PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

PL 298/XXIV/2024

2025.02.06

Exposição de motivos

A presente proposta de lei visa autorizar o Governo a aprovar o regime jurídico da cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União.

A preservação da cibersegurança desempenha um papel crucial em matéria de segurança nacional e internacional, no funcionamento do Estado e dos agentes económicos, bem como na construção da confiança dos cidadãos no processo de modernização digital da Administração Pública.

A transposição para o ambiente digital de funções essenciais das atividades institucionais e da vivência pessoal e profissional dos cidadãos justifica o reforço do quadro regulamentar e organizacional de cibersegurança, executado em harmonia com todo o espaço e em defesa contra ciberameaças comuns.

Esta iniciativa legislativa ocorre perante a consciência, não só da gravidade premente colocada pelas múltiplas ciberameaças, como do elevado potencial disruptivo das suas ações hostis contra ativos digitais, sendo imperioso um reforço da capacitação nacional para a prevenção de atos que possam condicionar a segurança e o interesse nacional, bem como as múltiplas dinâmicas funcionais e produtivas da sociedade portuguesa.

De facto, perante o aumento assinalável da quantidade e da sofisticação das ameaças, bem como a crescente utilização e dependência do uso das tecnologias de informação e comunicação por toda a sociedade, afigura-se indispensável assegurar a generalização da cibersegurança na cultura organizacional do tecido empresarial português e nas entidades, órgãos e serviços que constituem a Administração Pública.

Com efeito, o aumento da ocorrência de incidentes de cibersegurança pode comprometer a

Proposta de Lei n.º .....

segurança e o interesse nacional, acarretar perigo para a vida humana, perdas de natureza financeira, bem como comprometer a confidencialidade, a integridade e a disponibilidade da informação, das redes e dos sistemas de informação da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais. Em face destas ameaças e considerando o disposto na Diretiva a transpor, o regime aprovado pelo decreto-lei autorizado pela presente proposta de lei expande significativamente o conjunto de entidades abrangidas pelo regime, priorizando, por um lado, a generalização da prevenção dos riscos de cibersegurança, mas graduando a exigência regulatória em função da dimensão da entidade e da importância da sua atividade, bem como privilegiando a proporcionalidade das medidas aplicáveis. O seu âmbito de aplicação abrange uma parte significativa da Administração Pública, adaptando o regime à dimensão e tipologia da entidade pública em causa. É ainda de assinalar que, tal como admitido pela Diretiva a transpor, o regime aprovado pelo decreto-lei autorizado exclui do seu âmbito de aplicação as entidades públicas nos domínios da segurança nacional, da segurança pública, da defesa e dos serviços de informações.

Entre os aspetos relevantes do regime aprovado pelo decreto-lei autorizado, encontra-se ainda o aprofundamento de três instrumentos fundamentais para as políticas públicas de cibersegurança: a Estratégia Nacional de Segurança do Ciberespaço, definindo as prioridades e os objetivos estratégicos nacionais em matéria de cibersegurança; o Plano Nacional de Resposta a Crises e Incidentes de Cibersegurança em grande escala, regulando e aperfeiçoando a gestão deste tipo de incidentes; e o Quadro Nacional de Referência para a Cibersegurança, que reunirá e permitirá a divulgação de normas, padrões e boas práticas na gestão da cibersegurança.

Acresce que o quadro institucional do regime aprovado pelo decreto-lei autorizado é alargado em relação ao regime anterior, conforme imposto pela Diretiva a transpor. Nesse sentido, o Centro Nacional de Cibersegurança (CNCS) reforça a sua função de autoridade nacional de cibersegurança, destacando-se ainda o estabelecimento de autoridades de supervisão "setoriais" e "especiais", que exercem supervisão sobre setores específicos da economia,

.....

Proposta de Lei n.º .....

assim se garantindo a estabilidade na supervisão de cada um dos setores abrangidos, bem como aliviando as tarefas transversais cometidas ao CNCS.

No plano interadministrativo, o modelo proposto estabelece uma arquitetura de convergência, de cooperação e de interoperabilidade entre as várias entidades nacionais competentes em matéria de cibersegurança e de segurança interna e externa, fomentando, em particular, a transversalidade dos fluxos de informação relevante e a partilha de contributos táticos na resposta a incidentes entre as entidades nacionais competentes em matéria de cibersegurança, numa lógica de maximização das capacidades públicas portuguesas para a prevenção, a deteção precoce, a mitigação, a repressão e a responsabilização de ciberameaças.

O fortalecimento da cooperação com o setor privado é outro dos eixos do desenho institucional previsto no regime aprovado pelo decreto-lei autorizado, fomentando-se a colaboração entre as autoridades competentes e os privados nas várias matérias relevantes.

Quanto ao modelo de gestão dos riscos previsto no regime aprovado pelo decreto-lei autorizado, este consiste na fixação de padrões pré-definidos de risco, aplicáveis a cada setor e tipo de entidade, e na aplicação de medidas de prevenção correspondentes, acrescendo ainda uma análise do risco residual. Este modelo permite desonerar as autoridades de uma análise casuística do risco de cada entidade abrangida, facilitando ainda que as entidades abrangidas conheçam a categoria em que se inserem e, assim, as medidas mínimas que devem adotar. Nestes termos, o modelo proposto introduz simplicidade, previsibilidade e uma melhor adequação das medidas obrigatórias ao quadro de ameaças aplicável a cada setor de atividade. Por outro lado, o modelo fomenta a criação de um mercado de certificação em cibersegurança, o que terá utilidade económica e permitirá generalizar uma presunção de conformidade das entidades.

Por fim, quanto ao modelo de supervisão previsto no regime aprovado pelo decreto-lei autorizado, este, refletindo o disposto na Diretiva a transpor, prevê um regime dual, diferenciando o tratamento a dar às entidades essenciais e importantes em função dos riscos

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

de cibersegurança associados a cada categoria, em cumprimento, mais uma vez, do princípio da proporcionalidade.

O decreto-lei autorizado concentrou-se na construção do quadro jurídico aplicável em matéria de cibersegurança. Contudo, a entrada em vigor do novo regime implicará necessariamente um reforço significativo da capacidade do CNCS e uma nova reflexão sobre o seu enquadramento institucional.

Assim:

Nos termos da alínea *d)* do n.º 1 do artigo 197.º da Constituição, o Governo apresenta à Assembleia da República a seguinte proposta de lei:

Artigo 1.º

Objeto

Fica o Governo autorizado a aprovar o regime jurídico da cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União.

Artigo 2.º

Sentido e extensão

A autorização referida no artigo anterior tem como sentido e extensão:

a) Aprovar o regime jurídico da cibersegurança, transpondo, para a ordem jurídica interna, a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 1);

b) Executar, na ordem jurídica interna, as obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril, relativo à

Proposta de Lei n.º .....

ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança), implementando um quadro nacional de certificação da cibersegurança;

c) Proceder à nona alteração da Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho, pelo Decreto-Lei n.º 49/2017, de 24 de maio, pelas Leis n.ºs 21/2019, de 25 de fevereiro e 73/2021, de 12 de novembro, pelo Decreto-Lei n.º 122/2021, de 30 de dezembro, pela Lei n.º 24/2022, de 16 de dezembro e pelos Decretos-Leis n.ºs 41/2023, de 2 de junho e n.º 99-A/2023, de 27 de outubro;

d) Proceder à segunda alteração da Lei do Cibercrime, aprovada pela Lei n.º 109/2009, 15 de setembro, alterada pela Lei n.º 79/2021, de 24 de novembro.

e) Proceder à segunda alteração à Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, alterada pelo Decreto-Lei n.º 114/2024, de 20 de dezembro.

