

Este texto constitui um instrumento de documentação e não tem qualquer efeito jurídico. As Instituições da União não assumem qualquer responsabilidade pelo respetivo conteúdo. As versões dos atos relevantes que fazem fé, incluindo os respetivos preâmbulos, são as publicadas no Jornal Oficial da União Europeia e encontram-se disponíveis no EUR-Lex. É possível aceder diretamente a esses textos oficiais através das ligações incluídas no presente documento

► **B****REGULAMENTO (UE) 2019/796 DO CONSELHO**

de 17 de maio de 2019

relativo a medidas restritivas contra os ciberataques ► **C1** que constituem uma ameaça para a União ◀ ou os seus Estados-Membros

(JO L 129I de 17.5.2019, p. 1)

Alterado por:

		Jornal Oficial		
		n.º	página	data
► M1	Regulamento de Execução (UE) 2020/1125 do Conselho de 30 de julho de 2020	L 246	4	30.7.2020
► M2	Regulamento de Execução (UE) 2020/1536 do Conselho de 22 de outubro de 2020	L 351 I	1	22.10.2020
► M3	Regulamento de Execução (UE) 2020/1744 do Conselho de 20 de novembro de 2020	L 393	1	23.11.2020
► M4	Regulamento de Execução (UE) 2022/595 da Comissão de 11 de abril de 2022	L 114	60	12.4.2022

Retificado por:

- **C1** Retificação, JO L 230 de 17.7.2020, p. 37 (2019/796)

**REGULAMENTO (UE) 2019/796 DO CONSELHO****de 17 de maio de 2019****relativo a medidas restritivas contra os ciberataques ►C1 que constituem uma ameaça para a União ◄ ou os seus Estados-Membros***Artigo 1.º*

1. O presente regulamento aplica-se aos ciberataques com um efeito significativo, nomeadamente a tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros.

2. Os ciberataques que constituem uma ameaça externa incluem os que:

- a) têm origem no exterior da União ou são realizados a partir do exterior da União,
- b) fazem uso de infraestruturas fora da União,
- c) são levados a cabo por qualquer pessoa singular ou coletiva, entidade ou organismo estabelecido ou que opere fora da União, ou
- d) são realizados com o apoio, sob a direção ou sob o controlo de qualquer pessoa singular ou coletiva, entidade ou organismo que opere fora da União.

3. Para este efeito, consideram-se «ciberataques», as ações que envolvam qualquer dos seguintes elementos:

- a) Acesso aos sistemas de informações,
- b) Interferência nos sistemas de informação,
- c) Interferência respeitantes a dados, ou
- d) Interceção de dados,

se essas ações não forem devidamente autorizadas pelo proprietário ou por outro titular dos direitos do sistema ou dos dados, ou de parte deles, ou não forem permitidas pelo direito da União ou do Estado-Membro em causa.

4. Os ciberataques que constituem uma ameaça para os Estados-Membros incluem os que afetam os sistemas de informação relacionados, nomeadamente, com:

- a) infraestruturas críticas, incluindo cabos submarinos e objetos lançados no espaço extra-atmosférico, que sejam essenciais para a manutenção de funções vitais da sociedade, da saúde, da segurança e do bem-estar económico e social das pessoas,
- b) serviços necessários para a manutenção de atividades sociais e/ou económicas essenciais, nomeadamente nos setores da energia (eletricidade, petróleo e gás), dos transportes (aéreos, ferroviários, por água e rodoviários), da banca, das infraestruturas do mercado financeiro, da saúde (prestadores de cuidados de saúde, hospitais e clínicas privadas), do fornecimento e distribuição de água potável, das infraestruturas digitais e de qualquer outro setor que seja essencial para o Estado-Membro em causa,

▼B

- c) funções cruciais do Estado, em especial nos domínios da defesa, da governação e do funcionamento das instituições, nomeadamente em eleições públicas ou no processo de votação, do funcionamento das infraestruturas económicas e civis, da segurança interna e das relações externas, nomeadamente nas missões diplomáticas,
- d) o armazenamento ou o tratamento de informações classificadas, ou
- e) equipas da administração pública de resposta a emergências.

5. Os ciberataques que constituem uma ameaça para a União incluem os perpetrados contra as suas instituições, órgãos e organismos, as suas delegações em países terceiros ou organizações internacionais, as suas operações e missões da política comum de segurança e defesa (PCSD) e os seus representantes especiais.

