Conselho
da União Europeia

Bruxelas, 6 de junho de 2025
(OR. en)

9794/25

Dossiê interinstitucional:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	6 de junho de 2025
para:	Delegações
Assunto:	Recomendação do Conselho relativa a um plano de ação da UE para a gestão de cibercrises – Recomendação do Conselho aprovada pelo Conselho na sua reunião de 6 de junho de 2025

Junto se envia, à atenção das delegações, a recomendação do Conselho aprovada pelo Conselho na sua reunião de 6 de junho de 2025.

ANEXO

RECOMENDAÇÃO DO CONSELHO

relativa a um plano de ação da UE para a gestão de cibercrises

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) As tecnologias digitais e a conectividade mundial constituem a espinha dorsal do crescimento económico e da competitividade da União, bem como da transformação das suas infraestruturas críticas. No entanto, uma economia interligada e cada vez mais digital também aumenta o risco de incidentes de cibersegurança e ciberataques. Além disso, o recrudescimento das tensões geopolíticas, dos conflitos e da rivalidade estratégica reflete-se no impacto, no volume e na sofisticação das ciberatividades maliciosas. Essas atividades podem fazer parte de campanhas híbridas ou de operações militares. Podem também afetar diretamente a segurança, a economia e a sociedade da União. Além disso, podem ter um efeito de repercussão, especialmente quando visam países que são parceiros estratégicos internacionais, como os países candidatos ou os países vizinhos.

(2) Um incidente de cibersegurança em grande escala pode causar um nível de perturbação superior à capacidade de resposta de um Estado-Membro ou ter um impacto significativo em mais do que um Estado-Membro. Consoante a sua causa e o seu impacto, um incidente desse tipo poderá agravar-se e transformar-se numa verdadeira crise que impeça o correto funcionamento do mercado interno ou coloque graves riscos em termos de segurança pública para entidades ou cidadãos em vários Estados-Membros ou na totalidade da União. Uma gestão eficaz das crises é essencial para manter a estabilidade económica e proteger os governos, as infraestruturas críticas, as empresas e os cidadãos a nível europeu, bem como para apoiar a segurança e a estabilidade internacionais no ciberespaço. A gestão de cibercrises é, por conseguinte, parte integrante do quadro global de gestão de crises da UE.

(3) Atendendo às interdependências e interligações entre os ambientes TIC das entidades da União e os dos Estados-Membros, um incidente numa entidade da União pode representar um risco de cibersegurança para os Estados-Membros e vice-versa. A partilha de informações pertinentes e a coordenação no que respeita tanto a incidentes de cibersegurança em grande escala como a incidentes graves, tal como definidos no artigo 3.º, n.º 8, do Regulamento (UE, Euratom) 2023/2841[1], são cruciais no contexto do plano de ação da UE para a gestão de cibercrises («Plano de Ação para a Cibersegurança»).

[1] Regulamento (UE, Euratom) 2023/2841 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União, JO L, 2023/2841, 18.12.2023, p. 1.

(4) Caso ocorra uma crise em que seja acionado o Mecanismo Integrado da UE de Resposta Política a Situações de Crise («IPCR») nos termos da Decisão de Execução (UE) 2018/1993 do Conselho[2] («mecanismo IPCR»), o Plano de Ação para a Cibersegurança deverá respeitar plenamente o mecanismo IPCR no que toca à coordenação e à resposta. A coordenação política e estratégica far-se-á no âmbito do IPCR. O mecanismo IPCR é o instrumento de coordenação horizontal e de resposta a nível político da União. Nos termos do mecanismo IPCR, a decisão de ativar ou desativar o IPCR é tomada pela Presidência do Conselho da União Europeia. Os relatórios de conhecimento e análise integrados da situação («ISAA») elaborados pela Comissão e pelo Serviço Europeu para a Ação Externa («SEAE») apoiam os trabalhos do IPCR, tanto no modo de partilha de informações como no modo de ativação plena.

(5) Os Estados-Membros são os principais responsáveis pela gestão dos incidentes de cibersegurança e das cibercrises. Porém, a potencial natureza transfronteiriça e intersetorial dos incidentes de cibersegurança exige que os Estados-Membros e as entidades competentes da União cooperem a nível técnico, operacional e político tendo em vista uma coordenação eficaz em toda a União. Um ciclo de gestão de cibercrises completo inclui a preparação e o conhecimento situacional comum por forma a antecipar incidentes de cibersegurança em grande escala, as capacidades de deteção necessárias para identificar os instrumentos de resposta e recuperação necessários para atenuar e conter incidentes de cibersegurança em grande escala, bem como as capacidades de reação para dissuadir e evitar outros incidentes.

---

[2] 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.

(6) A Recomendação (UE) 2017/1584 da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala[3] estabelece os objetivos e as formas de cooperação entre os Estados-Membros e as entidades da União com vista a dar resposta a incidentes de cibersegurança em grande escala e a cibercrises. Identificou os intervenientes pertinentes a nível técnico, operacional e político e explicou de que forma se integravam nos mecanismos de gestão de crises existentes na União, como o mecanismo IPCR. Os princípios fundamentais estabelecidos na Recomendação (UE) 2017/1584 – nomeadamente a subsidiariedade, a complementaridade e a confidencialidade das informações, bem como a abordagem de três níveis (técnico, operacional e político) – permanecem válidos. A presente recomendação assenta nesses princípios fundamentais e destina-se a substituir a Recomendação (UE) 2017/1584, estabelecendo um novo quadro da União para a gestão de crises de cibersegurança.

(7) Algumas definições utilizadas na presente recomendação baseiam-se nas definições e termos utilizados na Diretiva (UE) 2022/2555[4]. No entanto, o âmbito de aplicação da presente recomendação difere do âmbito de aplicação da Diretiva (UE) 2022/2555. A presente recomendação estabelece o quadro da União para a gestão de cibercrises no contexto da preparação geral da UE para incidentes de cibersegurança em grande escala e cibercrises decorrentes desses incidentes – independentemente da entidade ou setor afetados. Na medida do possível, as definições baseiam-se nas que constam da Diretiva (UE) 2022/2555.

---

3 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.

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 (Diretiva SRI 2), JO L 333 de 27.12.2022, p. 80.

(8) É necessário um Plano de Ação para a Cibersegurança atualizado para que sejam fornecidas orientações claras e acessíveis que expliquem em que consiste um incidente de cibersegurança em grande escala ou uma cibercrise a nível da União, como é acionado o quadro de gestão de crises e quais são as funções das redes, dos intervenientes e dos mecanismos pertinentes a nível da União e qual é a interação entre estes intervenientes e mecanismos ao longo de todo o período de duração da cibercrise. O Plano de Ação para a Cibersegurança visa apoiar o quadro mais alargado das relações entre civis e militares no contexto da gestão de cibercrises, tendo ainda como pano de fundo o aprofundamento das relações entre a UE e a OTAN, sempre que possível através de mecanismos de partilha de informações reforçados, inclusivos, de natureza recíproca e não discriminatória, no domínio da gestão de cibercrises.

(9) Importa reforçar a gestão intersetorial de crises a nível da União, a fim de permitir uma resposta integrada a situações de crise, em especial nos casos em que as crises e os incidentes de cibersegurança em grande escala tenham consequências físicas. A presente recomendação complementa o mecanismo IPCR e outros mecanismos de gestão de crises da União, incluindo o sistema geral de alerta rápido ARGUS da Comissão, o Mecanismo de Proteção Civil da União («MPCU»), apoiado pelo Centro de Coordenação de Resposta de Emergência («CCRE») criado ao abrigo do MPCU pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho relativa a um Mecanismo de Proteção Civil da União Europeia[5] («Decisão MPCU»), o mecanismo de resposta a situações de crise («CRM») do SEAE, além de outros processos, como os descritos no conjunto de instrumentos de ciberdiplomacia da UE[6], no conjunto de instrumentos da UE contra as ameaças híbridas[7] e no protocolo revisto da UE para a luta contra as ameaças híbridas[8]. Além disso, complementa e deverá ser coerente com a Recomendação (UE) 2024/4371 do Conselho sobre um plano de ação para a coordenação da resposta a nível da União a perturbações em infraestruturas críticas com importante relevância transfronteiriça[9] («Plano de Ação da UE para as Infraestruturas Críticas»), que abrange a resiliência de aspetos físicos não cibernéticos e que visa melhorar a coordenação da resposta a nível da União neste domínio.

---

5 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.

6 Conclusões do Conselho sobre um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas (9916/17).

7 Conclusões do Conselho sobre um enquadramento para uma resposta coordenada da UE às campanhas híbridas, de 22 de junho de 2022.

8 Documento de trabalho conjunto dos serviços da Comissão – *EU Protocol for countering hybrid threats* [Protocolo da UE para a luta contra as ameaças híbridas], SWD(2023) 116 final.

9 JO C, C/2024/4371, 5.7.2024.

(10) A Rede Europeia de Organizações de Coordenação de Cibercrises («UE-CyCLONe») é a rede para a coordenação da gestão a nível operacional de crises e de incidentes de cibersegurança em grande escala, inclusivamente no caso de crises e de incidentes de cibersegurança em grande escala intersetoriais. Para não tornar os quadros existentes ainda mais complicados, deverá evitar-se a criação de estruturas setoriais que dupliquem as funções da UE-CyCLONe. A UE-CyCLONe também deverá receber dos diferentes setores informações operacionais relacionadas com a cibersegurança e transmiti-las ao nível político.

(11) Os Estados-Membros são incentivados a utilizar plenamente os recursos financeiros disponíveis para a cibersegurança previstos nos programas pertinentes da União. Importa assegurar que estes programas imponham encargos administrativos mínimos aos candidatos ao financiamento e que a participação dos Estados-Membros nestes programas seja facilitada graças ao fornecimento de orientações pertinentes sobre as opções de apoio financeiro viáveis.

(12) A presente recomendação contribui para ações de preparação de âmbito mais vasto, de que a União necessita para fazer face a crises intersetoriais, em conformidade com os princípios inscritos na Estratégia Europeia para uma União da Preparação, a saber, uma abordagem integrada que englobe todos os riscos, toda a governação e toda a sociedade, em especial no que respeita ao reforço da sensibilização para os riscos e as ameaças e a uma resposta intersetorial às crises,

ADOTOU A PRESENTE RECOMENDAÇÃO:

I: Objetivo, âmbito e princípios orientadores do quadro de gestão de cibercrises da UE

Objetivo e âmbito

1. A presente Recomendação relativa a um plano de ação da UE para a gestão de cibercrises («Plano de Ação para a Cibersegurança») define o quadro da União para a gestão de cibercrises no âmbito da preparação geral da UE face a incidentes de cibersegurança em grande escala e a cibercrises. O quadro reflete o papel que incumbe tanto aos Estados-Membros como às instituições, órgãos e organismos da União («entidades da União») no âmbito das respetivas competências, no pleno respeito das legislações nacionais e das regras internas, a fim de assegurar uma ação global e coordenada a nível da União.

2. O Plano de Ação para a Cibersegurança deverá ser aplicado em consonância com o Plano de Ação da UE para as Infraestruturas Críticas, em especial em caso de incidentes que afetem a resiliência física e a cibersegurança de infraestruturas críticas[10].

3. O Plano de Ação para a Cibersegurança fornece orientações para a resposta a incidentes de cibersegurança em grande escala ou cibercrises e a sua utilização deverá ser complementar a quaisquer mecanismos de resposta setoriais pertinentes, como os enumerados no anexo II. As partes interessadas relevantes no domínio da cibersegurança deverão ajudar e apoiar a consecução dos objetivos desses mecanismos setoriais, tanto a nível nacional como a nível da União.

