Conselho da
União Europeia

Bruxelas, 22 de março de 2022
(OR. en)

7474/22
ADD 1

Dossiê interinstitucional:
2022/0085(COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

PROPOSTA

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	22 de março de 2022
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2022) 122 final – ANEXOS 1 a 2
Assunto:	ANEXOS da Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

Envia-se em anexo, à atenção das delegações, o documento COM(2022) 122 final – ANEXOS 1 a 2.

Anexo: COM(2022) 122 final – ANEXOS 1 a 2

COMISSÃO
EUROPEIA

Bruxelas, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANEXOS

da

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANEXO I

A base de referência em matéria de cibersegurança abordará os seguintes domínios:

(1) políticas de cibersegurança, incluindo objetivos e prioridades para a segurança das redes e dos sistemas de informação, em especial no que respeita à utilização de serviços de computação em nuvem (na aceção do artigo 4.º, n.º 19, da diretiva [proposta SRI 2]) e a disposições técnicas que permitam o teletrabalho;

(2) organização da cibersegurança, incluindo a definição das funções e responsabilidades;

(3) gestão de ativos, incluindo o inventário dos ativos informáticos e o mapeamento da rede informática;

(4) controlo do acesso;

(5) segurança das operações;

(6) segurança das comunicações;

(7) aquisição, desenvolvimento e manutenção dos sistemas;

(8) relações com os fornecedores;

(9) gestão de incidentes, incluindo abordagens para melhorar a preparação, a resposta e a recuperação de incidentes e a cooperação com o CERT-UE, por exemplo no quadro da conservação de registos e da monitorização da segurança;

(10) gestão de crises e continuidade das atividades; e

(11) programas de educação, sensibilização e formação no domínio da cibersegurança.

ANEXO II

As instituições, órgãos e organismos da União devem tomar, no mínimo, as seguintes medidas específicas de cibersegurança na implementação da base de referência em matéria de cibersegurança e dos respetivos planos de cibersegurança, em consonância com os documentos de orientação e as recomendações do IICB:

(1) medidas concretas em prol da transição para uma arquitetura de confiança zero (isto é, um modelo de segurança, um conjunto de princípios de conceção do sistema e uma estratégia coordenada de cibersegurança e de gestão de sistemas assente no reconhecimento da existência de ameaças tanto dentro como fora das fronteiras tradicionais da rede);

(2) adoção por norma da autenticação multifatorial na rede e nos sistemas de informação;

(3) garantia da segurança da cadeia de abastecimento de *software* por meio de critérios para a criação e avaliação seguras de *software*;

(4) reforço das regras de contratação pública para facilitar um elevado nível comum de cibersegurança através:

   (a) da remoção dos obstáculos contratuais que limitam a partilha de informações com o CERT-UE por parte dos prestadores de serviços informáticos sobre os incidentes, vulnerabilidades e as ciberameaças;

   (b) da obrigação contratual de comunicar os incidentes, vulnerabilidades e as ciberameaças, bem como de dispor de um sistema adequado de monitorização e resposta a incidentes.