6. Sempre que for considerado necessário para atingir os objetivos da política externa e de segurança comum (PESC) nas disposições pertinentes do artigo 21.º do Tratado da União Europeia, podem também ser aplicadas medidas restritivas nos termos do presente regulamento em resposta aos ciberataques com um efeito significativo contra Estados terceiros ou organizações internacionais.

7. Para efeitos do presente regulamento, entende-se por:

- a) «Sistemas de informação», um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados digitais, bem como de dados digitais armazenados, tratados, extraídos ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;
- b) «Interferência no sistema de informação», o impedimento ou interrupção do funcionamento de um sistema de informação introduzindo dados digitais, transmitindo, danificando, apagando, deteriorando, alterando ou suprimindo esses dados, ou tornando-os inacessíveis;
- c) «Interferência nos dados», a eliminação, danificação, deterioração, alteração ou supressão de dados digitais de um sistema de informação, ou o impedimento do acesso a esses dados. Esta definição inclui igualmente o furto de dados, de fundos, de recursos económicos ou de propriedade intelectual.
- d) «Interceção de dados», a interceção, através de meios técnicos, das transferências não públicas de dados digitais para, a partir de ou no interior de um sistema de informação, incluindo as emissões eletromagnéticas de um sistema de informação que transmita esses dados digitais;

8. Para efeitos do presente regulamento, aplicam-se as seguintes definições adicionais:

- a) «Pedido», qualquer pedido, independentemente de assumir ou não forma contenciosa, apresentado antes ou depois da data de entrada em vigor do presente regulamento, no âmbito de um contrato ou transação ou com eles relacionado, nomeadamente:
 - i) um pedido destinado a obter a execução de uma obrigação decorrente de um contrato ou transação ou com estes relacionada,
 - ii) um pedido destinado a obter a prorrogação ou o pagamento de uma garantia ou contragarantia financeira ou de um crédito, independentemente da forma que assumam;
 - iii) um pedido de indemnização respeitante a um contrato ou transação;
 - iv) um pedido reconventional;

▼B

- v) um pedido destinado a obter o reconhecimento ou a execução, nomeadamente pelo procedimento de *exequatur*, de uma decisão judicial, uma decisão arbitral ou uma decisão equivalente, independentemente do lugar onde tenham sido proferidas;
- b) «Contrato ou transação», qualquer operação, independentemente da forma que assuma e da lei aplicável, que inclua um ou mais contratos ou obrigações similares que vincule as mesmas partes ou partes diferentes; para este efeito, um «contrato» inclui as garantias ou contragarantias, nomeadamente financeiras, e os créditos, juridicamente independentes ou não, bem como qualquer disposição conexa decorrente ou relacionada com a transação;
- c) «Autoridades competentes», as autoridades competentes dos Estados-Membros indicadas nos sítios Web enumerados no anexo II;
- d) «Recursos económicos», ativos de qualquer tipo, corpóreos ou incorpóreos, móveis ou imóveis, que não sejam fundos mas que possam ser utilizados para a obtenção de fundos, bens ou serviços;
- e) «Congelamento de recursos económicos», qualquer ação destinada a impedir a utilização de recursos económicos para a obtenção de fundos, bens ou serviços por qualquer meio, nomeadamente, mas não exclusivamente, a sua venda, locação ou hipoteca;
- f) «Congelamento de fundos», qualquer ação destinada a impedir o movimento, a transferência, a alteração, a utilização, o acesso, ou a operação de fundos por qualquer meio suscetível de resultar numa alteração do respetivo volume, montante, localização, propriedade, posse, natureza, destino ou qualquer outra alteração suscetível de permitir a sua utilização, incluindo a gestão de carteiras;
- g) «Fundos», ativos financeiros e benefícios económicos de qualquer tipo, nomeadamente, mas não exclusivamente:
 - i) numerário, cheques, direitos sobre numerário, livranças, ordens de pagamento e outros instrumentos de pagamento;
 - ii) depósitos em instituições financeiras ou outras entidades, saldos de contas, créditos e títulos de crédito;
 - iii) valores mobiliários e títulos de dívida de negociação aberta ao público ou restrita, incluindo ações e outros títulos de participação, certificados representativos de valores mobiliários, obrigações, promissórias, títulos de subscrição, títulos de dívida a longo prazo e contratos sobre instrumentos derivados;
 - iv) juros, dividendos ou outros rendimentos gerados por ativos ou mais-valias provenientes de ativos;
 - v) créditos, direitos de compensação, garantias, garantias de boa execução e outros compromissos financeiros;
 - vi) cartas de crédito, conhecimentos de embarque e comprovativos de vendas; e
 - vii) documentos que atestem a detenção de fundos ou recursos financeiros;

▼B

- h) «Território da União», os territórios dos Estados-Membros aos quais se aplica o Tratado, nas condições nele estabelecidas, incluindo o seu espaço aéreo.