4. Na eventualidade de uma crise intersetorial a nível da União que envolva aspetos cibernéticos e para a qual o IPCR seja acionado, a coordenação da resposta a nível político da União deverá ser assegurada pelo Conselho, recorrendo ao mecanismo IPCR. Sempre que o IPCR seja acionado, as medidas no âmbito do Plano de Ação para a Cibersegurança deverão apoiar a resposta da UE a nível político, fornecendo apoio específico no domínio da cibersegurança.

---

[10] A parte I, ponto 4, do anexo do Plano de Ação da UE para as Infraestruturas Críticas descreve mais pormenorizadamente a coordenação nesses casos.

Princípios orientadores

5. Os princípios orientadores a seguir indicados aplicam-se à gestão de cibercrises a nível da União:

a) *Proporcionalidade*: a maioria dos incidentes de cibersegurança que afetam os Estados-Membros tem uma dimensão inferior ao que se pode considerado um incidente de cibersegurança em grande escala ou uma cibercrise a nível nacional ou da União. Em caso de incidentes e ameaças de cibersegurança, os Estados-Membros cooperam e trocam informações, numa base voluntária e regular, no âmbito da rede de equipas de resposta a incidentes de segurança informática («rede de CSIRT») e da UE-CyCLONe, em conformidade com as Instruções Permanentes das redes.

b) *Subsidiariedade*: os Estados-Membros são os principais responsáveis por responder à situação e remediá-la caso sejam afetados por um incidente de cibersegurança, um incidente de cibersegurança em grande escala ou uma cibercrise. Tendo em conta os potenciais efeitos transfronteiriços, o Conselho, a Comissão, o alto representante, a Agência da União Europeia para a Cibersegurança («ENISA»), o Serviço de Cibersegurança para as Instituições, Órgãos e Organismos da União («CERT-UE»), a Europol e todas as outras entidades competentes da União deverão cooperar ao longo de todo o ciclo de uma crise. Este papel deriva do direito da União e reflete a forma como os incidentes de cibersegurança em grande escala e as cibercrises afetam um ou mais setores da atividade económica no âmbito do mercado único, a segurança e as relações internacionais da União, bem como as próprias entidades da União.

c) *Complementaridade*: a presente recomendação tem plenamente em conta os atuais mecanismos de gestão de crises a nível da União enumerados no anexo II, em especial, o mecanismo IPCR, o ARGUS e o CRM do SEAE. A presente recomendação tem em conta os mandatos da rede de CSIRT e da UE-CyCLONe, bem como o Regulamento (UE, Euratom) 2023/2841. Nos casos em que o IPCR seja acionado, o trabalho das redes, entidades e mecanismo setoriais ativados deverá prosseguir e deverá contribuir para a coordenação política e estratégica levada a cabo no âmbito do IPCR e apoiá-la.

d) *Confidencialidade das informações*: todos os intercâmbios de informações no contexto da presente recomendação deverão cumprir as regras aplicáveis em matéria de segurança e de proteção de dados pessoais. Sempre que adequado, deverão ser tidos em conta os acordos de não divulgação informais, como o protocolo «sinalização luminosa» para a classificação de informações sensíveis. Para o intercâmbio de informações classificadas, independentemente do sistema de classificação aplicado, deverá recorrer-se às regras e aos acordos vinculativos em vigor em matéria de tratamento de informações classificadas, bem como às ferramentas acreditadas e disponíveis.

6. Em conformidade com os princípios orientadores acima indicados, os Estados-Membros e as entidades da União deverão aprofundar a sua cooperação em matéria de gestão de cibercrises, promovendo a confiança mútua e tirando partido das redes e dos mecanismos existentes. Essa cooperação, inserida no quadro do Plano de Ação para a Cibersegurança, beneficia da aplicação dos artigos 22.º e 23.º do Regulamento (UE, Euratom) 2023/2841. Em particular, o plano de gestão de cibercrises estabelecido com base no artigo 23.º do Regulamento (UE, Euratom) 2023/2841 contribui, entre outras coisas, para o intercâmbio regular de informações pertinentes entre as entidades da União e com os Estados-Membros e define disposições relativas à coordenação e ao fluxo de informações entre as entidades da União.

II: Definições

7. Para efeitos do Plano de Ação para a Cibersegurança, entende-se por:

a) «Incidente», 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;

b) «Incidente significativo», um incidente que:

   a. Tiver causado ou for suscetível de causar graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa;

   b. Tiver afetado ou for suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis;

c) «Incidente de cibersegurança em grande escala», um incidente que cause um nível de perturbação superior à capacidade de resposta de um Estado-Membro ou que tenha um impacto significativo em, pelo menos, dois Estados-Membros;

d) «Cibercrise», um incidente de cibersegurança em grande escala que se agrava e se transforma numa verdadeira crise que impede o correto funcionamento do mercado interno ou coloca graves riscos em termos de segurança pública para entidades ou cidadãos em vários Estados-Membros ou na totalidade da União.

III: Estruturas e responsabilidades nacionais na gestão de cibercrises

8. Os Estados-Membros são os principais responsáveis pela resposta a incidentes de cibersegurança em grande escala ou a cibercrises que os afetem. Cada Estado-Membro, em conformidade com a Diretiva (UE) 2022/2555, tem uma ou mais autoridades de gestão de cibercrises e uma ou mais CSIRT.

9. Com a adoção da Diretiva (UE) 2022/2555 e de outros instrumentos legislativos e não legislativos em matéria de cibersegurança, os Estados-Membros têm vindo a harmonizar os seus quadros de cibersegurança, estabelecendo regras mínimas relativas ao funcionamento do quadro regulamentar coordenado, criando mecanismos para uma cooperação eficaz entre as autoridades responsáveis em cada Estado-Membro e prevendo vias de recurso e medidas de execução eficazes que são fundamentais para o cumprimento efetivo dessas obrigações.

10. De acordo com o artigo 9.º, n.º 4, da Diretiva (UE) 2022/2555, os Estados-Membros devem adotar planos nacionais de resposta a crises e a incidentes de cibersegurança em grande escala. Esses planos incluem, nomeadamente, medidas nacionais de preparação, procedimentos de gestão de cibercrises, procedimentos nacionais e acordos entre as autoridades e os organismos nacionais para assegurar o apoio dos Estados-Membros e a sua participação efetiva na gestão coordenada de incidentes de cibersegurança em grande escala e de cibercrises a nível da União. Os procedimentos de gestão de cibercrises incluem também disposições sobre a sua integração no quadro geral de gestão de crises e canais de intercâmbio de informações.

11. De acordo com o artigo 9.º, n.º 1, da Diretiva (UE) 2022/2555, os Estados-Membros devem assegurar a coerência com os quadros existentes de gestão geral de crises a nível nacional. Em caso de ativação do IPCR, as autoridades nacionais de gestão de crises deverão, para efeitos de informação ao IPCR, recolher contributos das autoridades de gestão de cibercrises e dos mecanismos setoriais de crise a nível nacional.

12. De acordo com o artigo 9.º, n.º 5, da Diretiva (UE) 2022/2555, a UE-CyCLONe, mediante solicitação de um Estado-Membro interessado, deverá trocar informações sobre partes pertinentes dos planos nacionais de resposta a crises e incidentes de cibersegurança em grande escala, em especial sobre as disposições que visam assegurar o apoio dos Estados-Membros e a sua participação efetiva na gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível da União, a fim de proceder ao intercâmbio de boas práticas e refletir sobre a exequibilidade do quadro geral.

13. A UE-CyCLONe e o Conselho Interinstitucional para a Cibersegurança («IICB») são convidados a trocar opiniões, sempre que adequado, sobre a coerência do plano de gestão de crises elaborado pelo IICB em conformidade com o artigo 23.º do Regulamento (UE, Euratom) 2023/2841 com os planos nacionais de resposta a crises e incidentes de cibersegurança em grande escala.

14. A UE-CyCLONe, com o apoio da ENISA, que assegura os seus serviços de secretariado, deverá manter atualizada a lista das autoridades nacionais de gestão de cibercrises, com os contactos dos agentes e dos executivos da UE-CyCLONe, e disponibilizá-la aos seus membros.

IV: Principais redes e intervenientes no ecossistema de gestão de cibercrises da UE

15. A rede de CSIRT é a principal rede técnica para o intercâmbio de informações importantes sobre incidentes, em especial no âmbito de aplicação da presente recomendação, de acordo com as funções pertinentes descritas no artigo 15.º, n.º 3, da Diretiva (UE) 2022/2555. Contribui para o desenvolvimento da confiança e promove uma cooperação operacional célere e eficaz entre os Estados-Membros. O presidente da rede de CSIRT pode participar no IICB na qualidade de observador.

16. O CERT-UE é o serviço de cibersegurança para todas as entidades da União. O CERT-UE atua como plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes, em conformidade com o artigo 13.º do Regulamento (UE) 2023/2841. O CERT-UE é membro da rede de CSIRT e apoia a Comissão no âmbito da UE-CyCLONe. O CERT-UE opera a nível técnico e tem a responsabilidade de coordenar a gestão de incidentes graves que afetem entidades da União.

17. A UE-CyCLONe funciona como intermediária entre os níveis técnico e político, em especial durante incidentes de cibersegurança em grande escala e cibercrises. Apoia a gestão coordenada de incidentes de cibersegurança em grande escala e cibercrises a nível operacional e assegura o intercâmbio regular de informações pertinentes entre os Estados-Membros e as instituições, órgãos e organismos da União, em conformidade com o artigo 16.º da Diretiva (UE) 2022/2555. O presidente da UE-CyCLONe pode participar no IICB na qualidade de observador.

18. A ENISA é a agência da União incumbida de exercer as atribuições que lhe são conferidas ao abrigo do Regulamento (UE) 2019/881[11] com o objetivo de alcançar um elevado nível comum de cibersegurança na União, nomeadamente apoiando ativamente os Estados-Membros e as instituições, órgãos e organismos da União. A ENISA assegura, entre outros, os serviços de secretariado da rede de CSIRT e da UE-CyCLONe, serviços de conhecimento situacional e presta assistência aos Estados-Membros, organizando regularmente exercícios de cibersegurança a nível da União. Nos termos da Diretiva (UE) 2022/2555 e do Regulamento (UE) 2024/2847[12], a ENISA recebe informações sobre incidentes transfronteiriços significativos, vulnerabilidades ativamente exploradas e incidentes que afetem produtos digitais.

19. O Conselho da União Europeia («o Conselho») é a instituição com funções de definição das políticas e de coordenação, nos termos do artigo 16.º do Tratado da União Europeia («TUE»), e é o responsável pelo IPCR que diz respeito à coordenação e à resposta a nível político da União. O Conselho atua através das formações do Conselho, do Comité de Representantes Permanentes e das instâncias preparatórias do Conselho, nomeadamente o Grupo Horizontal das Questões do Ciberespaço, bem como, se for caso disso, do mecanismo IPCR.

---

[11] 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.

[12] Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência), JO L, 2024/2847, 20.11.2024, p. 1.

20. A Comissão, enquanto instituição que promove o interesse geral da União que toma as iniciativas adequadas para esse efeito e que assegura a aplicação dos Tratados e das medidas adotadas pelas instituições por força do artigo 17.º do TUE, é responsável por determinadas ações gerais de preparação a nível da União e por determinadas ações que visem o conhecimento situacional, incluindo a gestão do CCRE e do Sistema Comum de Comunicação e de Informação de Emergência («CECIS»), em conformidade com a Decisão MPCU. Contribui para a coerência e a coordenação entre ações conexas a nível operacional empreendidas à escala da União para dar resposta a situações crises. A Comissão é consultada sobre as decisões de ativação ou desativação do IPCR, e os seus serviços elaboram, juntamente com o SEAE, os relatórios ISAA. É membro da UE-CyCLONe, nos casos em que um incidente de cibersegurança em grande escala, potencial ou em curso, tenha ou seja suscetível de ter um impacto significativo nos serviços e atividades abrangidos pelo âmbito de aplicação da Diretiva (UE) 2022/2555 e participa na qualidade de observadora nos outros casos. É o ponto de contacto entre o IICB e a UE-CyCLONe. Participa na rede de CSIRT na qualidade de observadora.

