Conselho da
União Europeia

Bruxelas, 21 de junho de 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	21 de junho de 2022
para:	Delegações
n.º doc. ant.:	9716/22
Assunto:	Conclusões do Conselho sobre o Relatório Especial n.º 5/2022 do Tribunal de Contas Europeu, intitulado "Cibersegurança das instituições, organismos e agências da UE: Em geral, o nível de preparação não é proporcional às ameaças" – Conclusões do Conselho aprovadas pelo Conselho na reunião de 21 de junho de 2022

Junto se envia, à atenção das delegações, as conclusões do Conselho em epígrafe, aprovadas pelo Conselho na sua reunião de 21 de junho de 2022.

ANEXO

CONCLUSÕES DO CONSELHO

sobre o Relatório Especial n.º 5/2022 do Tribunal de Contas Europeu, intitulado "Cibersegurança das instituições, organismos e agências da UE: Em geral, o nível de preparação não é proporcional às ameaças"

O CONSELHO DA UNIÃO EUROPEIA,

RECORDANDO as suas conclusões relativas ao melhoramento da análise dos relatórios especiais elaborados pelo Tribunal de Contas no âmbito do procedimento de quitação[1];

1. TOMA NOTA do Relatório Especial n.º 05/2022 do Tribunal de Contas Europeu intitulado "Cibersegurança das instituições, organismos e agências da UE: Em geral, o nível de preparação não é proporcional às ameaças"[2].

2. SUBLINHA a importância e a urgência de reforçar o nível de cibersegurança nas instituições, órgãos e organismos da UE, tendo em conta a recente intensificação da transformação digital nas instituições, as informações sensíveis que tratam, o número e a gravidade cada vez maiores dos ataques às instituições, órgãos e organismos da UE e o nível de ameaça que os afeta.

3. RECORDA as Conclusões do Conselho Europeu de 20 de junho de 2019[3], nas quais o Conselho Europeu convidou as instituições da UE a trabalharem, em conjunto com os Estados-Membros, em medidas para reforçar a resiliência e melhorar a cultura de segurança da UE contra ciberameaças e ameaças híbridas provenientes do exterior da UE, bem como para proteger melhor as redes de informação e comunicação da UE, e os seus processos de tomada de decisões, de todo o tipo de atos mal-intencionados.

---

1 7515/00 + COR 1.
2 8040/22
3 EUCO 9/19.

4. RECORDA as suas conclusões, de 10 de dezembro de 2019, sobre os esforços complementares para aumentar a resiliência e combater as ameaças híbridas[4], nas quais exortou as instituições, órgãos e organismos da UE, apoiados pelos Estados-Membros, a garantirem a capacidade da União para proteger a sua integridade e reforçar a segurança das redes de informação e comunicação e dos processos de tomada de decisão da UE contra atividades maliciosas de todos os tipos, com base numa avaliação global da ameaça. Para tal, afirma-se nas conclusões, as instituições, órgãos e organismos da UE, apoiados pelos Estados-Membros, deverão desenvolver e aplicar uma série de medidas abrangentes destinadas a garantir a sua segurança, em conformidade com o mandato do Conselho Europeu de junho de 2019[5].

5. RECORDA as suas conclusões de 22 de março de 2021 sobre a Estratégia de Cibersegurança da UE para a década digital[6], nas quais salientou que a cibersegurança é vital para o funcionamento da administração pública e das instituições, tanto a nível nacional como da UE, bem como para a nossa sociedade e a economia no seu todo.

6. RECORDA as suas conclusões de 23 de maio de 2022 sobre o desenvolvimento da postura da União Europeia no ciberespaço[7], nas quais as instituições, órgãos e organismos da UE foram incentivados a participar no levantamento dos instrumentos existentes para uma comunicação segura no domínio do ciberespaço, a ser analisado nas instâncias competentes do Conselho e com os grupos de cooperação pertinentes, nomeadamente a rede CSIRT e a EU CyCLONe.