Artigo 2.º

Os fatores determinantes para aferir do efeito significativo de um ciberratatque, a que se refere o artigo 1.º, n.º 1, incluem um dos seguintes elementos:

- a) O âmbito, a dimensão, o impacto ou a gravidade da perturbação causada, incluindo sobre as atividades económicas e sociais, os serviços essenciais, as funções cruciais do Estado, a ordem pública ou a segurança pública;
- b) O número de pessoas singulares ou coletivas, entidades ou organismos afetados;
- c) O número de Estados-Membros afetados;
- d) O montante das perdas económicas causadas, por exemplo, com o furto, em grande escala, de fundos, recursos económicos ou propriedade intelectual;
- e) Os benefícios económicos obtidos pelo infrator para si próprio ou para terceiros;
- f) A quantidade ou a natureza dos dados furtados ou a dimensão das violações de dados; ou
- g) A natureza dos dados comercialmente sensíveis a que se teve acesso.

Artigo 3.º

1. São congelados todos os fundos e recursos económicos pertencentes, na posse ou que se encontrem à disposição ou sob o controlo das pessoas singulares ou coletivas, entidades ou organismos enumerados no anexo I.

2. É proibido colocar, direta ou indiretamente, fundos ou recursos económicos à disposição das pessoas singulares ou coletivas, entidades ou organismos enumerados no anexo I, ou disponibilizá-los em seu proveito.

3. O anexo I inclui, tal como identificados pelo Conselho nos termos do artigo 5.º, n.º 1, da Decisão (PESC) 2019/797:

- a) As pessoas singulares ou coletivas, entidades ou organismos que são responsáveis por ciberataques ou tentativa de ciberataques;
- b) As pessoas singulares ou coletivas, entidades ou organismos que prestam apoio financeiro, técnico ou material ou estejam de qualquer outro modo envolvidos em ciberataques ou na tentativa de ciberataques, nomeadamente planeando tais ataques, preparando-os, participando neles, dirigindo-os, prestando assistência na sua execução ou incentivando-os ou tornando-os possíveis, por ação ou omissão;
- c) As pessoas singulares ou coletivas, entidades ou organismos associados às pessoas singulares ou coletivas, entidades ou organismos abrangidos pelas alíneas a) e b) do presente número.

▼B

Artigo 4.º

1. Em derrogação do artigo 3.º, as autoridades competentes dos Estados-Membros podem autorizar a liberação de determinados fundos ou recursos económicos congelados ou a disponibilização de determinados fundos ou recursos económicos, nas condições que considerem adequadas, após terem determinado que os fundos ou recursos económicos em causa:

- a) ►C1 São necessários para satisfazer as necessidades básicas das pessoas singulares ou coletivas, entidades ou organismos enumerados no anexo I ◄ e dos familiares dependentes das pessoas singulares em causa, incluindo o pagamento de alimentos, rendas ou empréstimos hipotecários, medicamentos e tratamentos médicos, impostos, apólices de seguro e taxas de serviços públicos;
- b) Se destinam exclusivamente ao pagamento de honorários profissionais razoáveis ou ao reembolso de despesas associadas à prestação de serviços jurídicos;
- c) Se destinam exclusivamente ao pagamento de encargos ou taxas de serviço correspondentes à manutenção ou gestão normal de fundos ou recursos económicos congelados;
- d) São necessários para cobrir despesas extraordinárias, desde que a autoridade competente em causa tenha comunicado às autoridades competentes dos demais Estados-Membros e à Comissão, pelo menos duas semanas antes da concessão da autorização, os motivos por que considera que deve ser concedida uma autorização específica; ou
- e) Devem ser creditados ou debitados numa conta de uma missão diplomática ou consular ou de uma organização internacional que goze de imunidades nos termos do direito internacional, desde que esses pagamentos se destinem a ser utilizados para fins oficiais da missão diplomática ou consular ou da organização internacional.

2. O Estado-Membro em causa informa os demais Estados-Membros e a Comissão sobre as autorizações concedidas nos termos do n.º 1, no prazo de duas semanas a contar da autorização.