21. O alto representante da União para os Negócios Estrangeiros e a Política de Segurança («alto representante»), assistido pelo SEAE, conduz a política externa e de segurança comum da União e contribui com as suas propostas para a elaboração dessa política, nomeadamente a política comum de segurança e defesa («PCSD»). Tal inclui estruturas e mecanismos diplomáticos, de informação e militares, designadamente a Capacidade Única de Análise de Informações («SIAC»), enquanto ponto de entrada único para os serviços de informação dos Estados-Membros, o Estado-Maior da União Europeia («EMUE»), enquanto fonte de competência militar, o conjunto de instrumentos de ciberdiplomacia da UE, bem como a rede de delegações da UE, que podem contribuir para a gestão de crises a partir de uma dimensão externa. O SEAE elabora, juntamente com a Comissão, os relatórios ISAA.

22. O anexo II descreve as funções e as competências dos intervenientes pertinentes a nível da União relativamente à gestão de cibercrises, incluindo as principais redes e intervenientes.

V: Preparação para incidentes de cibersegurança em grande escala e para uma cibercrise

Panorama das ameaças

23. Os Estados-Membros e as entidades pertinentes da União deverão tomar as medidas necessárias para melhorar o conhecimento situacional, reconhecendo que o panorama das ameaças e o conhecimento situacional específico de cada incidente exigem modos de operação distintos. Os Estados-Membros e as entidades pertinentes da União deverão trabalhar em conjunto com base em dados verificados e fiáveis que incluam as tendências em matéria de incidentes, táticas, técnicas e procedimentos, bem como as vulnerabilidades ativamente exploradas.

24. Ao partilharem informações classificadas a nível da UE, os Estados-Membros deverão utilizar plenamente as plataformas de cooperação técnica e operacional existentes, como as utilizadas pela rede de CSIRT e pela UE-CyCLONe.

25. A fim de melhorar o conhecimento situacional comum e facilitar a avaliação do impacto na UE, a UE-CyCLONe e a rede de CSIRT, com o apoio da ENISA, deverão utilizar o mecanismo de comunicação acordado internamente para traçar uma panorâmica a nível da UE das atividades técnicas e operacionais com base nas informações recolhidas a nível nacional.

26. A UE-CyCLONe e a rede de CSIRT deverão:

    a) Cooperar para melhorar a partilha de informações entre o nível técnico e o nível operacional e o conhecimento situacional no seu conjunto;

    b) Continuar a desenvolver um clima de confiança entre os seus membros e entre as redes;

    c) Utilizar plenamente as ferramentas disponíveis para a partilha de informações, com o apoio da ENISA, refletir sobre a forma de melhorar essas ferramentas e assegurar a interoperabilidade entre as redes.

27. A UE-CyCLONe, a rede de CSIRT e o IICB deverão cooperar de modo a assegurar um intercâmbio efetivo de informações pertinentes.

28. A ENISA, na qualidade de secretariado da rede de CSIRT e da UE-CyCLONe, tem um papel central de apoio aos Estados-Membros e às instituições, órgãos e organismos da União com vista a obter um conhecimento situacional comum da UE a nível técnico e operacional para apoiar a preparação para crises e incidentes de cibersegurança em grande escala.

29. Segundo a Diretiva (UE) 2022/2555 e o Regulamento (UE) 2019/881, os Estados-Membros e as entidades competentes da União deverão coordenar-se com o setor privado, incluindo comunidades de *software* aberto e fabricantes, a fim de melhorar a partilha de informações. A ENISA, em particular, deverá utilizar o seu programa de parcerias para o efeito. Além disso, os Estados-Membros e as entidades competentes da União poderão também basear-se nos centros de partilha e análise de informações («ISAC») existentes a nível nacional e da UE, a fim de reforçar a capacidade de cibersegurança e responder a incidentes de cibersegurança, nomeadamente através de reuniões conjuntas entre o setor privado e a UE-CyCLONe ou a rede de CSIRT.

30. A fim de aumentar a partilha de informações no seio das redes e entre elas, e de clarificar as expectativas recíprocas para essa partilha, a UE-CyCLONe deverá, com o apoio da ENISA na qualidade de secretariado e após consultar a rede de CSIRT e o grupo de cooperação SRI, chegar a acordo, no prazo de 24 meses a contar da data de adoção da presente recomendação, sobre uma taxonomia comum harmonizada a respeito dos níveis de gravidade dos incidentes. Esta taxonomia deverá permitir comparar a gravidade dos incidentes ocorridos nos diferentes Estados-Membros, tendo em conta o impacto na prestação de serviços, o número de entidades afetadas e o seu grau de relevância, o impacto em outros serviços e infraestruturas, bem como os danos financeiros, de reputação e políticos causados. Deverá basear-se em classificações ou taxonomias relevantes já disponíveis, como a «*Reference Incident Classification Taxonomy*» [Taxonomia de Referência para a Classificação de Incidentes].

Nível técnico

31. A rede de CSIRT é a plataforma para a cooperação técnica e a partilha de informações entre todos os Estados-Membros e, através da CERT-UE, com as entidades da União.

32. Nos termos da Diretiva (UE) 2022/2555, cada CSIRT tem a função de monitorizar e analisar ciberameaças, vulnerabilidades e incidentes a nível nacional. As CSIRT deverão trocar, tanto a nível da rede de CSIRT como a nível bilateral, informações pertinentes sobre incidentes, quase incidentes, ciberameaças, riscos e vulnerabilidades, a fim de obter um conhecimento situacional comum.

33. A fim de reforçar a cooperação operacional a nível da União, a rede de CSIRT deverá ponderar a possibilidade de convidar os organismos e as agências da União implicados na política de cibersegurança, como a Europol, a participar nos seus trabalhos.

34. Nos termos do Regulamento 2023/2841, a CERT-UE deverá recolher, gerir, analisar e partilhar com as instituições, órgãos e organismos da União as informações sobre as ciberameaças, as vulnerabilidades e os incidentes relativos à infraestrutura de TIC não classificada e, quando necessário, deverá emitir propostas ao IICB com vista à adoção de orientações e recomendações dirigidas às instituições, órgãos e organismos da União. A CERT-UE deverá cooperar e trocar informações com as contrapartes dos Estados-Membros, inclusive por meio da rede de CSIRT.

Nível operacional

35. Nos termos da Diretiva (UE) 2022/2555, a UE-CyCLONe deverá servir de plataforma para a cooperação entre as autoridades dos Estados-Membros responsáveis pela gestão de cibercrises e, através da Comissão, com as entidades competentes da União, com o objetivo de aumentar o nível de preparação para a gestão de incidentes de cibersegurança em grande escala e de cibercrises e de desenvolver um conhecimento situacional comum relativo a incidentes de cibersegurança em grande escala e cibercrises.

36. Nos termos da Diretiva (UE) 2022/2555 e do Regulamento (UE) 2024/2847, a ENISA recebe informações sobre incidentes transfronteiriços significativos, vulnerabilidades ativamente exploradas e incidentes que afetem produtos digitais. A ENISA, no exercício das suas funções de secretariado, deverá aconselhar a rede de CSIRT e a UE-CyCLONe com o objetivo de apoiar as redes na determinação da eventual necessidade de tomar mais medidas e de contribuir para o conhecimento situacional comum.

Nível político

37. Os Estados-Membros e as entidades competentes da União deverão acompanhar a evolução dos acontecimentos internacionais que afetem a cibersegurança (incluindo ciberameaças, ameaças híbridas e a manipulação da informação e ingerência por parte de agentes estrangeiros («FIMI»), bem como a desinformação, se for caso disso). Deverão ser tidas em conta iniciativas como os relatórios sobre a situação técnica da cibersegurança, as análises fornecidas pelo SIAC e outras iniciativas pertinentes que proporcionem uma visão especializada.

38. O alto representante deverá continuar a informar os Estados-Membros e a chamá-los a participarem nos esforços diplomáticos da União relacionados com as ciberameaças, em especial as que envolvem intervenientes estatais, no seu diálogo com países terceiros e organizações internacionais, incluindo a OTAN, e na aplicação de medidas diplomáticas, incluindo medidas restritivas.

39. A Presidência do Conselho da União Europeia pode criar uma página de acompanhamento na plataforma Web do IPCR, onde os Estados-Membros e as instituições e organismos da UE poderão trocar informações sobre uma potencial crise que esteja a emergir.

Exercícios comuns

40. A Comissão, em coordenação com o alto representante, apoiada pela ENISA e depois de consultar a UE-CyCLONe e a rede de CSIRT, deverá elaborar um programa anual evolutivo e eficaz de exercícios cibernéticos visando a preparação para cibercrises e o reforço da eficiência organizacional. O programa evolutivo de exercícios deverá ter em conta os exercícios do MPCU, bem como outros exercícios de mecanismos a nível da União de resposta a situações de crise, incluindo o exercício previsto no Plano de Ação da UE para as Infraestruturas Críticas. O primeiro programa evolutivo deverá ser elaborado no prazo de 12 meses a contar da data de adoção do Plano de Ação para a Cibersegurança, devendo os programas subsequentes estar concluídos até 31 de março de cada ano. O programa evolutivo deverá ser enviado ao Conselho a título informativo.

41. O programa evolutivo deverá abranger também exercícios concebidos com base nos cenários resultantes das avaliações de risco coordenadas a nível da UE. Deverá abranger exercícios que contem com a participação de todos os intervenientes pertinentes, em especial o setor privado e a OTAN.

42. A ENISA, no exercício das suas funções de secretariado da rede de CSIRT e da UE-CyCLONe, deverá assegurar a recolha sistemática dos ensinamentos retirados dos exercícios, bem como identificar e propor formas de pôr em prática as ações que deles resultem, a fim de garantir que sejam efetivamente executadas e tenham um impacto positivo sobre a resiliência comum da UE, incluindo as respetivas Instruções Permanentes.

43. Todos os intervenientes e todas as redes deverão melhorar a coordenação no caso de um incidente de cibersegurança em grande escala ou de uma cibercrise com base nos ensinamentos retirados dos exercícios. Em particular, a UE-CyCLONe e a rede de CSIRT deverão analisar os desafios identificados durante os exercícios, em especial os que dizem respeito à cooperação entre as redes, de modo a melhorar a coordenação e, se necessário, adaptar rapidamente as Instruções Permanentes.

44. O Grupo de cooperação SRI deverá convidar a rede de CSIRT, a UE-CyCLONe e a ENISA a apresentarem os ensinamentos retirados dos exercícios, bem como a identificarem as medidas a aplicar que deles resultem e a forma proposta para as pôr em prática.

45. O Conselho pode convidar os presidentes da rede de CSIRT, da UE-CyCLONe, do grupo de cooperação SRI e da ENISA a apresentarem a forma como os ensinamentos retirados dos exercícios foram aplicados.

46. A ENISA, em cooperação com a Comissão e o alto representante, é convidada a organizar um exercício para testar o Plano de Ação para a Cibersegurança no âmbito do próximo exercício CiberEuropa. O exercício deverá contar com a participação de todos os intervenientes pertinentes, incluindo os do nível político. A ENISA é convidada a coordenar com a Presidência do Conselho da União Europeia a participação do nível político. O exercício pode também incluir o setor privado e a OTAN.

