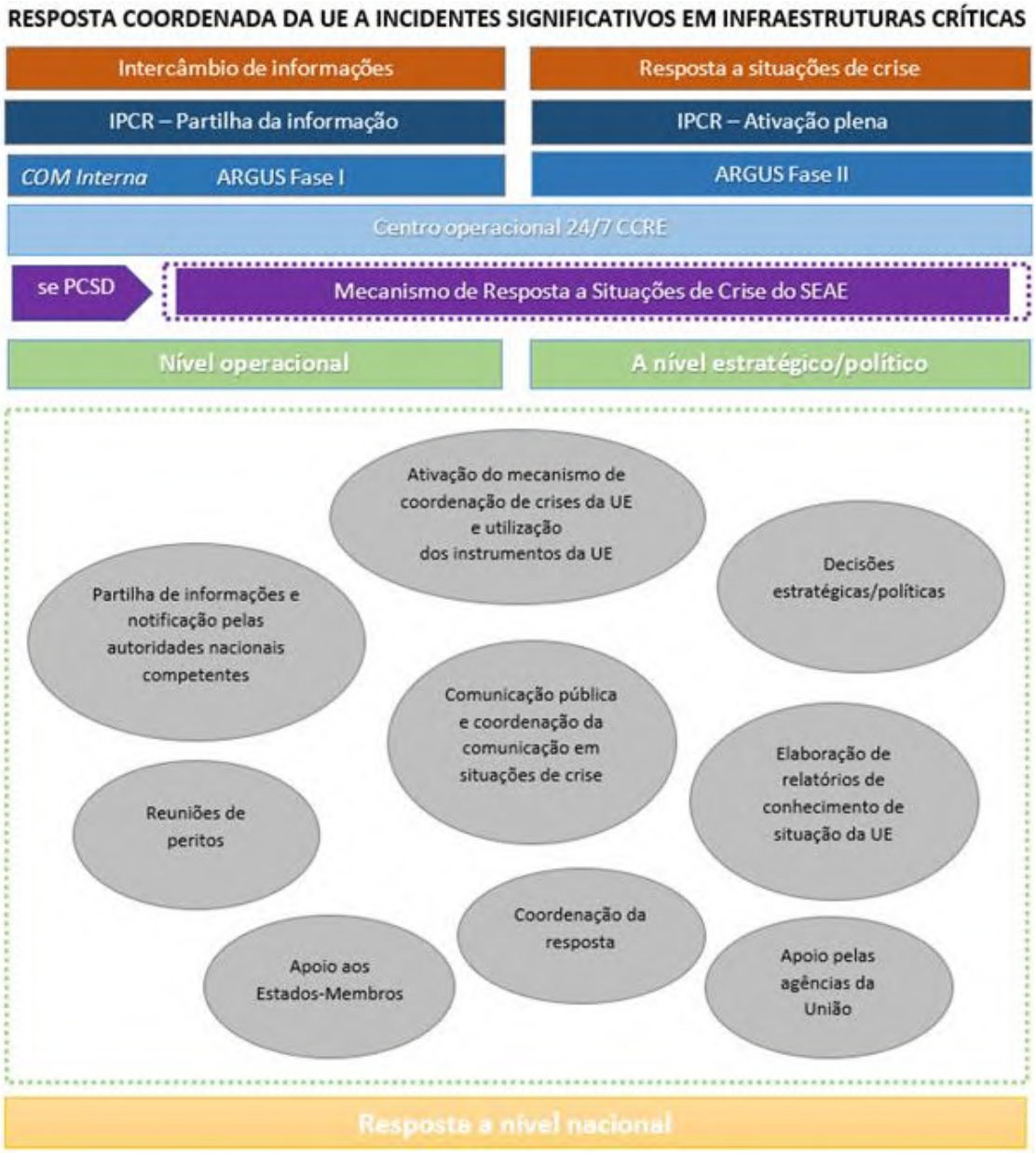

Gráfico 2: Decisão no quadro do Plano de Ação para as Infraestruturas Críticas