Artigo 5.º

1. Em derrogação do artigo 3.º, n.º 1, as autoridades competentes dos Estados-Membros podem autorizar a liberação de determinados fundos ou recursos económicos congelados, se estiverem preenchidas as seguintes condições:

- a) Os fundos ou recursos económicos são objeto de uma decisão arbitral proferida antes da data em que a pessoa singular ou coletiva, entidade ou organismo a que se refere o artigo 3.º foram incluídos na lista do anexo I, ou de uma decisão judicial ou administrativa proferida na União ou de uma decisão judicial executória no Estado-Membro em causa, anterior ou posterior a essa data;
- b) Os fundos ou recursos económicos serão exclusivamente utilizados para satisfazer créditos garantidos por essa decisão ou por esta reconhecidos como válidos, nos limites fixados pelas disposições legislativas e regulamentares que regem os direitos das pessoas titulares desses créditos;
- c) O beneficiário da decisão não é uma das pessoas singulares ou coletivas, entidades ou organismos enumerados no anexo I; e
- d) O reconhecimento da decisão não é contrário à ordem pública no Estado-Membro em causa.

▼B

2. O Estado-Membro em causa informa os demais Estados-Membros e a Comissão sobre as autorizações concedidas nos termos do n.º 1, no prazo de duas semanas a contar da autorização.

Artigo 6.º

1. Em derrogação do artigo 3.º, n.º 1, e desde que uma pessoa singular ou coletiva, entidade ou organismo enumerado no anexo I deva proceder a um pagamento por força de um contrato ou acordo celebrado ou de uma obrigação contraída por essa pessoa singular ou coletiva, entidade ou organismo antes da data da sua inclusão no anexo I, as autoridades competentes dos Estados-Membros podem autorizar, nas condições que considerarem adequadas, a liberação de determinados fundos ou recursos económicos congelados, desde que a autoridade competente em causa tenha determinado que:

- a) Os fundos ou recursos económicos serão utilizados num pagamento a efetuar por uma pessoa singular ou coletiva, entidade ou organismo enumerado no anexo I; e
- b) O pagamento não é contrário ao artigo 3.º, n.º 2.

2. O Estado-Membro em causa informa os demais Estados-Membros e a Comissão sobre as autorizações concedidas nos termos do n.º 1, no prazo de duas semanas a contar da autorização.

Artigo 7.º

1. O artigo 3.º, n.º 2, não obsta a que as contas congeladas sejam creditadas por instituições financeiras ou de crédito que recebam fundos transferidos por terceiros para a conta de uma pessoa singular ou coletiva, entidade ou organismo, desde que todos os valores creditados nessas contas sejam igualmente congelados. A instituição financeira ou de crédito informa sem demora as autoridades competentes acerca dessas transações.

2. O artigo 3.º, n.º 2, não é aplicável ao crédito em contas congeladas de:

- a) Juros ou outros rendimentos dessas contas;
- b) Pagamentos devidos por força de contratos ou acordos celebrados ou de obrigações contraídas antes da data da inclusão no anexo I da pessoa singular ou coletiva, entidade ou organismo referidos no artigo 3.º, n.º 1; ou
- c) Pagamentos devidos por força de decisões judiciais, administrativas ou arbitrais proferidas num Estado-Membro ou executórias no Estado-Membro em causa,

desde que os referidos juros, outros rendimentos e pagamentos continuem sujeitos às medidas previstas no artigo 3.º, n.º 1.

Artigo 8.º

1. Sem prejuízo das normas aplicáveis em matéria de transmissão de informações, confidencialidade e sigilo profissional, as pessoas singulares e coletivas, as entidades e os organismos devem:

▼B

- a) Comunicar imediatamente todas as informações que possam facilitar o cumprimento do presente regulamento, tal como os dados relativos às contas e aos montantes congelados nos termos do artigo 3.º, n.º 1, à autoridade competente do Estado-Membro onde residem ou estão estabelecidos, e transmitir tais informações, diretamente ou através do Estado-Membro, à Comissão; e
 - b) Colaborar com as autoridades competentes em qualquer verificação das informações a que se refere a alínea a).
2. As informações adicionais recebidas diretamente pela Comissão devem ser disponibilizadas aos Estados-Membros.
3. As informações comunicadas ou recebidas ao abrigo do presente artigo só podem ser utilizadas para os fins para os quais foram comunicadas ou recebidas.

Artigo 9.º

É proibido participar, com conhecimento de causa e intencionalmente, em atividades cujo objeto ou efeito seja contornar as medidas a que se refere o artigo 3.º.