VI: Deteção de incidentes suscetíveis de se transformarem em incidentes de cibersegurança em grande escala ou em cibercrises

47. De acordo com os respetivos mandatos e com base na abordagem multirriscos, todos os intervenientes deverão contribuir para as redes pertinentes com informações que indiciem um potencial incidente de cibersegurança em grande escala ou uma cibercrise.

48. Nos termos do Regulamento (UE) 2025/38[13], caso obtenham informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, as plataformas de cibersegurança transfronteiriças deverão assegurar, sem demora injustificada, para efeitos de conhecimento situacional comum, que são prestadas informações pertinentes às autoridades dos Estados-Membros e à Comissão através da UE-CyCLONe e da rede de CSIRT.

[13] Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho, de 19 de dezembro de 2024, que cria medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ciberameaças e incidentes de cibersegurança e que altera o Regulamento (UE) 2021/694 (Regulamento de Cibersolidariedade), JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

49. Sempre que se constate a ocorrência de um incidente significativo, em especial um que cause um impacto imediato, este poderá ser notificado a uma CSIRT ou detetado por uma CSIRT, bem como pelas autoridades dos Estados-Membros responsáveis pela gestão de cibercrises ou por outras autoridades setoriais. Os Estados-Membros são incentivados a partilhar as informações referentes a um incidente deste tipo nas redes, que deverão equacionar a adoção de medidas adequadas. A ativação da rede de CSIRT e da UE-CyCLONe, pode ocorrer de forma independente, em função da natureza do incidente e da resposta necessária. No entanto, estas duas redes são incentivadas a dar continuidade à cooperação mútua com base em disposições processuais acordadas. A decisão de proceder à ativação é da competência exclusiva de cada uma das redes e é tomada de forma independente.

50. A rede de CSIRT deverá aconselhar a UE-CyCLONe quanto à possibilidade de um incidente de cibersegurança detetado ser considerado um incidente de cibersegurança em grande escala, potencial ou em curso.

51. Conforme previsto na Diretiva (UE) 2022/2555, a rede de CSIRT e a UE-CyCLONe deverão estabelecer, sem demora, disposições processuais aplicáveis em caso de incidente de cibersegurança em grande escala, potencial ou em curso, a fim de assegurar a coordenação técnico-operacional e a disponibilização de informações atempadas e pertinentes ao nível político.

VII: Resposta a um incidente de cibersegurança em larga escala ou cibercrise a nível da União

Resposta a um incidente de cibersegurança em larga escala ou cibercrise em que o IPCR não seja acionado em modo de ativação plena

52. A resposta eficaz a incidentes de cibersegurança em larga escala ou cibercrises a nível da União depende de uma cooperação técnica, operacional e política eficaz que adote uma abordagem de governação integrada, incluindo, sempre que possível, as forças policiais.

53. Em cada nível, os intervenientes envolvidos deverão tomar medidas específicas com vista a obter um conhecimento situacional comum e uma resposta coordenada. Essas medidas devem assegurar a difusão ordenada e eficaz de informação.

54. A resposta deverá ser adequada ao impacto do incidente de cibersegurança em grande escala ou da cibercrise. De acordo com a Diretiva (UE) 2022/2555, as autoridades dos Estados-Membros responsáveis pela gestão de cibercrises deverão assegurar a coerência e a coordenação a nível nacional entre as respostas setoriais à cibercrise.

55. Em caso de incidente de cibersegurança em grande escala ou de cibercrise, todos os intervenientes e redes deverão reagir em estreita coordenação da seguinte forma:

a) A nível técnico:

i. Os Estados-Membros afetados e as suas CSIRT deverão cooperar com as entidades afetadas para dar resposta aos incidentes e prestar assistência, se for caso disso;

ii. As CSIRT deverão cooperar através da rede de CSIRT para partilhar informações técnicas relevantes sobre o incidente; as CSIRT cooperam nos seus esforços para analisar os artefactos técnicos disponíveis e outras informações técnicas relacionadas com o incidente, com vista a determinar a causa e possíveis medidas técnicas de atenuação;

iii. As CSIRT ou as autoridades de gestão de cibercrises de um Estado-Membro são incentivadas a partilhar na rede de CSIRT ou na UE-CyCLONe o conhecimento de um incidente significativo, assim que tiverem acesso a essa informação.

iv. A rede de CSIRT, com o apoio da ENISA, deverá fazer a compilação dos relatórios nacionais fornecidos pelas CSIRT, que deverá ser apresentada à UE-CyCLONe;

v. Se um incidente de cibersegurança tiver o potencial de se transformar num incidente de cibersegurança em grande escala ou numa cibercrise, a rede de CSIRT deverá partilhar as informações pertinentes com a UE-CyCLONe. A UE-CyCLONe deverá servir-se dessa informação para informar o Conselho;

vi. A rede de CSIRT deverá manter-se em estreito contacto com a Europol a fim de assegurar o intercâmbio de informações técnicas pertinentes. A rede de CSIRT e a Europol deverão estabelecer pontos de contacto para reforçar a partilha de informações, quando pertinente, em caso de incidente de cibersegurança em grande escala;

b) A nível operacional:

i. Os Estados-Membros deverão atenuar o impacto do incidente a nível nacional recorrendo a medidas adequadas;

ii. A rede de CSIRT deverá fornecer à UE-CyCLONe avaliações técnicas dos incidentes em curso que a UE-CyCLONe possa utilizar;

iii. A UE-CyCLONe deverá avaliar as consequências e o impacto dos incidentes de cibersegurança em grade escala ou das cibercrises relevantes, e propor possíveis medidas de atenuação, apoiar a gestão coordenada de incidentes de cibersegurança em grande escala ou cibercrises, e apoiar a tomada de decisão a nível político;

iv. Se um incidente de cibersegurança em grande escala e com impacto intersetorial exigir a ativação de medidas de resposta a nível da União, em especial a ativação dos mecanismos horizontais e setoriais de gestão de crises pertinentes a nível da União enumerados no anexo II,

a) os intervenientes com essa competência podem, em função do tipo de mecanismos setoriais de gestão de crises a nível da União, solicitar a ativação do referido mecanismo;

b) caso um mecanismo setorial desse tipo seja ativado, as entidades competentes apoiam as entidades setoriais na atenuação do impacto do incidente;

c) a Comissão deverá facilitar o fluxo das informações necessárias entre os pontos de contacto dos mecanismos horizontais e setoriais de gestão de crises pertinentes a nível da União, enumerados no anexo II, e a UE-CyCLONe, e deverá proceder a uma análise intersetorial integrada e propor opções para um plano de resposta integrado e adequado à situação;

d) a Comissão, por intermédio da UE-CyCLONe, quando pertinente, e em cooperação com o alto representante, deverá assegurar a coerência e a coordenação entre as medidas operacionais a nível da UE no domínio cibernético e as ações de resposta conexas a nível da União, em especial no que respeita aos pedidos de assistência realizados através do MPCU;

e) caso tenha sido criada uma página de acompanhamento do IPCR, as informações sobre o incidente, os seus impactos e as medidas tomadas deverão também ser partilhadas com os Estados-Membros e as entidades da União através da plataforma Web do IPCR;

v. Os Estados-Membros podem solicitar os serviços da Reserva de Cibersegurança da UE nos termos do artigo 15.º do Regulamento (UE) 2025/38. Sem prejuízo de quaisquer futuros atos de execução ao abrigo do referido regulamento, os serviços da Reserva de Cibersegurança da UE deverão ser disponibilizados no prazo de 24 horas após a solicitação.

c) A nível político:

i. A fim de dar uma resposta política e estratégica adequada, o Conselho pode solicitar informações às principais partes interessadas, em especial à Comissão, ao alto representante e à UE-CyCLONe;

ii. O Conselho, apoiado pela Comissão e pelo alto representante, poderá decidir quais as medidas adequadas para dar resposta ao incidente de cibersegurança em grande escala, incluindo as possíveis respostas diplomáticas, em conformidade com o capítulo IX;

iii. Os Estados-Membros podem ativar mecanismos ou instrumentos de gestão de cibercrises adicionais consoante a natureza e o impacto do incidente;

iv. Quando o IPCR é acionado no modo de partilha de informações, a capacidade de apoio ISAA é também acionada, aumentando o intercâmbio de informações através da plataforma Web do IPCR e assegurando uma panorâmica comum da situação. Os relatórios de situação da UE-CyCLONe e da rede de CSIRT deverão continuar a ser os principais instrumentos para a apresentação do conhecimento situacional comum a nível operacional e a nível técnico, respetivamente. Esses relatórios podem servir de base aos relatórios ISAA;

v. No caso de um incidente que exija a ativação de medidas de resposta a nível da União, em especial dos mecanismos horizontais e setoriais de gestão de crises pertinentes a nível da União, enumerados no anexo II, o Conselho, em cooperação com a Comissão e o alto representante, deverá assegurar a coerência e a coordenação entre as respostas à cibercrise e as ações de resposta conexas a nível da União;

vi. Sempre que os mecanismos pertinentes, em particular os serviços da Reserva de Cibersegurança, forem solicitados, os serviços da Comissão e, se for caso disso, o SEAE, bem como as instâncias competentes do Conselho, nomeadamente o Grupo Horizontal das Questões do Ciberespaço e o Grupo Horizontal para o Reforço da Resiliência e a Luta contra as Ameaças Híbridas, consoante o caso, deverão coordenar-se no que diga respeito à conceção e aplicação de medidas, bem como ao processo de tomada de decisão adequado para a adoção de medidas adicionais, em consonância com o conjunto de instrumentos contra as ameaças híbridas[14], no caso de ciberatividades maliciosas que façam parte de uma campanha híbrida mais vasta.

Resposta a um incidente de cibersegurança em larga escala ou cibercrise em que o IPCR seja acionado em modo de ativação plena

56. Deverão aplicar-se as medidas enumeradas na secção «*Resposta a um incidente de cibersegurança em larga escala ou cibercrise em que o IPCR não seja acionado em modo de ativação plena*».

57. Quando o IPCR é acionado em modo de ativação plena, os relatórios ISAA destinam-se a assegurar um conhecimento situacional comum a nível político. Os relatórios de situação da UE-CyCLONe e da rede de CSIRT deverão continuar a ser os principais instrumentos para a apresentação do conhecimento situacional comum a nível operacional e a nível técnico, respetivamente. Esses relatórios podem servir de base aos relatórios ISAA.

58. Em caso de incidente de cibersegurança em grande escala ou de cibercrise que resulte na ativação do IPCR em modo de ativação plena, todos os intervenientes deverão reagir em estreita coordenação, seguindo uma abordagem de governação integrada, da seguinte forma:

a) A coordenação da resposta a nível político da União é assegurada pelo Conselho, recorrendo ao mecanismo IPCR;

[14] O conjunto de instrumentos contra as ameaças híbridas consiste num enquadramento para uma resposta coordenada a campanhas híbridas que afetem a UE e os Estados-Membros, incluindo, por exemplo, medidas de prevenção, de cooperação, de estabilização, de restrição e de recuperação, e apoio à solidariedade e à assistência mútua.

b) A UE-CyCLONe, em cooperação com a rede de CSIRT, deverá fornecer informações claras ao nível político sobre o impacto, as possíveis consequências e as medidas de resposta e remediação do incidente, nomeadamente contribuindo para os relatórios ISAA;

c) Para além da capacidade ISAA, a Presidência do Conselho da União Europeia convocará mesas redondas no âmbito do IPCR de modo a assegurar a coordenação política e estratégica da resposta da UE, sendo as medidas no âmbito do Plano de Ação para a Cibersegurança e o trabalho dos mecanismos setoriais pertinentes integrados nos trabalhos do IPCR. As mesas redondas podem ainda servir para identificar algumas lacunas específicas a nível da resposta e convidar determinados intervenientes da UE a colmatá-las e a apresentar um relatório em futuras mesas redondas, a fim de apoiar a coordenação política e estratégica do IPCR;

d) A Presidência do Conselho da União Europeia deverá considerar a possibilidade de convidar a UE-CyCLONe para as reuniões relevantes, nomeadamente para mesas redondas no âmbito do mecanismo IPCR e outras reuniões pertinentes do Conselho;

e) As autoridades de gestão de crises dos Estados-Membros deverão assegurar a coerência e a coordenação entre as respostas setoriais à cibercrise apoiadas pelas autoridades de gestão de cibercrises;

f) As eventuais respostas diplomáticas deverão ser ponderadas e executadas de acordo com o capítulo IX.

