Conselho da
União Europeia

Bruxelas, 29 de março de 2022
(OR. en)

7670/22
ADD 3

Dossiê interinstitucional:
2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

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) 119 final – ANEXO 3
Assunto:	ANEXO 3 da Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à segurança da informação nas instituições, órgãos e organismos da União

Envia-se em anexo, à atenção das delegações, o documento COM(2022) 119 final – ANEXO 3.

Anexo: COM(2022) 119 final – ANEXO 3

COMISSÃO
EUROPEIA

Bruxelas, 22.3.2022
COM(2022) 119 final

ANNEX 3

ANEXO

da

Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à segurança da informação nas instituições, órgãos e organismos da União

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ANEXO III

Medidas para a proteção física das informações classificadas da União Europeia («ICUE»)

Equipamento e medidas organizativas para a proteção física das ICUE

1. Uma Zona Administrativa deve preencher os seguintes requisitos:

   a) Dispor de um perímetro visivelmente definido que permita o controlo de pessoas e, se possível, de veículos;

   b) Assegurar que as janelas que possam permitir o acesso visual não autorizado a ICUE dentro da zona sejam tornadas opacas ou sejam equipadas com estores, cortinas ou outros revestimentos;

   c) Só podem ter acesso sem escolta as pessoas devidamente autorizadas pela Autoridade de Segurança da instituição ou organismo da União em questão;

   d) Quaisquer outras pessoas são permanentemente escoltadas ou sujeitas a controlos equivalentes.

2. Para além dos requisitos previstos no ponto 1, uma Zona de Segurança deve preencher os seguintes requisitos:

   a) Dispor de um perímetro visivelmente definido e protegido em que qualquer entrada e saída seja controlada de forma permanente;

   b) Ser desprovida de dispositivos não autorizados como linhas de comunicação, telefones ou outros aparelhos de comunicação, bem como equipamento elétrico ou eletrónico;

   c) Estar equipada com um sistema de controlo do acesso e de monitorização em tempo real para a deteção de intrusos («IDS»), combinado com pessoal de segurança incumbido das situações de emergência;

   d) Ser inspecionada no final das horas normais de serviço e a intervalos aleatórios fora dessas horas, caso não esteja ocupada por pessoal em serviço 24 horas por dia e não esteja instalado um sistema IDS de monitorização em tempo real;

   e) Ser gerida por pessoal de segurança devidamente formado, supervisionado e com a devida credenciação de segurança;

   f) Dispor de procedimentos operacionais de segurança que incluam os seguintes elementos:

      i) o nível das ICUE que podem ser manuseadas, discutidas ou armazenadas nessa zona,

      ii) as medidas de vigilância e de proteção a manter,

      iii) as pessoas autorizadas a aceder sem escolta à zona por terem autorização de acesso e a necessidade de tomar conhecimento das ICUE em causa,

      iv) se necessário, os procedimentos respeitantes a escoltas ou à proteção das ICUE quando se autorize o acesso de outras pessoas a essa zona,

      v) quaisquer outras medidas e procedimentos relevantes.

3. Nos casos em que a entrada numa Zona de Segurança represente um acesso direto às informações classificadas que nela se encontrem, a zona deve ser definida como uma

Zona de Classe I e, nos casos em que tal não se verifique, a zona deve ser definida como uma Zona de Classe II.

Para ambas as classes de Zona de Segurança a que se refere o primeiro parágrafo e para além dos requisitos previstos no ponto 2, o Departamento/Responsável de Segurança da instituição ou organismo da União em causa deve indicar claramente o nível de classificação de segurança mais elevado das informações normalmente conservadas nessa zona e definir claramente um perímetro que permita o controlo das pessoas e, se possível, dos veículos.

As instituições e os organismos da União devem assegurar que as pessoas que acedem a uma Zona de Segurança cumprem os seguintes critérios:

a) Pedir autorização específica para entrar nessa zona;

b) Ser permanentemente escoltadas;

c) Possuir a devida credenciação de segurança, a menos que sejam tomadas medidas para assegurar que não seja possível ter acesso às ICUE.

4. Uma Zona de Segurança a proteger contra escutas passivas e ativas deve ser designada Zona Tecnicamente Segura. Para além dos requisitos aplicáveis às Zonas de Segurança, aplicam-se ainda os seguintes requisitos a estas zonas:

a) Devem estar equipadas com IDS, fechadas à chave quando não estiverem ocupadas e guardadas quando ocupadas. Todas as chaves devem ser controladas de acordo com o artigo 29.º, n.º 3;

b) São sujeitas a inspeção física e/ou técnica, ou ambas, de forma regular pela Autoridade de Segurança da instituição ou organismo da União em questão. Essas inspeções devem ser igualmente efetuadas na sequência de qualquer entrada não autorizada ou de suspeitas dessa possibilidade;

c) Devem dispor de uma proteção acústica e TEMPEST adequada.