Artigo 10.º

1. O congelamento de fundos e recursos económicos, ou a recusa da sua disponibilização, quando de boa-fé e no pressuposto de que essas ações são conformes com o presente regulamento, não implicam qualquer responsabilidade para a pessoa singular ou coletiva, entidade ou organismo que as pratique, nem para os seus diretores ou assalariados, a não ser que fique provado que os fundos e recursos económicos foram congelados ou retidos por negligência.
2. As ações de pessoas singulares ou coletivas, entidades ou organismos em nada responsabilizam essas pessoas singulares ou coletivas, entidades ou organismos caso não tivessem conhecimento, nem tivessem motivos razoáveis para suspeitar que as suas ações constituiriam uma infração às medidas estabelecidas no presente regulamento.

Artigo 11.º

1. Não é satisfeito qualquer pedido relacionado com contratos ou transações cuja execução tenha sido afetada, direta ou indiretamente, total ou parcialmente, pelas medidas impostas ao abrigo do presente regulamento, incluindo pedidos de indemnização ou qualquer outro pedido desse tipo, tal como um pedido de compensação ou um pedido ao abrigo de uma garantia, em especial um pedido de prorrogação ou de pagamento de uma garantia ou contragarantia, nomeadamente financeira, independentemente da forma que assuma, se for apresentado por:
- a) Pessoas singulares ou coletivas, entidades ou organismos designados enumerados no anexo I;
 - b) Pessoas singulares ou coletivas, entidades ou organismos que atuem por intermédio ou em nome das pessoas singulares ou coletivas, entidades ou organismos referidos na alínea a).
2. Nos procedimentos para execução de um pedido, o ónus da prova de que a satisfação do pedido não é proibida pelo n.º 1 cabe à pessoa singular ou coletiva, entidade ou organismo que requer a execução do pedido.
3. O presente artigo não prejudica o direito das pessoas singulares ou coletivas, entidades e organismos referidos no n.º 1 a um controlo judicial da legalidade do não cumprimento das obrigações contratuais em conformidade com o presente regulamento.

*Artigo 12.º*

1. A Comissão e os Estados-Membros informam-se reciprocamente das medidas tomadas por força do presente regulamento e partilham todas as outras informações pertinentes de que disponham a respeito do presente regulamento, em especial informações relativas:

- a) A fundos congelados ao abrigo do artigo 3.º, e autorizações concedidas ao abrigo dos artigos 4.º, 5.º e 6.º; e
- b) A violações do presente regulamento e problemas relacionados com a sua aplicação, assim como às sentenças proferidas pelos tribunais nacionais.

2. Os Estados-Membros informam-se reciprocamente e a Comissão de quaisquer outras informações pertinentes de que disponham suscetíveis de afetar a aplicação efetiva do presente regulamento.

Artigo 13.º

1. Caso o Conselho decida impor as medidas referidas no artigo 3.º a uma pessoa singular ou coletiva, entidade ou organismo, altera o anexo I em conformidade.

2. O Conselho comunica a decisão a que se refere o n.º1, incluindo os motivos para a inclusão na lista, à pessoa singular ou coletiva, entidade ou organismo em causa, quer diretamente, se o endereço for conhecido, quer através da publicação de um aviso, dando-lhe a oportunidade de apresentar as suas observações.

3. Caso sejam apresentadas observações ou novos elementos de prova substanciais, o Conselho reaprecia a decisão a que se refere o n.º 1 e informa do facto a pessoa singular ou coletiva, entidade ou organismo.

4. A lista constante do anexo I é revista a intervalos regulares, no mínimo, de 12 em 12 meses.

5. A Comissão fica habilitada a alterar o anexo II com base em informações transmitidas pelos Estados-Membros.

Artigo 14.º

1. O anexo I inclui os motivos para a inclusão na lista das pessoas singulares ou coletivas, entidades ou organismos em causa.

2. O anexo I contém, sempre que estejam disponíveis, as informações necessárias à identificação das pessoas singulares ou coletivas, entidades ou organismos em causa. Essas informações podem incluir, no que se refere às pessoas singulares, o nome, incluindo os pseudónimos, a data e o local de nascimento, a nacionalidade, os números do passaporte e bilhete de identidade, o sexo, o endereço, se for conhecido, e as funções ou a profissão exercidas. Tratando-se de pessoas coletivas, entidades e organismos, essas informações podem incluir o nome, o local e a data de registo, o número de registo e o local de atividade.

Artigo 15.º

1. Os Estados-Membros estabelecem as regras relativas às sanções aplicáveis em caso de violação do disposto no presente regulamento e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

▼B

2. Os Estados-Membros notificam a Comissão, sem demora após a entrada em vigor do presente regulamento, das regras referidas no n.º 1, e notificam-na de qualquer alteração posterior que as afete.