VIII: Iniciativas de comunicação pública

59. Embora a comunicação à população de cada Estado-Membro sobre um incidente de cibersegurança em grande escala ou uma cibercrise em curso, nomeadamente no âmbito de ações de sensibilização, seja da competência nacional, os Estados-Membros, a Comissão e o alto representante deverão procurar coordenar, na medida do possível, a sua comunicação pública. A rede informal de comunicadores de crise do IPCR pode ser envolvida, conforme adequado.

60. Para efeitos da preparação para incidentes de cibersegurança em grande escala e cibercrises, os Estados-Membros e, se for caso disso, a Comissão e a CERT-UE são convidados a trocar informações sobre as suas iniciativas de comunicação no âmbito da UE-CyCLONe e da rede de CSIRT, inclusive sobre boas práticas, como avisos ou campanhas de sensibilização. A ENISA deverá fornecer instrumentos que apoiem esse intercâmbio e garantam o seu fácil acesso.

61. Em caso de incidente de cibersegurança em grande escala ou de cibercrise, os Estados-Membros são convidados a partilhar, no âmbito da UE-CyCLONe, informações sobre as suas iniciativas de comunicação pública, a fim de criar uma consciencialização comum e coordenar as ações. A UE-CyCLONe, por iniciativa própria ou a pedido do Conselho, pode partilhar com este último uma panorâmica dessas abordagens.

IX: Resposta diplomática e cooperação com parceiros estratégicos

62. O alto representante, em estreita cooperação com a Comissão e outras entidades competentes da União, deverá:

    a) Apoiar, nomeadamente por meio de análises, relatórios e propostas, a tomada de decisões no Conselho sobre o recurso a possíveis medidas no âmbito do conjunto de instrumentos de ciberdiplomacia da UE. Tal permitirá fazer uso de todo o espetro de instrumentos de que a União dispõe para prevenir, dissuadir e responder a ciberatividades maliciosas, reforçando a sua postura no ciberespaço e promovendo a paz, a segurança e a estabilidade internacionais no ciberespaço;

b) Sempre que seja identificado um incidente relevante, facilitar o fluxo das informações necessárias com parceiros estratégicos, incluindo a OTAN, quando pertinente;

c) Reforçar a coordenação com os parceiros estratégicos, incluindo a OTAN, quando pertinente, no que respeita à resposta a ciberatividades maliciosas desenvolvidas por autores de ameaças persistentes, nomeadamente ao utilizar o conjunto de instrumentos de ciberdiplomacia da UE, em conformidade com as orientações de execução.

63. Os Estados-Membros, o alto representante, a Comissão e outras entidades competentes da União deverão cooperar com parceiros estratégicos e organizações internacionais para promover boas práticas e um comportamento responsável dos Estados no ciberespaço, e assegurar uma resposta rápida e coordenada em caso de incidentes de cibersegurança potenciais ou em grande escala.

64. A cooperação entre a União Europeia e a OTAN deverá ser conduzida em conformidade com os princípios orientadores acordados de inclusividade, reciprocidade e transparência, e no pleno respeito pela autonomia de decisão da União.

65. A Comissão e o alto representante, tendo em conta os acordos existentes, como o acordo técnico CERT-UE/OTAN de 2016, deverá estabelecer pontos de contacto para a coordenação com a OTAN em caso de cibercrise, a fim de trocar as informações necessárias sobre a situação e a utilização de mecanismos de resposta a situações de crise para intensificar a cooperação na resposta e aumentar a eficácia desta última. Para o efeito, a União deverá explorar formas de melhorar a partilha de informações com a OTAN, de uma forma inclusiva, recíproca e não discriminatória, em especial assegurando a existência de instrumentos que permitam uma comunicação segura, tendo simultaneamente em conta as normas em matéria de partilha de informações dos diferentes Estados-Membros.

66. No âmbito do programa evolutivo de exercícios de cibersegurança da União referido no capítulo V acima, os serviços da Comissão e o SEAE deverão considerar a possibilidade de organizar um exercício com a OTAN ao nível do pessoal, a fim de testar a cooperação entre entidades civis e militares na eventualidade de um incidente de cibersegurança em grande escala ou de uma cibercrise em que os Estados-Membros ou os aliados da OTAN procurem dar resposta a um ciberataque que afete a sua segurança. O exercício deverá ser conduzido de forma inclusiva e não discriminatória, e no pleno respeito dos princípios acordados nos parâmetros da cooperação UE-OTAN. O exercício deverá ser conduzido no quadro do exercício «*EU Integrated Resolve*» (Exercícios Paralelos e Coordenados, «PACE»). Deverão ser tomadas todas as medidas necessárias por forma a garantir a participação de todos os intervenientes referidos no Plano de Ação para a Cibersegurança.

67. Em consulta com o Conselho, a Comissão e o alto representante, deverá também ser ponderada a possibilidade de realizar exercícios conjuntos de cibersegurança a nível da União com os países dos Balcãs Ocidentais, a República da Moldávia e a Ucrânia, bem como com outros parceiros estratégicos e países terceiros que partilhem as mesmas ideias.

X. Coordenação da gestão de cibercrises com intervenientes militares a nível da UE

68. Os Estados-Membros deverão continuar a reforçar a cooperação a nível nacional entre intervenientes civis e militares no domínio cibernético.

69. A UE-CyCLONe e a rede de CSIRT deverão identificar possíveis formas e procedimentos de cooperação com os intervenientes militares da UE, como a Conferência de Cibercomandantes da UE e a rede operacional de equipas militares de resposta a emergências informáticas («MICNET»), a fim de beneficiarem de uma perspetiva militar e civil conjunta, nomeadamente por meio de reuniões conjuntas. A UE-CyCLONe e a rede de CSIRT deverão informar o Conselho sobre os progressos realizados no que respeita a essa cooperação.

70. O Estado-Membro afetado é convidado a informar a UE-CyCLONe, bem como o SEAE, caso sejam utilizadas capacidades de resposta militares relevantes, nacionais ou multinacionais, no contexto de um incidente de cibersegurança em grande escala ou de uma cibercrise, sendo o fornecimento dessas informações mutuamente acordado entre o utilizador e o fornecedor dessa capacidade de resposta.

71. No âmbito do programa evolutivo de exercícios de cibersegurança da União referido no capítulo V acima, a Comissão e o SEAE deverão ponderar a possibilidade de organizar um exercício conjunto, a fim de testar a cooperação entre intervenientes civis e militares no domínio cibernético na eventualidade de um incidente de cibersegurança em grande escala que afete um ou vários Estados-Membros.

XI: Recuperação de uma cibercrise e ensinamentos dela retirados

72. Os Estados-Membros e as entidades e redes competentes da União deverão colaborar durante a fase de recuperação após uma cibercrise a fim de garantir o rápido restabelecimento das funcionalidades essenciais. Sempre que pertinente, as forças policiais deverão também participar nessa cooperação. Nesta fase, a cooperação com o setor privado é crucial, nomeadamente para facilitar a recuperação de dados e o restabelecimento dos sistemas. Uma coordenação eficaz entre as partes interessadas deverá dar prioridade à minimização das perturbações e à garantia da continuidade operacional.

73. Os Estados-Membros e as entidades e redes competentes da União deverão trabalhar em conjunto na fase de recuperação, com base nos ensinamentos retirados de cibercrises ou de incidentes de cibersegurança geridos no passado, bem como nos relatórios de incidentes, em especial no contexto do Mecanismo Europeu de Análise de Incidentes de Cibersegurança criado pelo Regulamento (UE) 2025/38.

74. A UE-CyCLONe deverá fornecer à rede de CSIRT, ao grupo de cooperação SRI e ao Conselho uma lista exaustiva dos ensinamentos retirados de cibercrises ou de incidentes de cibersegurança geridos no passado, bem como das boas práticas. A ENISA deverá assegurar que esses ensinamentos retirados sejam devidamente refletidos em futuras atividades de preparação e no planeamento de futuros exercícios.

XII: Comunicação segura

75. Com base no levantamento das ferramentas existentes para uma comunicação segura[15], a Comissão deverá propor, até ao final de 2026, um conjunto interoperável de soluções de comunicação segura. O Conselho, a Comissão, o alto representante, a UE-CyCLONe e a rede de CSIRT deverão chegar a acordo sobre esse conjunto de soluções até ao final de 2027. Essas soluções deverão beneficiar das medidas no domínio das comunicações seguras que as instituições da UE poderão adotar no âmbito da Estratégia Europeia para uma União da Preparação e deverão abranger toda a gama de modos de comunicação necessários (voz, dados, videoconferência, mensagens, colaboração, bem como partilha e consulta de documentos). As soluções deverão cumprir os requisitos comummente definidos para a proteção de informações sensíveis não classificadas. Deverão ser utilizadas soluções baseadas num protocolo aberto com aplicações de fonte aberta adequadas para a comunicação em tempo real, geridas por uma entidade residente na UE.

76. Para efeitos de intercâmbio de informações classificadas como RESTREINT UE/EU RESTRICTED, a UE-CyCLONe e a rede de CSIRT deverão poder utilizar, se necessário, os canais de comunicação seguros assegurados às instituições, órgãos e organismos da UE para o intercâmbio de informações classificadas entre si e com os Estados-Membros.

---

15 WK 862/2023.

77. Sem prejuízo do futuro quadro financeiro plurianual, o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC), criado pelo Regulamento (UE) 2021/887[16], deverá considerar a possibilidade de financiamento através do Programa Europa Digital para ajudar os Estados-Membros a implantar estas ferramentas de comunicação segura. Deverá evitar-se a duplicação de investimentos em sistemas seguros interoperáveis.

78. Em especial, as entidades da UE e os Estados-Membros deverão desenvolver soluções de contingência para crises graves em que os canais de comunicação normais que dependem da Internet ou de redes de telecomunicações sofram perturbações ou não estejam disponíveis.

79. Deverão ser criados mecanismos de comunicação e partilha de informações entre as forças policiais e as redes de cibersegurança, em especial a nível técnico, para uma resposta eficaz às cibercrises. Estes mecanismos deverão respeitar o papel de cada parte, evitar interferir com as operações em curso e garantir a redundância das comunicações. O Sistema Europeu de Comunicações Críticas, que está em fase de desenvolvimento, pode ser útil para a resposta conjunta com as cibercomunidades pertinentes.

XIII: Disposições finais

80. A UE-CyCLONe, em cooperação com a rede de CSIRT e outros principais intervenientes no ecossistema de gestão de cibercrises da UE, apoiada pela ENISA, deverá elaborar, no prazo de um ano a contar da publicação da presente recomendação, diagramas de fluxos pormenorizados que descrevam os fluxos de informação entre os intervenientes pertinentes, os processos de tomada de decisão e os relatórios elaborados durante a gestão de um incidente de cibersegurança em grande escala ou de uma cibercrise conforme descrito na presente recomendação. Os diagramas de fluxos deverão abranger os diferentes modos e níveis de cooperação e ser atualizados sempre que necessário.