Artigo 3.º

Sentido e extensão relativos ao disposto na alínea *a)* do artigo 2.º

A autorização legislativa referida na alínea *a)* do artigo 2.º é concedida com o seguinte sentido e extensão:

a) Ampliar o âmbito de aplicação do regime jurídico da cibersegurança, excluindo as entidades nos domínios da segurança nacional, da segurança pública, da defesa e dos serviços de informações, mas abrangendo as designadas entidades essenciais, importantes e públicas relevantes, distinguidas mediante um conjunto de critérios relacionados com a importância, a dimensão e a tipologia da entidade, incluindo, designadamente:

i) No que respeita às entidades essenciais, o respetivo grau de exposição a

Proposta de Lei n.º .....

riscos, a dimensão da entidade, a importância da sua atividade e a probabilidade de ocorrência de incidentes e a sua gravidade, social e económica;

ii) No que respeita a entidades importantes, a não aplicação dos critérios aplicáveis às entidades essenciais;

iii) No que respeita a entidades públicas relevantes de Grupo A, a não aplicação dos critérios aplicáveis às entidades essenciais ou importantes, a natureza da entidade pública e a sua dimensão;

iv) No que respeita a entidades públicas relevantes de Grupo B, a não aplicação dos critérios aplicáveis às entidades essenciais ou importantes, a natureza da entidade pública e a sua dimensão;

b) Habilitar o desenvolvimento dos instrumentos estruturantes da segurança do ciberespaço, incluindo:

i) A Estratégia Nacional de Segurança do Ciberespaço, que definirá as prioridades e os objetivos estratégicos nacionais em matéria de cibersegurança;

ii) O Plano Nacional de Resposta a Crises e Incidentes de Cibersegurança em grande escala, regulando e aperfeiçoando a gestão deste tipo de incidentes;

iii) O Quadro Nacional de Referência para a Cibersegurança, reunindo e divulgando as normas, padrões e boas práticas na gestão da Cibersegurança;

c) Prever um novo quadro institucional da segurança do ciberespaço, incluindo, designadamente:

i) O Conselho Superior de Segurança do Ciberespaço, na qualidade de órgão consultivo do Primeiro-Ministro no domínio da cibersegurança;

ii) O CNCS, na qualidade de autoridade nacional de cibersegurança;

iii) O Gabinete Nacional de Segurança e a Autoridade Nacional de Comunicações, na qualidade de autoridades nacionais setoriais de

Proposta de Lei n.º .....

cibersegurança;

iv) A Autoridade de Supervisão de Seguros e Fundos de Pensões, a Comissão do Mercado de Valores Mobiliários e o Banco de Portugal, na qualidade de autoridades nacionais especiais de cibersegurança;

d) Prever um novo regime aplicável às avaliações de segurança e propostas emitidas pela Comissão de Avaliação de Segurança do Ciberespaço, bem como às decisões, cuja competência é atribuída ao membro do Governo responsável pela área da cibersegurança, de aplicação de restrições provisórias à utilização, a cessação de utilização ou exclusão de equipamentos, componentes ou serviços de tecnologias de informação e comunicação, considerados de elevado risco para a segurança do ciberespaço nacional;

e) Estabelecer um novo regime de gestão dos riscos de cibersegurança, incluindo, designadamente:

i) A previsão de obrigações próprias dos órgãos de gestão, direção e administração das entidades abrangidas;

ii) A previsão de um sistema de gestão de riscos de cibersegurança, constituído das medidas técnicas, operacionais e organizativas adequadas para gerir os riscos de cibersegurança;

iii) A imposição de uma análise do risco residual, da emissão de um relatório anual sobre cibersegurança e da designação de um responsável de cibersegurança e de um ponto de contacto permanente nas entidades abrangidas;

f) Prever um novo regime de prevenção e tratamento de incidentes de cibersegurança, incluindo, designadamente, o dever de as entidades abrangidas notificarem qualquer incidente significativo à autoridade de cibersegurança competente;

g) Prever um novo regime de supervisão e execução em matéria de cibersegurança, que habilita a autoridade de cibersegurança competente a supervisionar o cumprimento

do regime e a adotar, em relação às entidades abrangidas, medidas adequadas à prossecução daquele cumprimento, submetidas ao princípio da proporcionalidade e a garantias procedimentais, designadamente:

i. Inspeções no local e a supervisão remota;
ii. Auditorias de segurança e *ad hoc*;
iii. Verificações de segurança;
iv. Pedidos de informações e de apresentação das provas demonstrativas da aplicação das políticas e procedimentos de cibersegurança;
v. Advertências, ordens ou instruções vinculativas;
vi. Suspensão de certificação, autorização ou licença relativa à atividade da entidade;
vii. Solicitação ao órgão competente da suspensão da autorização ou da licença relativa à atividade da entidade;
viii. Bloqueio e redireccionamento de endereços de protocolo IP;

b) Estabelecer um novo regime sancionatório em matéria de cibersegurança, incluindo, designadamente, a previsão de um regime contraordenacional, a previsão da possibilidade de as entidades solicitarem fundamentadamente à autoridade de cibersegurança competente a dispensa da aplicação de coimas durante 12 meses a contar da entrada em vigor do regime, e ainda a impugnabilidade das decisões da autoridade de cibersegurança competente no âmbito de processos de contraordenação para os tribunais judiciais.

Artigo 4.º

Sentido e extensão relativos ao disposto na alínea *c)* do artigo 2.º

A autorização legislativa referida na alínea *c)* do artigo 2.º é concedida com o sentido e extensão de prever e regular um novo gabinete de crise, visando assegurar a condução de

.....

Proposta de Lei n.º .....

crises de cibersegurança com impacto na segurança interna.

Artigo 5.º

Sentido e extensão relativos ao disposto na alínea *d)* do artigo 2.º

A autorização legislativa referida na alínea *d)* do artigo 2.º é concedida com o sentido e extensão de proceder à despenalização de factos suscetíveis de consubstanciar os crimes de acesso ilegítimo e de interceção ilegítima mediante a verificação cumulativa de um conjunto de circunstâncias, incluindo, designadamente:

a) O agente atuar com a intenção única de identificar a existência de vulnerabilidades em sistema de informação, produtos e serviços de tecnologias de informação e comunicação, e com propósito de contribuir para a segurança do ciberespaço;

b) O agente não atuar com o propósito de obter vantagem económica ou promessa de vantagem económica decorrente da sua ação;

c) O agente comunicar imediatamente as eventuais vulnerabilidades identificadas, ao proprietário ou pessoa por ele designada para gerir o sistema de informação, produto ou serviço de tecnologias de informação e comunicação, ao titular de quaisquer dados obtidos e que se encontrem protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais;

d) A atuação do agente ser proporcional aos seus propósitos e estritamente limitada pelos mesmos;

e) A atuação do agente não violar dados pessoais protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Artigo 6.º

Duração

A autorização concedida pela presente lei tem a duração de 180 dias.

Visto e aprovado em Conselho de Ministros de (…)

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

DECRETO-LEI AUTORIZADO

Preâmbulo

O presente decreto-lei aprova o regime jurídico da cibersegurança, transpondo a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União.

A preservação da cibersegurança desempenha um papel crucial em matéria de segurança nacional e internacional, no funcionamento do Estado e dos agentes económicos, bem como na construção da confiança dos cidadãos no processo de modernização digital da Administração Pública.

A transposição para o ambiente digital de funções essenciais das atividades institucionais e da vivência pessoal e profissional dos cidadãos justifica o reforço do quadro regulamentar e organizacional de cibersegurança, executado em harmonia com todo o espaço e em defesa contra ciberameaças comuns.

Esta iniciativa legislativa ocorre perante a consciência, não só da gravidade premente colocada pelas múltiplas ciberameaças, como do elevado potencial disruptivo das suas ações hostis contra ativos digitais, sendo imperioso um reforço da capacitação nacional para a prevenção de atos que possam condicionar a segurança e o interesse nacional, bem como as múltiplas dinâmicas funcionais e produtivas da sociedade portuguesa.

De facto, perante o aumento assinalável da quantidade e da sofisticação das ameaças, bem como a crescente utilização e dependência do uso das tecnologias de informação e comunicação por toda a sociedade, afigura-se indispensável assegurar a generalização da cibersegurança na cultura organizacional do tecido empresarial português e nas entidades, órgãos e serviços que constituem a Administração Pública.

Com efeito, o aumento da ocorrência de incidentes de cibersegurança pode comprometer a segurança e o interesse nacional, acarretar perigo para a vida humana, perdas de natureza

Proposta de Lei n.º .....

financeira, bem como comprometer a confidencialidade, a integridade e a disponibilidade da informação, das redes e dos sistemas de informação da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais. Em face destas ameaças e considerando o disposto na Diretiva a transpor, o regime aprovado pelo presente decreto-lei expande significativamente o conjunto de entidades abrangidas pelo regime, priorizando, por um lado, a generalização da prevenção dos riscos de cibersegurança, mas graduando a exigência regulatória em função da dimensão da entidade e da importância da sua atividade, bem como privilegiando a proporcionalidade das medidas aplicáveis. O seu âmbito de aplicação abrange uma parte significativa da Administração Pública, adaptando o regime à dimensão e tipologia da entidade pública em causa. É ainda de assinalar que, tal como admitido pela Diretiva a transpor, o regime aprovado pelo presente decreto-lei exclui do seu âmbito de aplicação as entidades públicas nos domínios da segurança nacional, da segurança pública, da defesa e dos serviços de informações.

