



Bruxelas, 20 de março de 2019
(OR. en)

7737/19

CYBER 101	RELEX 287
COPEN 118	TELECOM 141
COPS 92	DAPIX 109
COSI 52	CATS 43
DATAPROTECT 98	CSC 111
IND 102	CSCI 47
JAI 313	IA 106
JAIEX 44	EJUSTICE 44
POLMIL 31	

RESULTADOS DOS TRABALHOS

de: Secretariado-Geral do Conselho

data: 19 de março de 2019

para: Delegações

n.º doc. ant.: 6866/19

Assunto: Conclusões do Conselho sobre o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE

Junto se enviam, à atenção das delegações, as conclusões do Conselho sobre o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE, adotadas pelo Conselho Assuntos Gerais, em 19 de março de 2019.

Conclusões do Conselho sobre o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE

O Conselho da União Europeia,

1. RECORDANDO as suas conclusões sobre o tema "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE"¹;
2. RECORDANDO as suas conclusões sobre a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala²;
3. RECORDANDO as suas conclusões sobre o reforço das cibercapacidades externas³;
4. REITERANDO que é possível assegurar um elevado nível de segurança das redes e dos sistemas de informação através do reforço das capacidades e competências dos Estados-Membros e das instituições, agências e organismos da UE em matéria de cibersegurança e, consequentemente, reforçando a sua ciber-resiliência;
5. CONGRATULANDO-SE com os progressos alcançados pelos Estados-Membros no sentido de reforçar as Equipas de Resposta a Incidentes de Segurança Informática (CSIRT);
6. LOUVANDO a criação da rede de CSIRT pelos Estados-Membros com o apoio ativo da Comissão e da ENISA, bem como o reforço da cooperação a nível estratégico através do grupo de cooperação SRI, constituído pelos Estados-Membros, pela Comissão e pela ENISA;

¹ Doc. 14435/17 (Conclusões do Conselho sobre a comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE, de 20 de novembro de 2017).

² Doc. 10086/18 (Conclusões sobre a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala, de 26 de junho de 2018).

³ Doc. 10496/18 (Conclusões do Conselho sobre as diretrizes da UE para o reforço das cibercapacidades externas, de 26 de junho de 2018).

7. DESTACANDO o papel central do grupo de cooperação SRI no fornecimento das orientações necessárias para alinhar tanto quanto possível a abordagem seguida na transposição da Diretiva SRI⁴ em toda a UE, bem como na resolução de questões de cibersegurança relevantes;
8. RECONHECENDO o apoio existente que está a ser prestado pela Comissão aos Estados-Membros visando o desenvolvimento de capacidades das CSIRT, através do Mecanismo Interligar a Europa;
9. RECONHECENDO o apoio prestado às autoridades responsáveis pela aplicação da lei no desenvolvimento das capacidades de luta contra a cibercriminalidade, através do Fundo para a Segurança Interna e da CEPOL;
10. CONGRATULANDO-SE com a atualização do Quadro Estratégico da UE para a Ciberdefesa para continuar a apoiar o desenvolvimento das capacidades de ciberdefesa dos Estados-Membros;
11. LOUVANDO os progressos realizados na aplicação da Diretiva SRI pelos Estados-Membros;
12. OBSERVANDO que a cibersegurança é um domínio complexo, interdependente e em constante evolução, que exige a adaptação do quadro político e jurídico a novas tendências tecnológicas e a tecnologias emergentes como a inteligência artificial, a tecnologia de cadeia de blocos e a computação quântica;

⁴ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016).

13. SALIENTANDO que os programas de formação e educação relacionados com a cibersegurança, assim como as ações de informação e sensibilização dos utilizadores finais sobre as ameaças à segurança, são fundamentais para diminuir os riscos de cibersegurança;
14. SUBLINHANDO que os exercícios de cibersegurança são instrumentos eficazes para avaliar e melhorar o grau de preparação da UE e dos seus Estados-Membros para fazer face a incidentes e crises de cibersegurança de grande escala;
15. REITERANDO que o ciberespaço não tem fronteiras, o que significa que as perspetivas e a cooperação transfronteiras e intersetorial são princípios inabaláveis das atividades e iniciativas de desenvolvimento das cibercapacidades;
16. REALÇANDO a importância da cooperação entre o setor público, o setor privado e o mundo académico, em especial através de projetos colaborativos;
17. DESTACANDO a importância da cooperação civil-militar, orientada para a concretização de objetivos comuns no domínio do ciberespaço, com vista a assegurar uma resposta eficaz e coerente às ciberameaças;
18. REGISTA os progressos alcançados por um grupo de Estados-Membros no desenvolvimento de equipas de resposta rápida a ciberataques para aprofundar a cooperação voluntária no domínio do ciberespaço através da assistência mútua;