5. Todas as pessoas que entrem em Zonas Tecnicamente Seguras devem cumprir os requisitos estabelecidos no ponto 3.

6. Poderão ser temporariamente criadas Zonas de Segurança e Zonas Tecnicamente Seguras no interior de determinada Zona Administrativa para a realização de uma reunião classificada ou para qualquer outro fim semelhante.

7. Devem ser construídas casas-fortes dentro das Zonas de Segurança. Uma casa-forte é uma instalação com uma construção física reforçada em que a Autoridade de Segurança da instituição ou organismo da União em questão aprova as paredes, o chão, os tetos, as janelas e as portas com sistema de fecho. Essas instalações devem beneficiar de proteção equivalente à de um contentor de segurança aprovado para armazenamento de ICUE com o mesmo nível de classificação.

Medidas de proteção física para o tratamento e armazenamento de ICUE

8. As ICUE com classificação RESTREINT UE/EU RESTRICTED devem ser tratadas e armazenadas em qualquer das seguintes zonas:

a) Em Zonas de Segurança;

b) Em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas;

c) Fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor se tenha comprometido a respeitar as medidas de compensação decididas pela Autoridade de Segurança de cada instituição e organismo da União.

9. As ICUE com classificação RESTREINT UE/EU RESTRICTED devem ser armazenadas em mobiliário de escritório apropriado e fechado à chave, numa Zona Administrativa ou Zona de Segurança. As referidas ICUE poderão ser temporariamente armazenadas fora de Zonas de Segurança ou de Zonas Administrativas, desde que o detentor se tenha comprometido a armazenar os documentos em causa em mobiliário de escritório apropriado e fechado à chave quando estes não estejam a ser lidos ou discutidos.

10. As instituições e os organismos da União podem tratar e armazenar informações com classificação RESTREINT UE/EU RESTRICTED fora das suas instalações, desde que as informações pertinentes sejam devidamente protegidas. Para o efeito, as instituições e organismos da União devem cumprir as medidas previstas no ponto 8, alínea c).

11. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser manuseadas e armazenadas numa das seguintes zonas:

a) Em Zonas de Segurança;

b) Em Zonas Administrativas, desde que as ICUE se encontrem protegidas do acesso por parte de pessoas não autorizadas;

c) Fora de Zonas de Segurança ou de Zonas Administrativas, sempre que limitadas em termos de volume e de tempo, e desde que o detentor se tenha comprometido a respeitar as medidas de compensação decididas pela Autoridade de Segurança da instituição ou organismo da União em questão. Além disso, o detentor de ICUE deve tomar as seguintes medidas:

i) informar o registo competente do facto de os documentos classificados estarem a ser manuseados fora das zonas protegidas,

ii) manter os documentos permanentemente sob o seu controlo pessoal.

12. As informações com classificação CONFIDENTIEL UE/EU CONFIDENTIAL e SECRET UE/EU SECRET devem ser armazenadas numa Zona de Segurança credenciada para esse nível pela Autoridade de Acreditação de Segurança competente da instituição ou organismo da União em questão, seja num contentor de segurança ou numa casa-forte.

13. Os documentos com classificação CONFIDENTIEL UE/EU CONFIDENTIAL ou superior só podem ser copiados pelo Registo pertinente.

14. As informações com a classificação TRES SECRET UE/EU TOP SECRET devem ser tratadas e armazenadas em Zonas de Segurança credenciadas para esse nível. Para o efeito, as instituições e organismos da União podem celebrar os convénios necessários para utilizar uma Zona de Segurança alojada e acreditada ao nível adequado pela Autoridade de Acreditação de Segurança de outra instituição e organismo da União.

15. As informações com a classificação TRES SECRET UE/EU TOP SECRET devem ser armazenadas em Zonas de Segurança credenciadas para esse nível pela

Autoridade de Acreditação de Segurança da instituição ou organismo competente da União em questão, numa das seguintes condições:

a) Num contentor de segurança aprovado pela Autoridade de Segurança de cada instituição e organismo da União, com um dos seguintes controlos complementares:

   i) proteção ou verificação permanente por pessoal de segurança ou de serviço com credenciação de segurança,

   ii) um IDS aprovado, conjugado com pessoal de segurança incumbido das situações de emergência;

b) Numa casa-forte com IDS, conjugada com pessoal de segurança incumbido das situações de emergência.