Entre os aspetos relevantes do regime aprovado pelo presente decreto-lei, encontra-se ainda o aprofundamento de três instrumentos fundamentais para as políticas públicas de cibersegurança: a Estratégia Nacional de Segurança do Ciberespaço, definindo as prioridades e os objetivos estratégicos nacionais em matéria de cibersegurança; o Plano Nacional de Resposta a Crises e Incidentes de Cibersegurança em grande escala, regulando e aperfeiçoando a gestão deste tipo de incidentes; e o Quadro Nacional de Referência para a Cibersegurança, que reunirá e permitirá a divulgação de normas, padrões e boas práticas na gestão da Cibersegurança.

Acresce que o quadro institucional do regime aprovado pelo presente decreto-lei é alargado em relação ao regime anterior, conforme imposto pela Diretiva a transpor. Nesse sentido, o Centro Nacional de Cibersegurança (CNCS) reforça a sua função de autoridade nacional de cibersegurança, destacando-se ainda o estabelecimento de autoridades de supervisão "setoriais" e "especiais", que exercem supervisão sobre setores específicos da economia, assim se garantindo a estabilidade na supervisão de cada um dos setores abrangidos, bem

Proposta de Lei n.º .....

como aliviando as tarefas transversais cometidas ao CNCS.

No plano interadministrativo, o modelo proposto estabelece uma arquitetura de convergência, de cooperação e de interoperabilidade entre as várias entidades nacionais competentes em matéria de cibersegurança e de segurança interna e externa, fomentando, em particular, a transversalidade dos fluxos de informação relevante e a partilha de contributos táticos na resposta a incidentes entre as entidades nacionais competentes em matéria de cibersegurança, numa lógica de maximização das capacidades públicas portuguesas para a prevenção, a deteção precoce, a mitigação, a repressão e a responsabilização de ciberameaças.

O fortalecimento da cooperação com o setor privado é outro dos eixos do desenho institucional previsto no regime aprovado presente pelo decreto-lei, fomentando-se a colaboração entre as autoridades competentes e os privados nas várias matérias relevantes.

Quanto ao modelo de gestão dos riscos previsto no regime aprovado pelo presente decreto-lei, este consiste na fixação de padrões pré-definidos de risco, aplicáveis a cada setor e tipo de entidade, e na aplicação de medidas de prevenção correspondentes, acrescendo ainda uma análise do risco residual. Este modelo permite desonerar as autoridades de uma análise casuística do risco de cada entidade abrangida, facilitando ainda que as entidades abrangidas conheçam a categoria em que se inserem e, assim, as medidas mínimas que devem adotar. Nestes termos, o modelo proposto introduz simplicidade, previsibilidade e uma melhor adequação das medidas obrigatórias ao quadro de ameaças aplicável a cada setor de atividade. Por outro lado, o modelo fomenta a criação de um mercado de certificação em cibersegurança, o que terá utilidade económica e permitirá generalizar uma presunção de conformidade das entidades.

Por fim, quanto ao modelo de supervisão previsto no regime aprovado pelo presente decreto-lei, este, refletindo o disposto na Diretiva a transpor, prevê um regime dual, diferenciando o tratamento a dar às entidades essenciais e importantes em função dos riscos de cibersegurança associados a cada categoria, em cumprimento, mais uma vez, do princípio

Proposta de Lei n.º .....

da proporcionalidade.

O presente decreto-lei tem, assim, como objetivo a consagração do novo quadro jurídico aplicável em matéria de cibersegurança, sem prejuízo de a entrada em vigor deste regime implicar necessariamente um reforço significativo da capacidade do CNCS e uma nova reflexão sobre o seu enquadramento institucional.

O presente decreto-lei foi submetido a consulta pública entre 22 de novembro e 31 de dezembro de 2024.

[Foram ouvidos os órgãos de governo próprio das Regiões Autónomas, a Comissão Nacional de Proteção de Dados, a Autoridade Nacional de Comunicações, o Gabinete Nacional de Segurança, o Centro Nacional de Cibersegurança, o Sistema de Segurança Interna, o Secretário-Geral do Sistema de Informações da República Portuguesa, a Autoridade Nacional de Emergência e Proteção Civil, o Banco de Portugal, a Comissão do Mercado de Valores Mobiliários, a Autoridade de Supervisão de Seguros e Fundos de Pensões, a Provedoria de Justiça, o Conselho Superior da Magistratura, o Conselho Superior dos Tribunais Administrativos e Fiscais, o Conselho Superior do Ministério Público e a Procuradoria-Geral da República].

Assim:

No uso da autorização legislativa concedida pelo artigo […] da Lei n.º […], de […], e nos termos das alíneas *a*) e *b*) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

Artigo 1º.

Objeto

1 - O presente decreto-lei aprova o regime jurídico da cibersegurança, transpondo, para a ordem jurídica interna, a Diretiva (UE) 2022/2555, do Parlamento Europeu e do

.....

Proposta de Lei n.º .....

Conselho, de 14 de dezembro, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 1).

2 - O presente decreto-lei procede ainda à:

a) Execução, na ordem jurídica interna, das obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança), implementando um quadro nacional de certificação da cibersegurança;

b) Nona alteração à Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua redação atual;

c) Segunda alteração à Lei do Cibercrime, aprovada pela Lei n.º 109/2009, 15 de setembro, alterada pela Lei n.º 79/2021, de 24 de novembro;

d) Segunda alteração à Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, alterada pelo Decreto-Lei n.º 114/2024, de 20 de dezembro.

3 - O disposto no presente decreto-lei não prejudica as medidas e o quadro legal vigente destinados a salvaguardar as funções essenciais do Estado, nomeadamente as medidas e disposições referentes à preservação da segurança e do interesse nacional, à produção de informações para a segurança interna e externa do Estado português, à proteção do segredo de Estado e da informação classificada, e ainda a salvaguardar a manutenção da ordem pública e a permitir a investigação, a deteção e a repressão de infrações criminais, sem prejuízo do previsto nos artigos 7.º e 8.º.

Artigo 2º.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Regime jurídico da cibersegurança

É aprovado, em anexo ao presente decreto-lei e do qual faz parte integrante, o regime jurídico da cibersegurança.

Artigo 3º.

Alteração à Lei n.º 53/2008, de 29 de agosto

O artigo 16.º da Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua redação atual, passa ter a seguinte redação:

«Artigo 16.º

[...]

1 - [...].

2 - [...].

3 - [...].

4 - Ao Secretário-Geral do Sistema de Segurança Interna compete convocar, nos termos do artigo 25.º-A, um gabinete de crise na sequência da atribuição de um grau de ameaça elevado pelo Serviço de Informações de Segurança , ou equivalente nível de alerta nacional para Cibersegurança, ou quando for informado pelo Centro Nacional de Cibersegurança ou por qualquer entidade competente, designadamente forças e serviços de segurança, sobre a ocorrência de uma ciberameaça significativa ou de crise ou incidente suscetível de ser considerado em grande escala.»

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Artigo 4º.

Alteração à Lei n.º 109/2009, de 15 de setembro

O artigo 2.º da Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, na sua redação atual, passa a ter a seguinte redação:

«Artigo 2.º

[...]

[…]:

a) [...];

b) [...];

c) [...];

d) [...];

e) [...];

f) [...];

g) [...];

h) «Vulnerabilidade», uma fragilidade, suscetibilidade ou falha, que afeta redes e sistemas de informação, produtos ou serviços de tecnologias da informação ou comunicação, passível de ser explorada por uma ciberameaça, definida na aceção do artigo 2.º, ponto n.º 8, do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho de 17 de abril.»

Artigo 5º.

Alteração à Lei n.º 16/2022, de 16 de agosto

O artigo 13.º da Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na sua redação atual, passa a ter a seguinte redação:

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

«Artigo 13.º

[…]

1 - […].

2 - Não obstante o disposto no número anterior, o artigo 177.º, a alínea *q*) do n.º 3 do artigo 178.º, o artigo 179.º, o artigo 180.º, o artigo 181.º, o artigo 182.º e o artigo 183.º da Lei das Comunicações Eletrónicas, aprovada em anexo à presente lei, entram em vigor no dia seguinte ao da sua publicação.»

Artigo 6º.