Artigo 16.º

1. A Comissão procede ao tratamento dos dados pessoais a fim de executar as suas atribuições decorrentes do presente regulamento. Essas atribuições incluem:

- a) O aditamento do conteúdo do anexo I à lista eletrónica consolidada de pessoas, grupos e entidades a quem a União aplicou sanções financeiras, bem como no mapa interativo de sanções, ambos acessíveis ao público;
- b) O tratamento das informações sobre o impacto das medidas previstas no presente regulamento, nomeadamente o valor dos fundos congelados, bem como sobre as autorizações concedidas pelas autoridades competentes.

2. Para efeitos do presente regulamento, o serviço da Comissão indicado no anexo II é designado «responsável pelo tratamento» para a Comissão, na aceção do artigo 3.º, ponto 8), do Regulamento (UE) 2018/1725, a fim de garantir que as pessoas singulares em causa possam exercer os seus direitos ao abrigo desse regulamento.

Artigo 17.º

1. Os Estados-Membros designam as autoridades competentes referidas no presente regulamento e identificam-nas nos sítios Web indicados no anexo II. Os Estados-Membros notificam à Comissão eventuais alterações dos endereços dos seus sítios Web indicados no anexo II.

2. Os Estados-Membros notificam a Comissão, sem demora após a entrada em vigor do presente regulamento, do nome das respetivas autoridades competentes, incluindo os seus dados de contacto, bem como de qualquer alteração subsequente das mesmas.

3. Sempre que o presente regulamento previr uma obrigação de notificação, de informação ou qualquer outra forma de comunicação com a Comissão, o endereço e outros dados de contacto a utilizar são os indicados no anexo II.

Artigo 18.º

O presente regulamento aplica-se:

- a) No território da União, incluindo o seu espaço aéreo;
- b) A bordo das aeronaves ou embarcações sob jurisdição de um Estado-Membro;
- c) A todas as pessoas singulares, nacionais de um Estado-Membro, dentro ou fora do território da União;
- d) A todas as pessoas coletivas, entidades ou organismos, dentro ou fora do território da União, registados ou constituídos nos termos do direito de um Estado-Membro;
- e) A todas as pessoas coletivas, entidades ou organismos relativamente a qualquer atividade económica que exerçam, total ou parcialmente, na União.

▼B

Artigo 19.º

O presente regulamento entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

▼B

ANEXO I

Lista de pessoas singulares e coletivas, entidades e organismos a que se refere o artigo 3.º

▼M1

A. Pessoas singulares

▼M3

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
1.	GAO Qiang	Data de nascimento: 4 de outubro de 1983 Local de nascimento: Província de Shandong, China Endereço: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nacionalidade: chinesa Sexo: masculino	Gao Qiang está envolvido na «Operation Cloud Hopper», uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A «Operação Cloud Hopper» atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. O interveniente conhecido por «APT10» («Advanced Persistent Threat 10») (t.c.p. «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») realizou a «Operation Cloud Hopper». Pode estabelecer-se uma ligação entre Gao Qiang e o interveniente «APT10», nomeadamente através da associação de Gao Qiang à infraestrutura de comando e controlo do interveniente «APT10». Além disso, a Huaying Haitai, entidade designada por apoiar e facilitar a «Operation Cloud Hopper», empregou Gao Qiang. Gao Qiang tem ligações a Zhang Shilong, também designado pela sua ligação à «Operation Cloud Hopper». Por conseguinte, Gao Qiang está associado à Huaying Haitai e a Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Data de nascimento: 10 de setembro de 1981 Local de nascimento: China Endereço: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidade: chinesa Sexo: masculino	Zhang Shilong está envolvido na «Operation Cloud Hopper», uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A «Operação Cloud Hopper» atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos.	30.7.2020

▼ M3

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			O interveniente conhecido por «APT10» («Advanced Persistent Threat 10») (t.c.p. «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») realizou a «Operation Cloud Hopper». Pode estabelecer-se uma ligação entre Zhang Shilong e o interveniente «APT10», nomeadamente através do programa malicioso que Zhang Shilong desenvolveu e testou em ligação com os ciberataques levados a cabo pelo interveniente «APT10». Além disso, a Huaying Haitai, entidade designada por apoiar e facilitar a «Operation Cloud Hopper», empregou Zhang Shilong. Zhang Shilong tem ligações a Gao Qiang, também designado pela sua ligação à «Operation Cloud Hopper». Por conseguinte, Zhang Shilong está associado à Huaying Haitai e a Gao Qiang.	