[16] Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação, JO L 202 de 8.6.2021, p. 1.

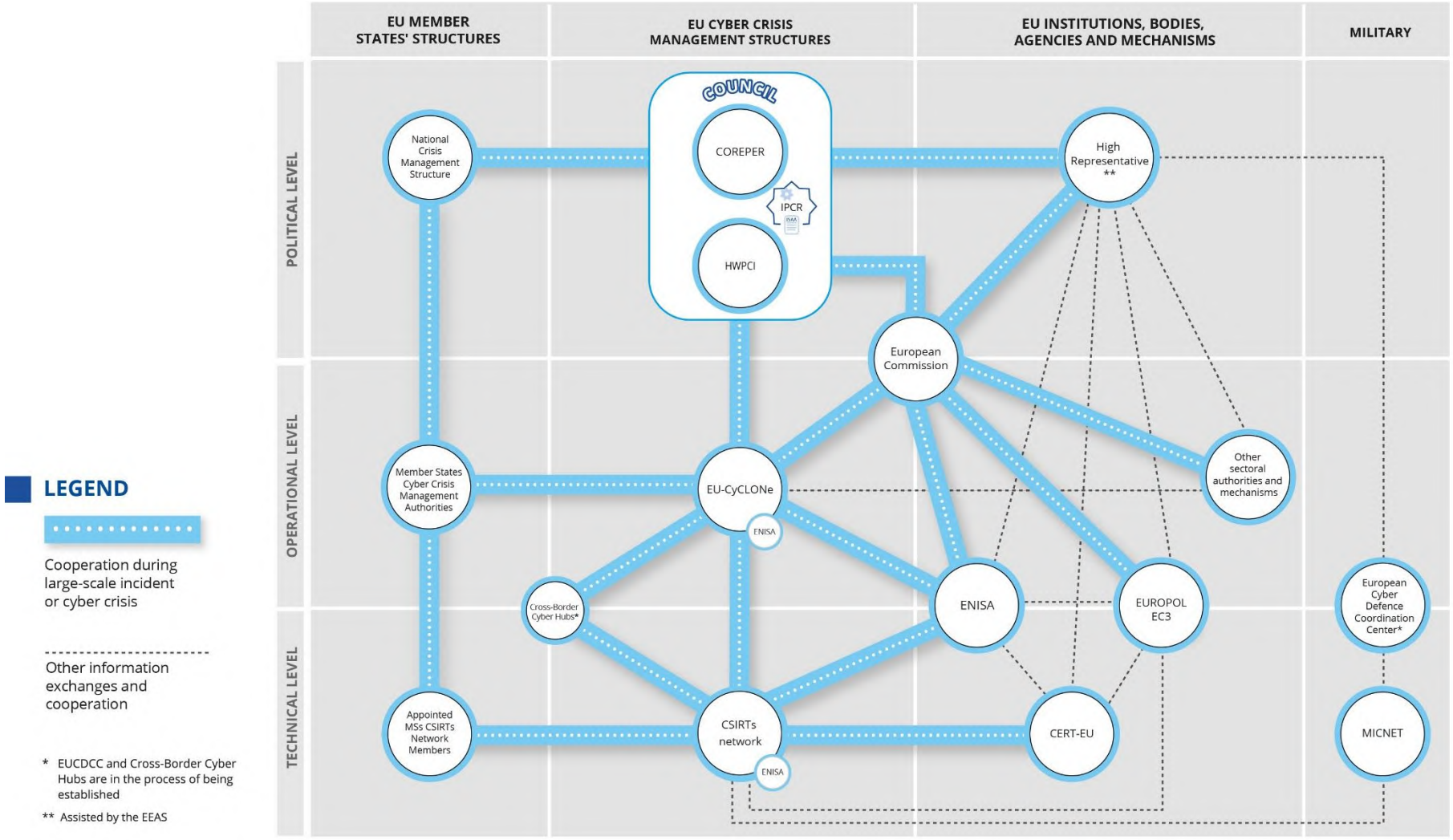
81. A fim de apoiar uma execução eficaz do Plano de Ação para a Cibersegurança revisto, e com base na experiência adquirida com os exercícios de cibersegurança conjuntos realizados no quadro desse plano, caso seja necessário, o Conselho pode formular orientações de execução. Estas orientações poderão incidir sobre os desafios práticos identificados no decurso dos exercícios e preencher as lacunas e os elos cuja ausência tenha sido detetada a nível da coordenação, da comunicação e da interação operacional.

82. A presente recomendação deverá ser revista pela Comissão, em cooperação com os Estados-Membros, pelo menos de quatro em quatro anos após a sua publicação. Após cada revisão, a Comissão deverá publicar um relatório e apresentá-lo ao Conselho. A Comissão e os Estados-Membros deverão ter em conta, em particular, o impacto da evolução do panorama de ameaças, os resultados dos exercícios conjuntos e as alterações legislativas – em especial quaisquer eventuais alterações decorrentes da revisão do Regulamento (UE) 2019/881.

Feito em Bruxelas, em

Pelo Conselho
O Presidente / A Presidente

ANEXO I – Plano de ação da União para responder a uma crise de cibersegurança



ANEXO II – INTERVENIENTES (ENTIDADES E REDES) E MECANISMOS PERTINENTES DE GESTÃO DE CRISES A NÍVEL DA UNIÃO

1) Participação dos principais intervenientes ao longo do ciclo de gestão de cibercrises (incidentes de cibersegurança em grande escala e cibercrises)

	Preparação	Deteção	Resposta a incidentes de cibersegurança em grande escala e a cibercrises			Comunicação pública	Recuperação e ensinamentos retirados
			a nível técnico	a nível operacional	a nível político		
Estados-Membros	X	X	X	X	X	X	X
Comissão	X			X	X	X	
Alto representante apoiado pelo SEAE	X			X	X	X	
Conselho	X				X	X	X
ENISA	X		X	X			
CERT-UE	X	X	X	X		X	X
Rede de CSIRT	X	X	X				X
UE-CyCLONe	X			X	X		X

2) Funções e competências dos intervenientes e mecanismos pertinentes a nível da União (por ordem alfabética) relativamente à gestão de cibercrises

Interveniente	Nível	Função e competência	Referência
CERT-UE	Técnico/operacional	Coordena a resposta a crises a nível técnico e a gestão de incidentes graves que afetem entidades da União. Mantém um inventário dos conhecimentos técnicos especializados disponíveis necessários para a resposta aos incidentes quando incidentes graves ocorram e presta assistência ao IICB na coordenação dos planos de gestão de cibercrises das entidades da União para incidentes graves. Membro da rede de CSIRT. Apoia a Comissão na UE-CyCLONe no que respeita à gestão coordenada de crises e incidentes de cibersegurança em grande escala. Atua enquanto plataforma de intercâmbio de informações de cibersegurança e centro de coordenação da resposta a incidentes, facilitando o intercâmbio de informações sobre incidentes, ciberameaças, vulnerabilidades e quase	Regulamento (UE, Euratom) 2023/2841 Regulamento (UE) 2025/38

Interveniente	Nível	Função e competência	Referência
		incidentes entre entidades da União e contrapartes. Solicita a disponibilização da Reserva de Cibersegurança da UE em nome de entidades da União. Coopera com o Centro de Cibersegurança da OTAN com base no respetivo acordo técnico.	
Conselho da União Europeia	Político	Funções de elaboração de políticas e de coordenação. É responsável pelo IPCR no que respeita à coordenação e à resposta da União a nível político.	Artigo 16.º do Tratado da União Europeia
Presidência do Conselho da União Europeia	Político	Decide (exceto se a cláusula de solidariedade tiver sido invocada nos termos do artigo 222.º do Tratado sobre o Funcionamento da União Europeia) se o IPCR é ou não acionado, em consulta com os Estados-Membros afetados, conforme adequado, bem como com a Comissão e o alto representante.	Artigo 16.º do Tratado da União Europeia Decisão de Execução (UE) 2018/1993 do Conselho
Plataformas de cibersegurança transfronteiriças	Técnico	Uma plataforma de cibersegurança transfronteiriça é uma plataforma plurinacional, criada através de	Regulamento (UE) 2025/38

Interveniente	Nível	Função e competência	Referência
		um acordo de consórcio por escrito, que reúne, numa estrutura de rede coordenada, plataformas de cibersegurança nacionais de, pelo menos, três Estados-Membros, e que é concebida para otimizar a monitorização, deteção e análise de ciberameaças, prevenir incidentes e apoiar a produção de informações sobre ciberameaças, sobretudo através do intercâmbio de dados e informações pertinentes, anonimizados se for caso disso, bem como através da partilha de ferramentas de ponta e do desenvolvimento conjunto de capacidades de deteção, análise, prevenção e proteção no domínio da cibersegurança num ambiente de confiança; Cooperam estreitamente com a rede de CSIRT para partilhar informações. Fornecem informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, às autoridades dos Estados--Membros e à Comissão através da UE-CyCLONe e da rede de CSIRT.	

Interveniente	Nível	Função e competência	Referência
Rede de CSIRT	Técnico	Contribui para o desenvolvimento da confiança e promove uma cooperação operacional célere entre os Estados-Membros. É a principal rede de intercâmbio de informações importantes sobre incidentes, quase incidentes, ciberameaças, riscos e vulnerabilidades. A pedido de um membro potencialmente afetado por um incidente, a rede troca e discute informações relacionadas com esse incidente e com ciberameaças conexas. A rede pode igualmente contribuir para uma resposta coordenada a um incidente identificado no âmbito da jurisdição de um membro requerente. Presta assistência aos Estados-Membros na gestão de incidentes transfronteiriços e explora outras formas de cooperação, incluindo a assistência mútua. Recebe informações dos Estados-Membros sobre os respetivos pedidos	Diretiva (UE) 2022/2555 Regulamento (UE) 2025/38

Interveniente	Nível	Função e competência	Referência
		apresentados à Reserva de Cibersegurança da UE.	
Conferência de Cibercomandantes		Um fórum onde os cibercomandantes a nível nacional (Estados-Membros) colaboram e trocam informações vitais sobre operações e estratégias em curso no âmbito do ciberespaço com vista a atenuar os ciberincidentes em grande escala. É organizado pela Presidência rotativa do Conselho da União Europeia, com o apoio da Agência Europeia de Defesa (AED), do Serviço Europeu para a Ação Externa (SEAE), bem como do Estado-Maior da União Europeia (EMUE).	Comunicação conjunta sobre a política de ciberdefesa da UE (2022)
Comissão	Operacional/político	Órgão executivo da União Europeia. Garante o bom funcionamento do mercado interno. Contribui para a coerência e a coordenação entre ações conexas empreendidas à escala da União para dar resposta a situações crises. Encarrega-se de determinadas ações gerais de preparação a nível da União ao abrigo da	Artigo 17.º do Tratado da União Europeia Decisão de Execução (UE) 2018/1993 Decisão n.º 1313/2013/UE Diretiva (UE) 2022/2555

Interveniente	Nível	Função e competência	Referência
		Decisão MPCU, incluindo a gestão do Centro de Coordenação de Resposta de Emergência e do Sistema Comum de Comunicação e de Informação de Emergência. Participa na UE-CyCLONe na qualidade de observadora e é membro desta rede nos casos em que um incidente de cibersegurança em grande escala, potencial ou em curso, tenha ou seja suscetível de ter um impacto significativo nos serviços e atividades abrangidos pelo âmbito de aplicação da Diretiva (UE) 2022/2555. Participa na rede de CSIRT na qualidade de observadora. Tem a responsabilidade global pela execução da Reserva de Cibersegurança da UE. Serve de ponto de contacto junto do Conselho Interinstitucional para a Cibersegurança para fins de partilha de informações importantes sobre incidentes graves com a UE-CyCLONe. É consultada pela Presidência do Conselho sobre as decisões de ativação ou desativação o IPCR (exceto se a cláusula de solidariedade tiver sido	Regulamento (UE) 2025/38 Regulamento (UE, Euratom) 2023/2841