Aditamento à Lei n.º 53/2008, de 29 de agosto

É aditado o artigo 25.º-A à Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, na sua redação atual, com a seguinte redação:

«Artigo 25.º-A

Gabinete de crise

1 - O gabinete de crise referido no n.º 4 do artigo 16.º é composto por representantes da Polícia Judiciária, do Serviço de Informações de Segurança, do Serviço de Informações Estratégicas de Defesa, do Centro Nacional de Cibersegurança e do Comando de Operações de Ciberdefesa, ou de outras entidades com relevância em razão da matéria.

2 - O gabinete de crise referido no número anterior visa assegurar, de forma coordenada e sem prejuízo das competências legalmente atribuídas a cada entidade, a condução de crises de cibersegurança com impacto na segurança interna e, em situações de ocorrências com impacto transnacional, garantir a interoperabilidade funcional com entidades congéneres da União Europeia.»

Artigo 7º.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Aditamento à Lei n.º 109/2009, de 15 de setembro

É aditado o artigo 8.º-A à Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, na sua redação atual, com a seguinte redação:

«Artigo 8.º-A

Atos não puníveis por interesse público de cibersegurança

1 - Não são puníveis factos suscetíveis de consubstanciar os crimes de acesso ilegítimo e de interceção ilegítima previstos, respetivamente, nos artigos 6.º e 7.º, se verificadas, cumulativamente, as seguintes circunstâncias:

a) O agente atue com a intenção única de identificar a existência de vulnerabilidades em sistema de informação, produtos e serviços de tecnologias de informação e comunicação, que não tenham sido criadas por si ou por terceiro de quem dependa, e com propósito de, através da sua divulgação, contribuir para a segurança do ciberespaço;

b) O agente não atue com o propósito de obter vantagem económica ou promessa de vantagem económica decorrente da sua ação, sem prejuízo da remuneração que aquele obtenha como contrapartida da sua atividade profissional;

c) O agente comunique, imediatamente após a sua ação, as eventuais vulnerabilidades identificadas, ao proprietário ou pessoa por ele designada para gerir o sistema de informação, produto ou serviço de tecnologias de informação e comunicação, ao titular de quaisquer dados obtidos e que se encontrem protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais, designadamente, o Regulamento Geral de Proteção de Dados (RGPD), aprovado pelo Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, a Lei n.º 26/2016, de 22 de agosto,

Proposta de Lei n.º .....

na sua redação atual, a Lei n.º 58/2019, de 8 de agosto e a Lei n.º 59/2019, de 8 de agosto;

d) A atuação do agente seja proporcional aos seus propósitos e estritamente limitada pelos mesmos, bastando-se com as ações necessárias à identificação das vulnerabilidades e não provocando:

i) Uma perturbação ou interrupção do funcionamento do sistema ou serviço em causa;

ii) A eliminação ou deterioração de dados informáticos ou a sua cópia não autorizada;

iii) Qualquer efeito prejudicial, danoso ou nocivo sobre a pessoa ou entidade afetada, direta ou indiretamente, ou sobre quaisquer terceiros, excluindo os efeitos correspondentes ao próprio acesso ilegítimo ou interceção ilegítima, nos termos previstos nos artigos 6.º e 7.º, e ainda os que resultariam já, com elevada probabilidade, da própria vulnerabilidade detetada ou da sua exploração.

e) A atuação do agente não consubstancie a violação de dados pessoais protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais, designadamente, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, da Lei n.º 58/2019, de 8 de agosto e da Lei n.º 59/2019, de 8 de agosto.

2 - A comunicação prevista na alínea c) do número anterior, deve ser feita também à autoridade nacional de cibersegurança, que a remete à Polícia Judiciária sempre que revista relevância criminal.

3 - Para efeitos de determinação da proporcionalidade da atuação do agente, tomar-se-á em conta se a mesma era necessária à deteção da vulnerabilidade

Proposta de Lei n.º .....

e se a extensão dos sistemas ou dados informáticos acedidos, consultados e/ou copiados era imposta pelo interesse em contribuir para a segurança do ciberespaço, sendo expressamente vedado o uso das seguintes práticas:

a) Mecanismos de negação de serviço (DoS) ou negação de serviço distribuída (DDoS);

b) Engenharia social, definido como facto de enganar de responsáveis ou utilizadores dos sistemas de informação com vista à disponibilização de informação sensível ou sigilosa;

c) "Phishing" e variantes;

d) Roubo ou furto de palavras-passe ou outras informações sensíveis;

e) Eliminação ou alteração dolosa de dados informáticos;

f) Inflição dolosa de danos a sistema de informação;

g) Instalação e distribuição de software malicioso.

4 - Sem prejuízo das regras aplicáveis em matéria de proteção de dados, os dados informáticos que sejam comunicados ao proprietário ou pessoa encarregue da gestão do sistema de informação, produto e serviço de tecnologias de informação e comunicação, ou à autoridade nacional de cibersegurança devem ser eliminados no prazo de 10 dias contados a partir do momento em que a vulnerabilidade for corrigida, devendo garantir-se a sua natureza secreta durante todo o procedimento.

5 - Não são igualmente puníveis os factos praticados com consentimento do proprietário ou administrador de sistema de informação, produto ou serviço de tecnologias de informação e comunicação, sem prejuízo do dever de notificação das vulnerabilidades eventualmente identificadas à autoridade nacional coordenadora encarregada da resposta a incidentes de cibersegurança das vulnerabilidades eventualmente identificadas, nos termos previstos no regime jurídico da cibersegurança.»

.....

Proposta de Lei n.º .....

Artigo 8º.

Norma revogatória

São revogados:

a) O artigo 2.º-A do Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual, que aprova a orgânica do Gabinete Nacional de Segurança.

b) O regime jurídico da segurança do ciberespaço, aprovado pela Lei n.º 46/2018, de 13 de agosto;

c) A regulamentação do regime jurídico da segurança do ciberespaço, aprovada pelo Decreto-Lei n.º 65/2021, de 30 de julho;

d) Os artigos 59.º a 65.º e as alíneas *m*) a *t)* do n.º 3 do artigo 178.º da Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na sua redação atual.

Artigo 9º.

Norma transitória

1 - A entrada em vigor do presente decreto-lei não prejudica a validade das decisões tomadas pela Comissão de Avaliação de Segurança ao abrigo do regime anterior, que continuam a produzir efeitos pelo período de 180 dias após a data da entrada em vigor do presente decreto-lei, durante o qual deve ser realizada nova avaliação de segurança.

2 - Com base na nova avaliação de segurança referida no número anterior, e ao abrigo do regime aprovado em anexo ao presente decreto-lei, o membro do Governo responsável pela área da cibersegurança pode decidir pela renovação, modificação ou substituição das decisões adotadas pela Comissão de Avaliação de Segurança

.....

Proposta de Lei n.º .....

no âmbito do regime anterior.

Artigo 10º.

Produção de efeitos

O disposto nos n.ºs 1 e 2 do artigo 27.º, nos artigos 28.º a 30.º, 33.º e nas alíneas *b)*, *c)* e *f)* do n.º 1 do artigo 61.º do regime jurídico da cibersegurança, aprovado em anexo ao presente decreto-lei, produz efeitos 24 meses após a publicação da regulamentação referida nos artigos 8.º, 14.º, 26.º, 31.º, 32.º e 83.º do referido regime.

Artigo 11º.

Entrada em vigor

O presente decreto-lei entra em vigor 120 dias após a sua publicação.

Visto e aprovado em Conselho de Ministros de

O Primeiro-Ministro

O Ministro da Presidência

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

ANEXO

(a que se refere o artigo 2.º)

Regime jurídico da cibersegurança

Capítulo I

Disposições gerais

Artigo 1.º

Objeto

1 - O presente decreto-lei estabelece o regime jurídico da cibersegurança, transpondo, para a ordem jurídica interna, a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 1).