▼ M1

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data de nascimento: 27 de maio de 1972 Local de nascimento: Oblast de Perm, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 120017582 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17 de abril de 2017 a 17 de abril de 2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Alexey Minin participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos. Como agente de apoio em matéria de informações humanas da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Alexey Minin fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data de nascimento: 31 de julho de 1977 Local de nascimento: Oblast de Murmanskaya, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 100135556 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17 de abril de 2017 a 17 de abril de 2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Aleksei Morenets participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos. Como «ciberoperador» da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Aleksei Morenets fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
5.	Evgenii Mikhailovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data de nascimento: 26 de julho de 1981 Local de nascimento: Kursk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 100135555 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17 de abril de 2017 a 17 de abril de 2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Evgenii Serebriakov participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos. Como «ciberoperador» da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Evgenii Serebriakov fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020
6.	Oleg Mikhailovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data de nascimento: 24 de agosto de 1972 Local de nascimento: Ulyanovsk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 120018866 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17 de abril de 2017 a 17 de abril de 2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Oleg Sotnikov participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos. Como agente de apoio em matéria de informações humanas da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Oleg Sotnikov fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020

▼ M1

▼ M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data de nascimento: 15 de novembro de 1990 Local de nascimento: Kursk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Nacionalidade: russa Sexo: masculino	Dmitry Badin participou num ciberataque com efeitos importantes contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>). Enquanto agente dos serviços de informação militares do 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GU/GRU), Dmitry Badin fez parte de uma equipa de agentes dos serviços de informações militares russos que lançaram um ataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) em abril e maio de 2015. O referido ciberataque visou o sistema informático do Parlamento Federal alemão e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТИУКОВ Data de nascimento: 21 de fevereiro de 1961 Nacionalidade: russa Sexo: masculino	Igor Kostyukov é o atual chefe da Direção-Geral do Estado-Maior das Forças Armadas da Federação da Rússia (GU/GRU), tendo anteriormente ocupado o cargo de primeiro chefe adjunto. Uma das unidades sob o seu comando é o 85.º Centro Principal de Serviços Especiais (GTsSS), também chamada «unidade militar 26165» (outros nomes por que é conhecida no setor da cibersegurança: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» e «Strontium»). No exercício desse cargo, Igor Kostyukov é responsável por ciberataques lançados pelo GTsSS, incluindo ataques com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros. Mais especificamente, agentes de informações militares do GTsSS participaram no ciberataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) de abril e maio de 2015, bem como na tentativa de ciberataque destinado a piratear a rede <i>Wi-Fi</i> da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos. O ciberataque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.	22.10.2020