Interveniente	Nível	Função e competência	Referência
		invocada nos termos do artigo 222.º do TFUE). Os serviços da Comissão elaboram, juntamente com o SEAE, os relatórios ISAA.	
Agência da União Europeia para a Cibersegurança (ENISA)	Técnico/operacional	Exerce as suas atribuições com o objetivo de alcançar um elevado nível de cibersegurança na União, nomeadamente apoiando ativamente os Estados-Membros e as instituições da União. Assegura o secretariado da rede de CSIRT e da UE-CyCLONe. Elabora regularmente um relatório aprofundado sobre a situação técnica da cibersegurança na UE quanto a incidentes e ciberameaças (com o EC3 e o CERT-UE e em estreita colaboração com os Estados-Membros). Contribui para o desenvolvimento de uma resposta comum a incidentes ou crises transfronteiriças, sobretudo: – agregando e analisando relatórios provenientes de fontes nacionais;	Diretiva (UE) 2022/2555 Regulamento (UE) 2019/881 Regulamento (UE) 2025/38 Regulamento (UE) 2024/2847

Interveniente	Nível	Função e competência	Referência
		– assegurando o fluxo de informações entre os níveis técnico, operacional e político; – a pedido, facilitando o tratamento técnico desses incidentes; – apoiando as entidades da União no que diz respeito à comunicação pública; – apoiando os Estados-Membros no que diz respeito à comunicação pública, quando solicitada; – testando as capacidades de resposta a incidentes e organizando regularmente exercícios de cibersegurança. Atua como entidade adjudicante sempre que seja incumbida de operar e a administrar, parcial ou totalmente, a Reserva de Cibersegurança da UE. Organiza, a cada dois anos, um exercício de cibersegurança abrangente em grande escala a nível da União com elementos técnicos, operacionais ou estratégicos. Elabora um relatório de análise do incidente em colaboração com o Estado-Membro afetado e outras partes interessadas pertinentes, a fim de avaliar as causas, os impactos e as medidas de atenuação de um incidente (a pedido da	

Interveniente	Nível	Função e competência	Referência
		Comissão ou da UE-CyCLONe e com a aprovação do Estado-Membro afetado). Informa a UE-CyCLONe se as informações fornecidas por força das obrigações de comunicação previstas no Regulamento de Ciber-resiliência forem relevantes para a gestão coordenada de incidentes e crises de cibersegurança em grande escala a um nível operacional.	
Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe)	Operacional	Apoia a gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível operacional. Assegura o intercâmbio regular de informações importantes entre os Estados-Membros e as instituições, órgãos e organismos da União. Coordena a gestão de crises e de incidentes de cibersegurança em grande escala e apoia a tomada de decisões a nível político em relação a tais incidentes e crises.	Diretiva (UE) 2022/2555 Regulamento (UE) 2025/38

Interveniente	Nível	Função e competência	Referência
		Avalia as consequências e o impacto de crises e incidentes de cibersegurança em grande escala relevantes e propõe eventuais medidas de atenuação. Discute, a pedido do Estado-Membro em causa, os planos nacionais de resposta a crises e incidentes de cibersegurança em grande escala. Elabora, juntamente com a ENISA e a Comissão, o modelo para facilitar a apresentação de pedidos de apoio à Reserva de Cibersegurança da UE. Recebe informações dos Estados-Membros sobre os respetivos pedidos apresentados à Reserva de Cibersegurança da UE. Recebe informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, provenientes das plataformas de cibersegurança transfronteiriças ou da rede de CSIRT.	
Alto representante da União para os Negócios	Político	Lidera e coordena os esforços da União para fazer face a ameaças externas contra a	Decisão 2010/427/UE do Conselho

Interveniente	Nível	Função e competência	Referência
Estrangeiros e a Política de Segurança, apoiado pelo Serviço Europeu para a Ação Externa		segurança nos domínios das ameaças híbridas e das ciberameaças É responsável pela ciberdiplomacia e pelos instrumentos de ciberdefesa da União para dissuadir e responder a ameaças externas, nomeadamente utilizando os conjuntos de instrumentos de ciberdiplomacia e contra as ameaças híbridas da União. Colabora com parceiros externos, incluindo por via de ações no âmbito da PCSD. Assegura a preparação da União e dos Estados-Membros no que respeita ao conhecimento situacional das ameaças híbridas e ciberameaças e à capacidade de reação às mesmas, por exemplo através de exercícios práticos, formação e redes. Lida com as implicações em matéria de segurança e defesa dos recursos espaciais da UE, especialmente no âmbito da política comum de segurança e defesa (PCSD) da União. Apoia a Conferência de Cibercomandantes da UE. Apoia a rede operacional de equipas militares de resposta a	

Interveniente	Nível	Função e competência	Referência
		emergências informáticas (MICNET). É consultado pela Presidência do Conselho sobre as decisões de ativação ou desativação o IPCR (exceto se a cláusula de solidariedade tiver sido invocada nos termos do artigo 222.º do TFUE). O SEAE elabora, juntamente com os serviços da Comissão, os relatórios ISAA.	
Centro de Coordenação da Ciberdefesa da UE	Horizontal	Tem como objetivo principal reforçar o conhecimento situacional comum da União e dos Estados-Membros sobre atividades maliciosas no ciberespaço, em especial no que diz respeito às missões e operações militares da PCSD.	Comunicação conjunta sobre a política de ciberdefesa da UE (2022)
Europol	Operacional	Presta apoio operacional e técnico às autoridades competentes dos Estados-Membros com vista à prevenção e dissuasão da cibercriminalidade. Assiste as autoridades competentes dos Estados-Membros, a seu pedido, na resposta a ciberataques que se suspeite serem de origem criminosa.	Regulamento (UE) 2016/794, com a última redação que lhe foi dada

Interveniente	Nível	Função e competência	Referência
Conselho Interinstitucional para a Cibersegurança		Estabelece um plano de gestão de cibercrises com vista a apoiar, a nível operacional, a gestão coordenada de incidentes graves que afetem entidades da União e a contribuir para o intercâmbio regular de informações pertinentes. Coordena a adoção dos planos individuais de gestão de cibercrises das entidades da União. Adota, com base numa proposta do CERT-UE, orientações ou recomendações sobre a cooperação na resposta a incidentes significativos que afetem entidades da União.	Regulamento (UE, Euratom) 2023/2841
Rede operacional de equipas militares de resposta a emergências informáticas (MICNET)	Técnico	Promove uma resposta mais forte e coordenada a ciberameaças que afetam os sistemas de defesa na União, incluindo os utilizados em missões e operações militares da PCSD; é apoiada pela Agência Europeia de Defesa.	Comunicação Conjunta sobre Ciberdefesa de 2022

Interveniente	Nível	Função e competência	Referência
Capacidade Única de Análise de Informações (SIAC)		É composta pelo Centro de Situação e de Informações da UE (INTCEN) e pela Direção de Informações do Estado-Maior da UE (EMUE INT). Fornece informações estratégicas sobre política externa, terrorismo, bem como ciberameaças e ameaças híbridas, Gere as informações militares destinadas às missões da PCSD e apoia as operações de defesa e de gestão de crises da União. Atua sob a autoridade do alto representante.	Artigo 38.º e artigos 42.º a 46.º do Tratado da União Europeia

3) Mecanismos e plataformas pertinentes de gestão de crises a nível da União

Mecanismo	Horizontal / setorial / específico do ciberespaço	Descrição	Referência
ARGUS	Horizontal	Processo de coordenação e sistema geral de alerta da Comissão para uma resposta coerente em caso de crise transfronteiriça grave que exija uma ação a nível da UE. Agrupa todos os serviços e gabinetes competentes para decidir e coordenar medidas. Permite à Comissão trocar informações importantes sobre crises multissetoriais emergentes ou ameaças previsíveis ou iminentes que exijam uma ação a nível da União.	Comunicação COM(2005) 662 da Comissão
Centro de Resposta a Situações de Crise (CRSC)	Horizontal	Ponto de entrada único no SEAE para todas as questões relacionadas com as crises e capacidade permanente de resposta a situações de crise – 24 horas por dia e 7 dias por semana – para emergências que ameacem a segurança do pessoal em delegações da UE e/ou em resposta a crises que afetem cidadãos da União no estrangeiro. Reúne peritos em questões consulares, de segurança e de conhecimento situacional, e conta também com profissionais	Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais (21 de março de 2022)

Mecanismo	Horizontal / setorial / específico do ciberespaço	Descrição	Referência
		empenhados destacados nas delegações da União.	
Plano de Ação para as Infraestruturas Críticas	Horizontal	Coordena a resposta a nível da União a perturbações em infraestruturas críticas com importante relevância transfronteiriça.	Recomendação C/2024/4371 do Conselho
Sistema de Alerta em matéria de Cibersegurança	Específico do ciberespaço	Assegura capacidades avançadas da União que lhe permitam reforçar as capacidades de deteção, análise e tratamento de dados relacionadas com ciberameaças e a prevenção de incidentes na União.	Regulamento (UE) 2025/38
Conjunto de instrumentos de ciberdiplomacia (quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas)	Específico do ciberespaço	Permite uma resposta diplomática conjunta da União às ciberatividades maliciosas, o que contribui para a prevenção de conflitos, a atenuação das ameaças à cibersegurança e uma maior estabilidade nas relações internacionais.	Conclusões do Conselho de 19 de junho de 2017 Orientações de execução revistas, doc. 10289/23, de 8 de junho de 2023
Reserva de Cibersegurança da UE	Específico do ciberespaço	Mobiliza peritos e recursos no domínio da cibersegurança durante situações de crise para apoiar os esforços de resposta nos Estados-Membros e nas instituições, órgãos ou organismos da União.	Regulamento (UE) 2025/38

Mecanismo	Horizontal / setorial / específico do ciberespaço	Descrição	Referência
Código de rede relativo a regras setoriais para os aspetos ligados à cibersegurança dos fluxos transfronteiriços de eletricidade	Setorial	Estabelece um processo recorrente de avaliação dos riscos de cibersegurança no setor da eletricidade, a nível da União, dos Estados-Membros, das regiões e das entidades. Contém disposições específicas para a gestão de crises e a cooperação com as CSIRT e a UE-CyCLONe nos casos em que um incidente de cibersegurança em grande escala tenha impacto noutros setores dependentes da segurança do abastecimento de eletricidade.	Regulamento Delegado (UE) 2024/1366 da Comissão
Conjunto de instrumentos contra as ameaças híbridas	Horizontal	Inclui um conjunto de disposições para proporcionar uma panorâmica dos instrumentos disponíveis a nível da UE para responder a todo o tipo de ameaças híbridas e garantir a sua utilização coordenada, assegurando a coerência das nossas ações em todos os domínios. Ajuda a assegurar que a tomada de decisões se baseia num conhecimento situacional abrangente e nos ensinamentos retirados.	Conclusões do Conselho, de 22 de junho de 2022, sobre um enquadramento para uma resposta coordenada da UE às campanhas híbridas. Orientações de execução do enquadramento para uma resposta coordenada da UE às campanhas híbridas, 14 de dezembro de 2022