2 - O disposto no presente decreto-lei não prejudica o cumprimento do disposto na legislação aplicável em matéria de:

a) Processos de investigação criminal pelas autoridades judiciais e pelos órgãos de polícia criminal competentes, nomeadamente pelo Ministério Público e pela Polícia Judiciária;

b) Processos das respetivas competências exclusivas do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa em matéria de produção de informações referentes à salvaguarda da independência nacional, dos interesses nacionais, da segurança externa e interna do Estado Português, e da prevenção da sabotagem, do terrorismo, da espionagem e da prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido;

Proposta de Lei n.º .....

c) Proteção de dados pessoais, designadamente no âmbito do RGPD, da Lei n.º 26/2016, de 22 de agosto, na sua redação atual, da Lei n.º 58/2019, de 8 de agosto, e da Lei n.º 59/2019, de 8 de agosto;

d) Tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrónicas, designadamente no âmbito do disposto na Lei n.º 41/2004, de 18 de agosto na sua redação atual.

e) Identificação e designação de infraestruturas críticas nacionais e europeias, designadamente no âmbito do Decreto-Lei n.º 20/2022, de 28 de janeiro;

f) Luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, designadamente no âmbito da Lei n.º 103/2015, de 24 de agosto;

g) Proteção do utente de serviços públicos essenciais, designadamente no âmbito da Lei n.º 23/96, de 26 de julho, na sua redação atual;

h) Segurança e emergência no setor das comunicações eletrónicas, designadamente no âmbito do disposto na Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na sua redação atual;

i) Segredo de Estado e Informação Classificada, designadamente no âmbito do disposto na Lei Orgânica n.º 2/2014, de 6 de agosto, alterada pela Lei n.º 1/2015, de 8 de janeiro.

Artigo 2.º

Definições

Para efeitos do presente decreto-lei, entende-se por:

a) «Ativo», todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.

b) «Autoridade de cibersegurança competente», o Centro Nacional de

Proposta de Lei n.º .....

Cibersegurança (CNCS), ou, quando aplicável, a autoridade nacional setorial de cibersegurança competente nos termos da alínea a) do n.º 2 do artigo 15., sem prejuízo das reservas de competência exclusiva de entidades públicas com responsabilidades em matéria de investigação criminal, de produção de informações e de ciberdefesa;

c) «Ciberameaça», uma ciberameaça nos termos do ponto 8 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril;

d) «Ciberameaça significativa», uma ciberameaça que, com base nas suas características técnicas, possa ser considerada suscetível de ter um impacto grave nas redes e sistemas de informação de uma entidade ou dos utilizadores dos serviços das entidades, causando danos materiais ou imateriais consideráveis;

e) «Cibersegurança», cibersegurança nos termos do ponto 1 do artigo 2.º Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril;

f) «Entidade», uma pessoa coletiva criada e reconhecida como tal pelo direito nacional do seu local de estabelecimento, que, atuando em seu próprio nome, pode exercer direitos e estar sujeita a obrigações;

g) "Entidades competentes no âmbito da segurança do ciberespaço», o Comando de Ciberdefesa do Estado Maior General das Forças Armadas, a Polícia Judiciária, o Serviço de Informações de Segurança e o Serviço de Informações Estratégicas de Defesa;

h) «Entidade que presta serviços de registo de nomes de domínio», um agente de registo ou um agente que atua em nome de agentes de registo, tal como um prestador ou revendedor de serviços de proteção da privacidade ou de registo de servidores intermediários;

i) «Especificação técnica», uma especificação técnica nos termos do ponto 4 do artigo 2.º do Regulamento (UE) n.º 1025/2012, do Parlamento Europeu e do

Proposta de Lei n.º .....

Conselho, de 25 de outubro;

j) «Incidente», um evento que ponha em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou dos serviços oferecidos por redes e sistemas de informação ou acessíveis por intermédio destas;

k) «Crise ou incidente de cibersegurança em grande escala», um incidente que cause um nível de perturbação superior à capacidade de resposta do Estado Português, que tenha um impacto significativo em, pelo menos, dois Estados-Membros da União Europeia, ou que, pelo seu alcance e impacto sistémico, reclame coordenação intersectorial urgente;

l) «Incidente significativo», um incidente que:

i) Cause, ou seja suscetível de causar, graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa;

ii) Afete, ou seja suscetível de afetar, outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis.

m) «Matriz de risco», o quadro referencial que estabelece os valores de risco para o conjunto de cenários de risco que recai sobre um setor e subsetor de atividade, considerando os ativos comuns, as principais ameaças e vulnerabilidades;

n) «Medidas de gestão dos riscos de cibersegurança ou medidas de cibersegurança», medidas de âmbito técnico, operacional e organizacional, visando gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações ou na prestação dos seus serviços, bem como impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços;

o) «Mercado em linha», um mercado em linha nos termos da alínea n) do artigo 3.º do Decreto-Lei n.º 57/2008, de 26 de março, na redação atual, que estabelece o

regime aplicável às práticas comerciais desleais;

p) «Motor de pesquisa em linha», um motor de pesquisa em linha nos termos conjugados do disposto no ponto 5) do artigo 2.º do Regulamento (UE) 2019/1150, do Parlamento Europeu e do Conselho, de 20 de junho, e da alínea j) do artigo 3.º do Regulamento (UE) 2022/2065, do Parlamento e do Conselho, de 19 de outubro;

q) «Norma», uma norma nos termos do ponto 1 do artigo 2.º do Regulamento (UE) n.º 1025/2012, do Parlamento Europeu e do Conselho, de 25 de outubro;

r) «Operações de cibersegurança», ações de operacionalização das medidas de gestão dos riscos de cibersegurança;

s) «Organismo de investigação», uma entidade cujo objetivo principal é realizar investigação aplicada ou desenvolvimento experimental com vista à exploração dos resultados dessa investigação para fins comerciais, excluindo os estabelecimentos de ensino;

t) «Plataforma de serviços de redes sociais», uma plataforma em linha, definida de acordo com a alínea i) do artigo 3.º do Regulamento (UE) 2022/2065, do Parlamento Europeu e do Conselho, de 19 de outubro, que permite que utilizadores finais se conectem, partilhem, descubram e comuniquem entre si em vários dispositivos, especialmente por intermédio de conversas, publicações, vídeos e recomendações;

u) «Ponto de troca de tráfego», uma estrutura de rede que:

i) Permita a interligação de mais de duas redes independentes (sistemas autónomos), sobretudo a fim de facilitar a troca de tráfego na *Internet*;

ii) Só interligue sistemas autónomos;

iii) Não implique que o tráfego na *Internet* entre um par de sistemas autónomos

participantes passe através de um terceiro sistema autónomo, não altere esse tráfego nem interfira nele de qualquer outra forma.

v) «Prestador de serviços de DNS», uma entidade que presta serviços de resolução recursiva de nomes de domínio acessíveis ao público para os utilizadores finais de *Internet* ou serviços de resolução com autoridade para nomes de domínio para utilização por terceiros, com exceção dos servidores de nomes raiz;

w) «Prestador de serviços de confiança», um prestador de serviços de confiança nos termos do ponto 19 do artigo 3.º do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, conforme alterado pela Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, e pelo Regulamento (UE) n.º 2024/1183, do Parlamento Europeu e do Conselho, de 11 de abril;

x) «Prestador de serviços de segurança geridos», um prestador de serviços geridos que realize ou preste assistência a atividades relacionadas com a gestão dos riscos de cibersegurança;

y) «Prestador de serviços geridos», uma entidade que preste serviços relacionados com a instalação, gestão, operação ou manutenção de produtos de TIC, redes, infraestruturas, aplicações ou quaisquer outras redes e sistemas de informação, através de assistência ou administração ativa efetuadas nas instalações dos clientes ou à distância;

z) «Prestador qualificado de serviços de confiança», um prestador qualificado de serviços de confiança nos termos do ponto 20 do artigo 3.º Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, conforme alterado pela Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, e pelo Regulamento (UE) n.º 2024/1183, do Parlamento Europeu e do Conselho, de 11 de abril;

Proposta de Lei n.º .....