▼M1

B. Pessoas coletivas, entidades e organismos

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Tcp Haitai Technology Development Co. Ltd Localização: Tianjin, China	A Huaying Haitai prestou apoio financeiro, técnico ou material e facilitou a «Operation Cloud Hopper», uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A «Operação Cloud Hopper» atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. O interveniente conhecido por «APT10» («Advanced Persistent Threat 10») (t.c.p. «Red Apollo», «CVNX», «Stone Panda», «MenuPass» e «Potassium») realizou a «Operation Cloud Hopper». Pode estabelecer-se uma ligação entre a Huaying Haitai e o interveniente «APT10». Além disso, a Huaying Haitai empregou Gao Qiang e Zhang Shilong, ambos designados pela sua ligação à «Operation Cloud Hopper». Por conseguinte, a Huaying Haitai está associada a Gao Qiang e a Zhang Shilong.	30.7.2020
2.	Chosun Expo	Tcp Chosen Expo; Korea Export Joint Venture Localização: RPDC	A Chosun Expo prestou apoio financeiro, técnico ou material e facilitou uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros, incluindo os ciberataques conhecidos por «WannaCry» e os ciberataques contra a autoridade polaca de supervisão financeira e a Sony Pictures Entertainment, bem como o roubo informático do Banco do Bangladesh e a tentativa de roubo informático do Banco Tien Phong do Vietname. O ciberataque «WannaCry» perturbou os sistemas de informação em todo o mundo, atacando os sistemas de informação com programas sequestradores e bloqueando o acesso aos dados. Afetou os sistemas de informação de empresas na União, incluindo os sistemas de informação relativos aos serviços necessários para a manutenção de serviços essenciais e de atividades económicas nos Estados-Membros.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			O interveniente conhecido por «APT38» («Advanced Persistent Threat 38») ou o «Lazarus Group» realizaram o ciberataque «WannaCry». Pode estabelecer-se uma ligação entre a Chosun Expo e o interveniente «APT38» e o grupo «Lazarus», nomeadamente através das contas utilizadas para os ciberataques.	
3.	Centro Principal de Tecnologias Especiais (GTsST) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU)	Endereço: 22 Kirova Street, Moscovo, Federação da Rússia	O Centro Principal de Tecnologias Especiais (GTsST) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), também conhecido pelo seu código postal de campanha 74455, é responsável por ciberataques com um efeito significativo, provenientes do exterior da União e que constituem uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros, incluindo os ciberataques publicamente conhecidos por «NotPetya» ou «EternalPetya», em junho de 2017, e os ciberataques que visaram uma rede elétrica ucraniana no inverno de 2015 e 2016. Os ciberataques «NotPetya» ou «EternalPetya» impediram o acesso aos dados em várias empresas da União, da Europa em geral e de todo o mundo, atacando os computadores com programas sequestradores e bloqueando o acesso aos dados, o que resultou, nomeadamente, em significativos prejuízos económicos. O ciberataque a uma rede de energia ucraniana teve como resultado o não funcionamento de partes da referida rede durante o inverno. O interveniente conhecido por «Sandworm» (t.c.p. «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» e «Telebots»), também responsável pelo ataque à rede elétrica ucraniana, realizou os ciberataques «NotPetya» ou «EternalPetya». O Centro Principal de Tecnologias Especiais (GTsST) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU) tem um papel ativo nas ciberatividades realizadas pelo interveniente «Sandworm», pelo que pode estabelecer-se uma ligação entre ambos.	30.7.2020

▼ M1▼ M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
4.	85 th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia]	Endereço: Komsomol'skiy Prospekt, 20, Moscovo, 119146, Federação da Rússia	O 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), também chamada «unidade militar 26165» (outros nomes por que é conhecida no setor da cibersegurança: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» e «Strontium»), é responsável por ciberataques com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros. Mais especificamente, agentes de informações militares do GTsSS participaram no ciberataque contra o Parlamento Federal alemão (<i>Deutscher Bundestag</i>) de abril e maio de 2015, bem como na tentativa de ciberataque destinado a piratear a rede <i>Wi-Fi</i> da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos. O ciberataque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da chanceler federal, Angela Merkel.	22.10.2020

▼B*ANEXO II***Sítios Web que contêm informações sobre as autoridades competentes e endereço da Comissão Europeia para o envio das notificações****▼M4****BÉLGICA**

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGÁRIA

<https://www.mfa.bg/en/EU-sanctions>

CHÉQUIA

www.financnianalytickurad.cz/mezinarodni-sankce.html

DINAMARCA

<http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/>

ALEMANHA

<https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html>

ESTÓNIA

<https://vm.ee/et/rahvusvahelised-sanktsioonid>

IRLANDA

<https://www.dfa.ie/our-role/policies/ireland-in-the-eu/eu-restrictive-measures/>

GRÉCIA

<http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html>

ESPANHA

<https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx>

FRANÇA

<http://www.diplomatie.gouv.fr/fr/autorites-sanctions/>

CROÁCIA

<https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955>

ITÁLIA

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CHIPRE

<https://mfa.gov.cy/themes/>

LETÓNIA

<http://www.mfa.gov.lv/en/security/4539>

LITUÂNIA

<http://www.urm.lt/sanctions>

LUXEMBURGO

<https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html>

HUNGRIA

<https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato>

▼ M4**MALTA**

<https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx>

PAÍSES BAIXOS

<https://www.rijksoverheid.nl/onderwerpen/internationale-sancties>

ÁUSTRIA

<https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/>

POLÓNIA

<https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe>

<https://www.gov.pl/web/diplomacy/international-sanctions>

PORTUGAL

<https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas>

ROMÉNIA

<http://www.mae.ro/node/1548>

ESLOVÉNIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

ESLOVÁQUIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLÂNDIA

<https://um.fi/pakotteet>

SUÉCIA

<https://www.regeringen.se/sanktioner>

Endereço da Comissão Europeia para o envio das notificações:

Comissão Europeia

Direção-Geral da Estabilidade Financeira, dos Serviços Financeiros e da União dos Mercados de Capitais (DG FISMA)

Rue de Spa 2

B-1049 Bruxelas, Bélgica

Correio eletrónico: relex-sanctions@ec.europa.eu