7. SUBLINHA a necessidade de abordar o risco sistémico que existe na interligação entre as instituições, órgãos e organismos da UE, bem como entre estes e as instituições dos Estados-Membros, apesar da sua independência institucional e autonomia administrativa.

---

4 14972/19
5 EUCO 9/19.
6 6722/21
7 9364/22

8. TOMA NOTA das observações do Relatório Especial, nomeadamente de que as instituições, organismos e agências da UE não alcançaram um nível de preparação cibernética proporcional às ameaças e têm diferentes níveis de maturidade em matéria de cibersegurança. RECONHECE que deverá ser reforçado o nível de preparação das instituições, órgãos e organismos da UE em matéria de cibersegurança, bem como as sinergias existentes entre estes.

9. Por conseguinte, INCENTIVA fortemente as instituições, órgãos e organismos da UE a continuarem a aplicar medidas de gestão dos riscos cibernéticos que assegurem um nível proporcional de cibersegurança, tal como previsto na proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que visa revogar a Diretiva (UE) 2016/1148, a fim de reforçar o seu nível de preparação.

10. CONVIDA as instituições, órgãos e organismos da UE a intensificarem os seus esforços para se defenderem das ciberameaças, e bem assim a sua cooperação no estabelecimento de normas e especificações coerentes, em especial para os contratos públicos, projetos e serviços relacionados com a cibersegurança, e a aperfeiçoarem a interoperabilidade dos seus sistemas informáticos, nomeadamente com vista a garantir a comunicação segura de conteúdos não classificados.

11. CONVIDA a Agência da União Europeia para a Cibersegurança (ENISA) e a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) a, no âmbito das suas competências, intensificarem a sua cooperação no apoio às instituições, órgãos e organismos da UE nos seus esforços em matéria de cibersegurança, em especial no que diz respeito ao reforço das capacidades de tais instituições, órgãos e organismos que apresentem um nível de maturidade inferior em matéria de cibersegurança.

12. TOMA NOTA das conclusões e recomendações do Relatório Especial e RECONHECE que deverá ser substancialmente reforçado o nível de preparação das instituições, órgãos e organismos da UE em matéria de cibersegurança, bem como as sinergias existentes entre estes. As instituições, órgãos e organismos da UE deverão dispor de um quadro abrangente em matéria de gestão dos riscos para a cibersegurança, realizar avaliações e auditorias regulares dos riscos, com base numa metodologia comum ou notoriamente conhecida e em normas internacionais, e sistematizar programas de sensibilização e formação em cibersegurança para o pessoal.

13. SALIENTA igualmente que as instituições, órgãos e organismos da UE deverão prever um orçamento suficiente para assegurar a aplicação de medidas de proteção contra as ciberameaças, respeitando o quadro financeiro plurianual, e TOMA NOTA da recomendação do Relatório Especial de que deve ser nomeado um órgão representativo de todas as instituições, órgãos e organismos da UE, dotado do mandato e dos meios adequados, para controlar o cumprimento das regras comuns em matéria de cibersegurança.

14. RECONHECE que a CERT-UE deverá ser informada sem demora de ciberincidentes significativos ocorridos nas instituições, órgãos e organismos da UE e, para o efeito, dispor de recursos adequados que sejam previsíveis e adaptados ao atual nível de ameaça e às necessidades das instituições, órgãos e organismos da UE, em particular em termos de pessoal, equipamento técnico e infraestruturas.

15. OBSERVA que deverão ser reforçados e sistematizados a cooperação e o intercâmbio de informações sobre cibersegurança, bem como a interoperabilidade de canais de comunicação seguros entre as instituições, órgãos e organismos da UE. APELA a que essa cooperação e intercâmbio de informações incluam também as autoridades públicas responsáveis pela cibersegurança nos Estados-Membros.

16. TOMA NOTA das respostas da Comissão, da CERT-UE e da ENISA que acompanham o Relatório Especial.

17. CONVIDA a Comissão a ter em conta as recomendações do Relatório Especial e a ser ambiciosa na conceção das políticas de cibersegurança das instituições, órgãos e organismos da UE, bem como a defender a geração de mais sinergias entre estes.