aa) «Processo de TIC», um processo de TIC nos termos do ponto 14 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril;

bb) «Produto de TIC», um produto de TIC nos termos do ponto 12 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril;

cc) «Quase incidente», um evento que poderia ter posto em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade de dados armazenados, transmitidos ou tratados ou de serviços oferecidos por redes e sistemas de informação ou acessíveis por intermédio destas, que, no entanto, foi possível evitar ou não se materializou;

dd) «Rede de distribuição de conteúdos», uma rede de servidores distribuídos geograficamente para o efeito de assegurar uma elevada disponibilidade, acessibilidade ou rápida distribuição de serviços e conteúdos digitais a utilizadores da *Internet* por conta de fornecedores de conteúdos e serviços;

ee) «Registo de nomes de domínio de topo» ou «Registo de nomes de TLD (*top level domain*, na expressão e sigla de língua inglesa)», uma entidade a quem foi delegado um TLD específico e que é responsável pela sua administração, incluindo o registo de nomes de domínio sob o TLD e a operação técnica desse TLD, incluindo a operação dos seus servidores de nomes, a manutenção das suas bases de dados e a distribuição de ficheiros da zona de TLD pelos servidores de nomes, independentemente de qualquer uma destas operações ser executada pela própria entidade ou ser externalizada, mas excluindo situações em que os nomes do TLD sejam utilizados por um registo apenas para uso próprio;

ff) «Rede pública de comunicações eletrónicas», uma rede pública de comunicações eletrónicas nos termos da alínea oo) do n.º 1 do artigo 3.º da Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na

sua redação atual;

gg) «Redes e sistemas de informação»:

i) Uma rede de comunicações eletrónicas, nos termos da alínea mm) do n.º 1 do artigo 3.º da Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na sua redação atual;

ii) Um dispositivo ou um grupo de dispositivos interligados ou associados, dos quais um ou vários efetuam o tratamento automático de dados digitais com base num programa; ou

iii) Os dados digitais armazenados, tratados, obtidos ou transmitidos por elementos indicados nas alíneas i) e ii), tendo em vista a sua exploração, utilização, proteção e manutenção;

hh) «Representante», qualquer pessoa singular ou coletiva, estabelecida na União Europeia, expressamente designada para atuar por conta de um prestador de serviços de DNS, um Registo de nomes de domínio de topo, uma entidade que presta serviços de registo de nomes de domínio, um prestador de serviços de computação em nuvem, um prestador de serviços de centro de dados, um fornecedor de redes de distribuição de conteúdos, um prestador de serviços geridos, um prestador de serviços de segurança geridos, um prestador de serviços de mercados em linha, de motores de pesquisa em linha ou de plataformas de serviços de redes sociais que não se encontre estabelecido na União Europeia, que possa ser contactada pelas entidades competentes, em vez da entidade representada, quanto às obrigações que incumbem a esta última por força do presente decreto-lei;

ii) «Risco», a medida da possibilidade de uma perda ou perturbação causada por um incidente, resultante da combinação da magnitude de tal perda ou perturbação e da probabilidade de ocorrência do incidente;

.....

Proposta de Lei n.º .....

jj) «Risco residual», medida de risco existente após a adoção das medidas de cibersegurança mínimas;

kk) «Segurança das redes e sistemas de informação», a capacidade das redes e sistemas de informação para resistir, com um dado nível de confiança, a eventos suscetíveis de pôr em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos por essas redes e sistemas de informação, ou acessíveis por intermédio destes;

ll) «Serviço de centro de dados», um serviço que engloba estruturas ou grupos de estruturas dedicados ao alojamento, à interligação e à operação centralizadas de equipamento de redes e TI que preste serviços de armazenamento, tratamento e transmissão de dados, juntamente com todas as instalações e infraestruturas de distribuição de energia e controlo ambiental;

mm) «Serviço de computação em nuvem», um serviço digital que permite a administração a pedido e um amplo acesso remoto a um conjunto modulável e adaptável de recursos de computação partilháveis, inclusive quando esses recursos estão distribuídos por várias localizações;

nn) «Serviço de comunicações eletrónicas», um serviço de comunicações eletrónicas nos termos da alínea ss) do n.º 1 do artigo 3.º da Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, na sua redação atual;

oo) «Serviço de confiança», um serviço de confiança nos termos do ponto 16 do artigo 3.º Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, conforme alterado pela Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, e pelo Regulamento (UE) n.º 2024/1183, do Parlamento Europeu e do Conselho, de 11 de abril;

pp) «Serviço de confiança qualificado», um serviço de confiança qualificado nos

Proposta de Lei n.º .....

termos do ponto 17 do artigo 3.º do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, conforme alterado pela Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, e pelo Regulamento (UE) n.º 2024/1183, do Parlamento Europeu e do Conselho, de 11 de abril;

qq) «Serviço de TIC», um serviço de TIC nos termos do ponto 13 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril;

rr) «Sistema de nomes de domínio» ou «DNS», um sistema de nomes distribuídos hierarquicamente que possibilita a identificação de serviços e recursos na *Internet*, permitindo que os dispositivos dos utilizadores finais utilizem os serviços de encaminhamento e de conectividade da *Internet* para aceder a esses serviços e recursos;

ss) «Serviço digital», um serviço nos termos da alínea g) do artigo 3.º do Decreto-Lei n.º 30/2020, de 29 de junho, que estabelece as regras a que obedece o procedimento de informação no domínio das regras técnicas relativas a produtos e das regras relativas aos serviços da sociedade da informação;

tt) «Tratamento de incidentes», todas as ações e procedimentos que visam a prevenção, a deteção, a análise, a contenção ou a resposta a um incidente e a recuperação de um incidente;

uu) «Vulnerabilidade», uma fragilidade, suscetibilidade ou falha, que afeta redes e sistemas de informação, produtos ou serviços de tecnologias da informação ou comunicação (TIC), passível de ser explorada por uma ciberameaça.

Artigo 3.º

Âmbito de aplicação subjetivo

1 - O presente decreto-lei aplica-se às entidades privadas de um dos tipos que constam

Proposta de Lei n.º .....

nos anexos I ou II ao presente decreto-lei e do qual fazem parte integrante, que, respeitados os critérios de âmbito territorial fixados no artigo seguinte:

a) Sejam qualificadas como médias empresas nos termos do artigo 2.º do anexo III ao presente decreto-lei e do qual faz parte integrante, correspondentes ao previsto na Recomendação 2003/361/CE, da Comissão, de 6 de maio, ou que excedam os limiares relativos às médias empresas previstos no n.º 1 desse artigo; e

b) Prestem os seus serviços ou exerçam as suas atividades na União Europeia.

2 - O presente decreto-lei aplica-se igualmente às entidades de um dos tipos que constam nos anexos I ou II ao presente decreto-lei que, independentemente da sua natureza e dimensão e respeitados os critérios de âmbito territorial fixados no artigo seguinte, preencham pelo menos um dos seguintes requisitos:

a) A entidade em causa seja:

i) Fornecedor de redes públicas de comunicações eletrónicas ou prestador de serviços de comunicações eletrónicas acessíveis ao público;

ii) Prestador de serviços de confiança;

iii) Registo de nomes de domínio de topo, prestador de serviços de registo de nomes de domínio, e prestador de serviços de sistemas de nomes de domínio.

b) A entidade em causa seja o único prestador de um serviço que é essencial para a manutenção de atividades sociais ou económicas críticas, designadamente as atividades correspondentes aos setores, subsetores e tipos de entidades referidos nos anexos I e II ao presente decreto-lei;

c) Uma perturbação do serviço por si prestado possa afetar consideravelmente a segurança pública, a proteção pública ou a saúde pública;

d) Uma perturbação do serviço por si prestado possa gerar riscos sistémicos consideráveis, especialmente para os setores relativamente aos quais tal perturbação possa ter um impacto transfronteiriço;

e) A entidade seja crítica devido à sua importância específica, a nível nacional ou regional, para o setor ou tipo de serviço em causa, ou para outros setores interdependentes.

3 - O presente decreto-lei aplica-se à Administração Pública, abrangendo:

a) Os serviços da administração direta do Estado, central e periférica;

b) Os serviços da administração direta das Regiões Autónomas, central e periférica;

c) As entidades da administração indireta do Estado;

d) As entidades da administração indireta das Regiões Autónomas;

e) As entidades da administração autónoma;

f) Os organismos e as entidades administrativas independentes, com exceção do Banco de Portugal, da Comissão do Mercado dos Valores Mobiliários e da Autoridade de Supervisão de Seguros e Fundos de Pensões.

4 - O presente decreto-lei aplica-se às seguintes entidades:

a) Provedoria de Justiça;

b) Conselho Económico e Social;

c) Serviços técnicos e administrativos da Presidência da República, da Assembleia da República, dos Tribunais e das secretarias com competência para a tramitação de procedimentos, do Conselho Superior da Magistratura, do Conselho Superior dos Tribunais Administrativos e Fiscais e do Conselho Superior do Ministério Público, sem prejuízo do disposto no n.º 6.

5 - O presente decreto-lei aplica-se às entidades que, independentemente da sua dimensão,

Proposta de Lei n.º .....

sejam identificadas como entidades críticas nos termos do disposto da Diretiva (UE) 2022/2557, do Parlamento Europeu e o Conselho, de 14 de dezembro, relativa à resiliência das entidades críticas, sem prejuízo da alínea f) do n.º 3.