Mecanismo	Horizontal / setorial / específico do ciberespaço	Descrição	Referência
Equipas de resposta rápida às ameaças híbridas (HRRT da UE)	Horizontal	Fazem parte do conjunto de instrumentos da UE contra as ameaças híbridas e recorrem a conhecimentos especializados setoriais a nível nacional e conhecimentos especializados civis e militares a nível da UE para prestar assistência personalizada e direcionada a curto prazo aos Estados-Membros, a missões e operações da política comum de segurança e defesa e a países parceiros na luta contra as ameaças e campanhas híbridas.	Quadro de referência para a criação prática de equipas de resposta rápida da UE contra as ameaças híbridas (21 de maio de 2024) Orientações operacionais para o destacamento de equipas de resposta rápida às ameaças híbridas, aprovadas pelo Coreper em 4 de dezembro de 2024
IPCR	Horizontal	Apoia a tomada de decisões rápidas e coordenadas a nível político da União em caso de crises graves e complexas. É ativado e desativado por decisão da Presidência do Conselho, que consulta (exceto nos casos em que a cláusula de solidariedade tenha sido invocada) os Estados-Membros afetados, a Comissão e o alto representante. O SGC, os serviços da Comissão e o SEAE podem também acordar, em consulta com a Presidência, em	Decisão de Execução (UE) 2018/1993 do Conselho

Mecanismo	Horizontal / setorial / específico do ciberespaço	Descrição	Referência
		ativar o IPCR em modo de partilha de informações. Os trabalhos do IPCR têm em conta os relatórios ISAA elaborados pelos serviços da Comissão e pelo SEAE. Esses relatórios baseiam-se em informações e análises relevantes fornecidas pelos Estados-Membros (por exemplo, pelos centros nacionais de crise pertinentes) e pelos organismos e órgãos competentes da União.	
Protocolo da UE de Resposta de Emergência dos Serviços Repressivos	Horizontal	Trata-se de um instrumento para apoiar as forças policiais da União na resposta imediata a ciberataques transfronteiriços graves por meio de uma avaliação rápida, da partilha segura e atempada de informações críticas e da coordenação eficaz dos aspetos internacionais das suas investigações.	Conclusões do Conselho, de 26 de junho de 2018, sobre a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala.
Equipas de resposta rápida a ciberataques	Específico do ciberespaço	As CRRT constituídas no âmbito da CEP são uma capacidade de ciberdefesa civil-militar desenvolvida em comum pelos Estados-Membros da UE para	Artigo 42.º, n.º 6, artigo 46.º e Protocolo n.º 10 do Tratado da União Europeia.

Mecanismo	Horizontal / setorial / específico do ciberespaço	Descrição	Referência
(CRRT) no âmbito da CEP		responder rapidamente a incidentes de cibersegurança e a cibercrises, bem como para executar ações preventivas, como avaliações de vulnerabilidades e observações eleitorais. A missão das CRRT constituídas no âmbito da CEP consiste em consiste em prestar apoio cibernético, quando solicitado, aos Estados-Membros da UE, às instituições, órgãos e organismos da UE, às missões e operações militares da PCSD da UE, bem como aos países parceiros.	

Arquitetura de resposta a ameaças espaciais (STRA)	Setorial (ameaças espaciais, incluindo ciberameaças)	Diz respeito à competência que cabe ao Conselho e ao alto representante a fim de evitar ameaças decorrentes da implantação, operação ou utilização dos sistemas estabelecidos e dos serviços prestados no âmbito do Programa Espacial da União.	Decisão (PESC) 2021/698 do Conselho
Quadro de coordenação em caso de ciberincidentes sistémicos (EU-SCICF)	Setorial	Está em fase de desenvolvimento; estabelecerá modalidades de comunicação e coordenação para abordar e gerir potenciais eventos de cibersegurança sistémicos no setor financeiro. Basear-se-á numa das funções preconizadas para as Autoridades Europeias de Supervisão (AES) pelo Regulamento (UE) 2022/2554, a saber, permitir a preparação gradual de uma resposta coordenada eficaz a nível da União em caso de incidente transfronteiriço grave relacionado com as tecnologias da informação e da comunicação (TIC) ou de ameaça conexa com impacto sistémico no setor financeiro da União no seu conjunto.	Recomendação do Comité Europeu do Risco Sistémico, de 2 de dezembro de 2021, sobre um quadro pan-europeu de coordenação para as autoridades competentes relativo a ciberincidentes sistémicos (CERS/2021/17)
Mecanismo de Proteção Civil da União (MPCU)	Horizontal	Assegura a cooperação no domínio da proteção civil para melhorar a prevenção, preparação e resposta a catástrofes.	Decisão n.º 1313/2013/UE.

CISE – Ambiente comum de partilha de informação	Específico do domínio marítimo, abrangendo sete setores.	Trata-se de uma rede que liga sistemas das autoridades da UE/EEE responsáveis pela vigilância marítima. Permite o intercâmbio de informações pertinentes para lá das fronteiras geográficas e setoriais, de forma contínua e automatizada.	Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais (21 de março de 2022).

4) Setores de importância crítica e outros setores críticos ao abrigo da Diretiva (UE) 2022/2555 e mecanismos de gestão de crises setoriais a nível da União (quando aplicável)

Setores	**Subsetor**	**Mecanismos de gestão de crises setoriais aplicáveis**
Energia	Eletricidade	Grupo de Coordenação da Eletricidade
	Sistemas de aquecimento e arrefecimento urbano	não aplicável
	Petróleo	Grupo de Coordenação do Petróleo Grupo de Autoridades Offshore da União Europeia (EUOAG)
	Gás	Grupo de Coordenação do Gás
	Hidrogénio	não aplicável
Transportes	Transporte aéreo	Célula de Coordenação de Crises da Aviação Europeia (CCCAE)
	Transporte ferroviário	não aplicável
	Transporte aquático	Agência Europeia de Controlo das Pescas (AECP) SafeSeaNet (SSN) Serviços Marítimos Integrados (IMS) Centro de dados do sistema de Identificação e Seguimento de Navios a Longa Distância (LRIT) Serviços de apoio marítimo da EMSA

	Transporte rodoviário	não aplicável
	Horizontal	Rede de Pontos de Contacto para os Transportes, estabelecida pelo Plano de emergência para os transportes [COM(2022) 211]
Setor bancário		EU-SCICF
Infraestruturas do mercado financeiro		EU-SCICF Mecanismo Europeu de Estabilização Financeira

Saúde		Sistema de Alerta Rápido e de Resposta (SARR) Centro de Gestão de Situações de Crise no Domínio Sanitário (HEOF) Sistema de alerta rápido para tecidos e células e para componentes sanguíneos (RATC/RAB) Quadro para Emergências de Saúde Pública Sistema de Alerta Rápido para Incidentes Químicos (RASCHEM) Portal Europeu de Vigilância das Doenças Infecciosas Autoridade de Preparação e Resposta a Emergências Sanitárias (HERA) Sistema de Informação Médica (MediSys) Grupo Diretor Executivo sobre Ruturas de Dispositivos Médicos (GDRDM) Alerta Rápido de Farmacovigilância Grupo de Trabalho da UE para a Saúde (EUHTF) Comité de Segurança da Saúde
Água potável		não aplicável

Águas residuais		não aplicável
Infraestruturas digitais		não aplicável
Gestão de serviços TIC		não aplicável
Administração pública		não aplicável
Espaço		Arquitetura de resposta a ameaças espaciais (STRA)
Serviços postais e de estafeta		não aplicável
Gestão de resíduos		não aplicável
Produção, fabrico e distribuição de produtos químicos		Sistema de Alerta Rápido para Incidentes Químicos (RASCHEM)

Produção, transformação e distribuição de produtos alimentares		Sistema europeu de monitorização das culturas Deteção de pontos críticos anómalos na produção agrícola mundial (ASAP) Rede Europeia de Sistemas de Informação Fitossanitária (EUROPHYT) Equipa de Emergência Veterinária da UE (EUVET) Sistema de Alerta Rápido para os Géneros Alimentícios e Alimentos para Animais (RASFF) Mecanismo Europeu de Preparação e Resposta a Crises de Segurança Alimentar (EFSCM) Regulamento de Emergência e Resiliência do Mercado Interno (ERMI)
Indústria transformadora	Dispositivos médicos	não aplicável
	Equipamentos informáticos, eletrónicos e óticos	não aplicável
	Máquinas e equipamentos	não aplicável
	Fabricação de veículos automóveis, reboques e semirreboques	não aplicável
	Fabricação de outro equipamento de transporte	não aplicável

Prestadores de serviços digitais		não aplicável
Investigação		não aplicável

ANEXO III – Quadro da UE para a Gestão de Crises de Cibersegurança e Instrumentos Conexos

Desde 2017, a União alargou o seu quadro de cibersegurança com vários instrumentos que contêm disposições pertinentes para a gestão de crises de cibersegurança:

- Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[1];
- Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[2];
- Regulamento de Execução (UE) 2024/2690 da Comissão[3], Regulamento (UE, Euratom) 2023/2841 do Parlamento Europeu e do Conselho[4];
- Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho[5];
- Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho[6], e
- Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho (Regulamento de Cibersolidariedade)[7].

As medidas específicas sobre crises de cibersegurança setoriais incluem o Regulamento Delegado (UE) 2024/1366 da Comissão[8] e o futuro quadro de coordenação relativo a ciberincidentes sistémicos (EU-SCICF) no contexto do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho[9].

A Diretiva 2013/40/UE[10] estabelece a referência para a definição de atividades criminosas relacionadas com ciberataques e as regras da União em matéria de acesso transfronteiriço a provas eletrónicas, em especial o Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho[11], que, assim que for aplicável, facilitará significativamente as ações policiais neste domínio.

A política de ciberdefesa da UE[12] define as funções de uma rede operacional de equipas militares de resposta a emergências informáticas (MICNET) da UE e da Conferência de Cibercomandantes da UE e prevê a criação de um Centro de Coordenação da Ciberdefesa da UE (EUCDCC).

Existem outros mecanismos de conhecimento situacional e de resposta a crises não relacionados com o ciberespaço em alguns dos setores críticos enumerados nos anexos I e II da Diretiva (UE) 2022/2555.

A Recomendação do Conselho sobre um plano de ação para a coordenação da resposta a nível da União a perturbações em infraestruturas críticas com importante relevância transfronteiriça[13] prevê a cooperação entre os intervenientes pertinentes sempre que um incidente afete tanto os aspetos físicos como a cibersegurança das infraestruturas críticas.

[1] 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Regulamento de Execução (UE) 2024/2690 da Comissão, de 17 de outubro de 2024, que estabelece regras de execução da Diretiva (UE) 2022/2555 relativamente aos requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança e especifica mais pormenorizadamente os casos em que se considera que um incidente é significativo no que respeita aos prestadores de serviços de DNS, aos registos de nomes de TLD, aos prestadores de serviços de computação em nuvem, aos prestadores de serviços de centro de dados, aos fornecedores de redes de distribuição de conteúdos, aos prestadores de serviços geridos, aos prestadores de serviços de segurança geridos, aos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais e aos prestadores de serviços de confiança (JO L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Regulamento (UE, Euratom) 2023/2841 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União (JO L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação (JO L 202, de 8.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência) (JO L, 2024/2847, 20.11. 2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho, de 19 de dezembro de 2024, que cria medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a

ciberameaças e incidentes de cibersegurança e que altera o Regulamento (UE) 2021/694 (Regulamento de Cibersolidariedade) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Regulamento Delegado (UE) 2024/1366 da Comissão, de 11 de março de 2024, que completa o Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho estabelecendo um código de rede relativo a regras setoriais para os aspetos ligados à cibersegurança dos fluxos transfronteiriços de eletricidade (JO L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO L 218 de 14.8.2013, p. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais, e Diretiva (UE) 2023/1544 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, que estabelece regras harmonizadas aplicáveis à designação de estabelecimentos designados e à nomeação de representantes legais para efeitos de recolha de prova eletrónica em processos penais (JO L 191 de 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022JC0049

[13] *JO C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C_202404371