19. CONGRATULA-SE com os debates em curso no Conselho sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação, apresentada pela Comissão;
20. INCENTIVA à participação ativa nos trabalhos em curso do grupo de cooperação SRI, em especial no que diz respeito ao desenvolvimento das cibercapacidades;
21. INCENTIVA os trabalhos em curso do grupo de cooperação SRI relativos à resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala;
22. CONVIDA os Estados-Membros a desenvolverem as suas estratégias nacionais de cibersegurança e a integrarem a cibersegurança em todos os setores, tendo em conta os requisitos específicos de cada setor;
23. CONVIDA os Estados-Membros a efetuarem permanentemente o acompanhamento e a avaliação/apreciação do impacto das medidas tomadas para reforçar a ciber-resiliência e melhorar as suas cibercompetências e cibercapacidades a nível nacional;
24. CONVIDA os Estados-Membros a integrarem a literacia digital e a cibersegurança nos programas curriculares de todos os níveis de ensino (primário, secundário, terciário, aprendizagem ao longo da vida), com base, se for caso disso, em perfis profissionais atuais e futuros;
25. CONVIDA os Estados-Membros a levarem a cabo iniciativas de sensibilização do público e dos utilizadores finais para a cibersegurança e a ciber-higiene, destinadas especificamente aos trabalhadores do setor público;
26. INCENTIVA os Estados-Membros a realizarem exercícios de cibersegurança a nível nacional, bem como a realizarem e/ou participarem em exercícios de cibersegurança a nível da UE, a fim de testarem e de treinarem os aspetos tecnológicos e estratégicos, bem como para desenvolverem as qualificações necessárias de forma eficaz e em termos práticos;

27. CONVIDA os Estados-Membros a continuarem a desenvolver as capacidades técnicas e operacionais em matéria de cibersegurança das suas CSIRT no respeitante à prevenção, atenuação e resposta a incidentes;
28. INSTA a Comissão e a ENISA a continuarem a dar o seu apoio ao desenvolvimento das capacidades e competências da rede de CSIRT dos Estados-Membros, com o objetivo de melhorar a cooperação, partilhar informações sobre incidentes e dar uma resposta eficaz a incidentes transfronteiras em grande escala;
29. CONVIDA os Estados-Membros a continuarem a ajudar as autoridades responsáveis pela aplicação da lei a desenvolver competências específicas em coordenação com as autoridades europeias competentes, a fim de combater eficazmente a cibercriminalidade a nível da UE;
30. CONVIDA os Estados-Membros a aumentarem o investimento no desenvolvimento das cibercapacidades;
31. INSTA a Comissão e a ENISA a executarem programas de sensibilização e formação em matéria de cibersegurança destinados especificamente aos trabalhadores das instituições, agências e organismos da UE;
32. INSTA a UE e os seus Estados-Membros a procederem ao intercâmbio de informações e de boas práticas, numa base voluntária, a fim de contribuírem para a identificação e suprimento das principais necessidades em termos de desenvolvimento de cibercapacidades a nível nacional e da UE;
33. CONVIDA a UE e os seus Estados-Membros a apoiarem a investigação no domínio da cibersegurança, a promoverem a cibersegurança como uma temática para outras áreas de estudo, aproximando os diversos ramos da investigação e desenvolvimento relacionados com a cibersegurança para criar um conjunto integrado, e a fomentarem a excelência na investigação no domínio da cibersegurança;
34. CONVIDA a UE e os seus Estados-Membros a desenvolverem investigação no domínio da cibersegurança que reflita as necessidades sociais e integre no mercado os resultados da investigação;
35. INSTA a UE e os seus Estados-Membros a tomarem em consideração a cibersegurança nos concursos para a contratação pública no domínio das TIC, conforme adequado.