6 - O presente decreto-lei não é aplicável:

a) Ao Estado-Maior General das Forças Armadas e dos ramos das Forças Armadas, no que respeita às redes e sistemas de informação diretamente relacionados com o seu comando e controlo;

b) Às entidades públicas com responsabilidades de investigação criminal e aos órgãos de polícia criminal e de segurança pública, no que respeita às redes e sistemas de informação diretamente relacionados com o seu comando e controlo;

c) Às entidades públicas com responsabilidades exclusivas em matéria de produção de informações, nomeadamente ao Sistema de Informações da República Portuguesa, ao Serviço de Informações Estratégicas de Defesa e ao Serviço de Informações de Segurança, no que respeita às redes e sistemas de informação diretamente relacionados com o seu comando e controlo;

d) Às entidades públicas cuja atividade incida sobre redes e sistemas de informação diretamente relacionados com a produção e difusão de informação classificada, nomeadamente com as marcas nacionais, da Organização do Tratado do Atlântico Norte (OTAN), e da União Europeia, ou catalogada como segredo de Estado, no que respeita a essas redes e sistemas de informação;

e) Às demais entidades públicas que exercem a sua atividade nos domínios da segurança nacional, da segurança pública, da defesa, e dos serviços de informações, no que respeita às redes e sistemas de informação diretamente relacionados com as atividades de produção de informações e prevenção, investigação, deteção e repressão de infrações penais;

f) Às entidades privadas que prestem serviços exclusivamente a uma ou mais entidades previstas nas alíneas anteriores e no que respeita a estas atividades.

.....

Proposta de Lei n.º .....

7 - Às entidades referidas na alínea b) do n.º 2 do artigo 15.º aplica-se o presente decreto-lei apenas no que respeita ao exercício das suas competências na qualidade de autoridades nacionais especiais de cibersegurança.

8 - O presente decreto-lei não prejudica o disposto no Regulamento (UE) 2022/2554, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro.

Artigo 4.º

Delimitação territorial do âmbito de aplicação subjetivo

1 - O presente decreto-lei aplica-se às entidades referidas nos n.ºs 1 e 2 do artigo anterior que:

a) Tenham estabelecimento no território nacional;

b) Tratando-se de empresas que oferecem redes públicas de comunicações eletrónicas ou prestam serviços de comunicações eletrónicas acessíveis ao público, disponibilizem os mesmos no território nacional;

c) Tratando-se de prestadores de serviços de sistemas de nomes de domínio, registo de nomes de domínio de topo, entidades que prestam serviços de registo de nomes de domínio, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados, aos fornecedores de redes de distribuição de conteúdos, prestadores de serviços geridos, aos prestadores de serviços de segurança geridos, bem como prestadores de serviços de mercados em linha, de motores de pesquisa em linha ou de plataformas de serviços de redes sociais:

i) Tenham o seu estabelecimento principal no território nacional;

ii) Não tendo estabelecimento na União Europeia, o seu representante tenha

estabelecimento no território nacional.

2 - Para efeitos da subalínea i) da alínea c) do número anterior, considera-se que a entidade tem estabelecimento principal no território nacional quando:

a) As decisões relacionadas com as medidas de gestão dos riscos de cibersegurança são predominantemente tomadas em território nacional;

b) As operações de cibersegurança são levadas a cabo em território nacional, se não for possível determinar se as decisões relacionadas com as medidas de gestão de risco de cibersegurança foram nele tomadas de forma predominante ou em outro Estado-Membro da União Europeia;

c) O estabelecimento da entidade com maior número de trabalhadores se situa no território nacional, se não for possível determinar se as operações de cibersegurança são nele levadas a cabo.

3 - Nos termos do artigo 20.º, o CNCS, perante um pedido de assistência mútua proveniente de outro Estado-Membro da União Europeia e em relação a uma entidade a que se refere a alínea c) do n.º 1, pode, dentro dos limites desse pedido, tomar medidas de supervisão e execução adequadas em relação à entidade em causa.

Artigo 5.º

Âmbito extraterritorial

1 - A fim de evitar ciberameaças significativas para a segurança das redes e sistemas de informação de um grande número de utilizadores, o CNCS pode, ouvido o Conselho Superior de Segurança do Ciberespaço, adotar medidas de execução corretivas ou restritivas, incluindo a ordem de suspensão do serviço no território nacional, dirigidas a um prestador de serviços sem estabelecimento ou representação no território nacional que não ofereça as medidas adequadas de cibersegurança.

2 - Salvo quando as medidas forem urgentes, o CNCS apresenta uma fundamentação

preliminar das decisões ao prestador de serviços, concedendo um prazo de resposta não inferior a 10 dias.

3 - Para efeitos da determinação e fundamentação das medidas de execução previstas nos números anteriores, o CNCS terá em consideração as ações e medidas, bem como a sua eficácia e extensão, tomadas pelas autoridades de cibersegurança europeias e internacionais.

4 - A autoridade de cibersegurança competente, nos termos das suas competências e na medida do necessário, pode, relativamente a uma entidade com conexão relevante com o território nacional, prestar assistência às autoridades competentes dos Estados-Membros da União Europeia, a pedido fundamentado destas, designadamente mediante:

a) Prestação de informações relativamente a uma medida de supervisão ou execução tomada em relação a essa entidade, através do respetivo ponto de contacto único;

b) Aplicação de medidas de supervisão ou execução nos termos do disposto no Capítulo VI, se necessário conjuntamente com a autoridade competente do respetivo Estado-Membro da União Europeia;

c) Prestação de apoio à autoridade competente do respetivo Estado-Membro da União Europeia quanto à aplicação por esta de medidas de supervisão ou execução, podendo este apoio incluir as formas de assistência referidas nas alíneas anteriores.

5 - A autoridade de cibersegurança competente apenas pode recusar a assistência pedida nos termos no número anterior se esta exceder as suas competências, for desproporcional em relação às suas funções de supervisão ou comprometer interesses essenciais do Estado Português em matéria de segurança nacional, segurança pública ou defesa.

Proposta de Lei n.º .....

Artigo 6.º

Entidades essenciais e entidades importantes

1 - Para efeitos do presente decreto-lei, consideram-se entidades essenciais:

a) As entidades de um dos tipos referidos no anexo I ao presente decreto-lei que excedam os limiares para as médias empresas previstos no artigo 2.º do anexo III ao presente decreto-lei, correspondentes aos da Recomendação 2003/361/CE, da Comissão, de 6 de maio;

b) Os prestadores de serviços de confiança qualificados e registo de nomes de domínio de topo, e os prestadores de serviços de sistemas de nomes de domínio, independentemente da sua dimensão;

c) As empresas que oferecem redes públicas de comunicações eletrónicas ou serviços de comunicações eletrónicas acessíveis ao público que sejam consideradas médias empresas nos termos do artigo 2.º do anexo III ao presente decreto-lei, correspondentes aos da Recomendação 2003/361/CE da Comissão, de 6 de maio;

d) As entidades da Administração Pública que tenham como atribuições a prestação de serviços nas áreas do desenvolvimento, manutenção e gestão de infraestruturas de tecnologias de informação e comunicação ou aquelas que apresentem um grau particularmente elevado de integração digital na prestação dos seus serviços, identificadas e qualificadas nos termos do artigo 8.º;

e) As entidades identificadas como entidades críticas nos termos da Diretiva (UE) 2022/2557 do Parlamento Europeu e o Conselho, de 14 de dezembro, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho, independentemente da sua dimensão;

f) Qualquer outra entidade de um dos tipos constantes dos anexos I ou II ao presente decreto-lei, referida nas alíneas b) a e) do n.º 2 do artigo 3.º, que seja

qualificada como entidade essencial com base no respetivo grau de exposição da entidade aos riscos, na dimensão da entidade e na probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico.

2 - Para efeitos do presente decreto-lei, são entidades importantes as entidades dos tipos referidos nos anexos I e II ao presente decreto-lei que não sejam consideradas entidades essenciais ao abrigo do número anterior.

3 - Para efeitos do presente decreto-lei, são também entidades importantes as entidades de um dos tipos constantes nos anexos I ou II ao presente decreto-lei, referidas nas alíneas b) a e) do no n.º 2 do artigo 3.º, que justifiquem tal qualificação com base no respetivo grau de exposição da entidade aos riscos, na dimensão da entidade e na probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico.

4 - A atribuição das qualificações de entidades essenciais e entidades importantes previstas nos números anteriores resulta dos mecanismos previstos no artigo 8.º.

Artigo 7.º

Entidades públicas relevantes

1 - As entidades públicas que não sejam qualificadas como entidades essenciais ou importantes nos termos do artigo anterior, consideram-se entidades públicas relevantes, integrando-se em dois grupos para efeitos de aplicação de regimes específicos nos termos do presente decreto-lei e restante regulamentação emitida pelo CNCS.

2 - São consideradas entidades públicas relevantes do Grupo A:

a) Os serviços da administração direta do Estado, central e periférica, com 250 ou mais trabalhadores no seu quadro de pessoal;

.....

Proposta de Lei n.º .....

b) Os serviços da administração direta das Regiões Autónomas, central e periférica, com 250 ou mais trabalhadores no seu quadro de pessoal;

c) As entidades da administração indireta do Estado, com mais de 250 trabalhadores no seu quadro de pessoal;

d) As entidades da administração indireta das Regiões Autónomas, com mais de 250 trabalhadores no seu quadro de pessoal;

e) As entidades da administração autónoma, com mais de 250 trabalhadores no seu quadro de pessoal;

f) As entidades públicas empresariais que excedam os limiares previstos no artigo 2.º do anexo III ao presente decreto-lei, correspondentes aos da Recomendação 2003/361/CE, da Comissão, de 6 de maio;

g) As entidades administrativas independentes;

h) O Conselho Económico e Social, a Provedoria da Justiça, os serviços técnicos e administrativos da Presidência da República, da Assembleia da República, dos Tribunais e das secretarias com competência para a tramitação de procedimentos, do Conselho Superior da Magistratura, do Conselho Superior dos Tribunais Administrativos e Fiscais e do Conselho Superior do Ministério Público.

3 - São consideradas entidades públicas relevantes do Grupo B:

a) Os serviços da administração direta do Estado, central e periférica, que tenham entre 75 e 249 trabalhadores no seu quadro de pessoal;

b) Os serviços da administração direta das Regiões Autónomas, central e periférica, que tenham entre 75 e 249 trabalhadores no seu quadro de pessoal;

c) As entidades da administração indireta do Estado, que tenham entre 75 e 249 trabalhadores no seu quadro de pessoal;

d) As entidades da administração indireta das Regiões Autónomas, que tenham

Proposta de Lei n.º .....

entre 75 e 249 trabalhadores no seu quadro de pessoal;

e) As entidades da administração autónoma, que tenham entre 75 e 249 trabalhadores no seu quadro de pessoal;

f) As entidades públicas empresariais qualificadas como empresas médias nos termos do anexo III ao presente decreto-lei, correspondentes aos da Recomendação 2003/361/CE, da Comissão, de 6 de maio.

4 - A atribuição da qualificação de entidade pública relevante prevista nos números anteriores resulta dos mecanismos de qualificação previstos no artigo seguinte.

Artigo 8.º

Procedimento de qualificação das entidades

1 - As entidades previstas no artigo 3.º identificam-se em plataforma eletrónica disponibilizada pelo CNCS, no prazo de 30 dias após o início da sua atividade ou, caso a entidade já se encontre em atividade aquando da entrada em vigor do presente decreto-lei, no prazo de 60 dias após a disponibilização da referida plataforma eletrónica, sendo responsáveis por manter essa informação devidamente atualizada.

2 - A qualificação das entidades pelo CNCS com base nos critérios previstos nas alíneas a) a c) e e) do n.º 1, e do n.º 2, do artigo 6.º, e ainda no artigo 7.º, resulta do mecanismo previsto no número anterior.

3 - A qualificação das entidades pelo CNCS com base nos critérios previstos nas alíneas d) e f) do n.º 1, e do n.º 3, do artigo 6.º, é comunicada com a antecedência mínima de 60 dias ao membro do Governo responsável pela área da cibersegurança e revista pelo menos de dois em dois anos.

4 - A qualificação prevista no número anterior é devidamente fundamentada pelo CNCS, sendo precedida de audiência prévia da entidade em causa e, quando aplicável, de parecer das autoridades nacionais setoriais de cibersegurança referidas

Proposta de Lei n.º .....

na alínea a) do n.º 2 do artigo 15.º.

5 - O CNCS, ou, quando aplicável, as autoridades nacionais setoriais de cibersegurança competentes nos termos da alínea a) do n.º 2 do artigo 15.º, notifica a entidade da sua qualificação nos termos dos n.ºs 2 e 3, no prazo máximo de 30 dias a contar da data da referida qualificação.

6 - Os prestadores de serviços de registos de nomes de domínio devem identificar-se e comunicar a informação prevista no n.º 2 do artigo 35.º através da plataforma eletrónica disponibilizada pelo CNCS, no prazo de 30 dias após o início da sua atividade.

7 - As regras de funcionamento da plataforma eletrónica referida no presente artigo são definidas através de regulamento a aprovar pelo CNCS.

8 - O procedimento de qualificação referido no presente artigo não prejudica, para as entidades abrangidas, o cumprimento do dever previsto no artigo 35.º.

Artigo 9.º

Concurso de qualificações e medidas de cibersegurança

1 - Caso uma entidade se enquadre simultaneamente em mais do que uma qualificação, aplica-se o regime que resultar mais exigente para gerir os riscos que se colocam à segurança das redes e sistemas de informação, de acordo com a seguinte ordem:

a) Entidades essenciais;

b) Entidades importantes;

c) Entidades públicas relevantes do Grupo A;

d) Entidades públicas relevantes do Grupo B.

2 - O CNCS pode associar à qualificação da entidade, nos termos do disposto no n.º 4 do artigo 26.º e do artigo 33.º, medidas de cibersegurança e demais medidas técnicas

Proposta de Lei n.º .....

e organizativas resultantes dos instrumentos previstos do presente decreto-lei, cujo incumprimento pode determinar a aplicação das sanções correspondentes nos termos do regime sancionatório previsto no Capítulo VII do presente decreto-lei.

Artigo 10.º

Tratamento de dados pessoais

1 - As entidades que integram o quadro institucional da segurança do ciberespaço, nos termos do artigo 15.º, tratam dados pessoais na medida do estritamente necessário para assegurar o cumprimento de obrigações legais e a prossecução de missões de interesse público ou de autoridade pública em que estão investidos, nos termos do disposto nas alíneas c) ou e) do n.º 1 e no n.º 3 do artigo 6.º do RGPD e em conformidade com o presente decreto-lei e demais legislação nacional aplicável.

2 - As entidades que integram o quadro institucional da segurança do ciberespaço podem ainda tratar dados pessoais para a prossecução de um interesse legítimo das entidades essenciais e importantes, tal como referido na alínea f), n.º 1 do artigo 6.º do RGPD.

3 - Sem prejuízo do disposto no artigo 29.º da Lei n.º 58/2019, de 8 de agosto, as entidades que integram o quadro institucional da segurança do ciberespaço podem proceder ao tratamento de categorias especiais de dados pessoais para, na medida do estritamente necessário:

a) Evitar a consumação de uma ciberameaça significativa para a segurança das redes e sistemas de informação;

b) Responder eficazmente a um incidente de cibersegurança.

Capítulo II

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Instrumentos estruturantes

Artigo 11.º

Instrumentos estruturantes da Segurança do Ciberespaço

São instrumentos estruturantes da Segurança do Ciberespaço, observando as disposições legais e regulamentares nacionais e internacionais aplicáveis:

a) Estratégia Nacional de Segurança do Ciberespaço (ENSC);

b) Plano nacional de resposta a crises e incidentes de cibersegurança em grande escala;

c) Quadro Nacional de Referência para a Cibersegurança (QNRCS);

d) Estratégia Nacional de Ciberdefesa;

e) Conceito Estratégico de Defesa Nacional.

Artigo 12.º

Estratégia Nacional de Segurança do Ciberespaço

1 - A ENSC define o enquadramento, as prioridades, os objetivos estratégicos nacionais e um quadro de governação definidor das funções e responsabilidades das partes interessadas a nível nacional com relevância para a execução da ENSC.

2 - A ENCS inclui, designadamente:

a) Os objetivos e prioridades da ENCS, abrangendo, designadamente, os setores nos anexos I e II ao presente decreto-lei;

b) Um quadro de governação para cumprir os objetivos e prioridades referidos na alínea a) do presente número;

c) Um quadro de governação definidor das funções e responsabilidades das partes

Proposta de Lei n.º .....

interessadas a nível nacional com relevância para a execução da ENSC e que consolide a cooperação e coordenação institucional ao abrigo do presente decreto-lei;

d) Um mecanismo para identificar ativos pertinentes e uma avaliação dos riscos em Portugal;

e) A identificação das medidas de preparação, de resposta e de recuperação em caso de incidentes, incluindo a cooperação entre os setores público e privado;

f) Uma lista das diversas autoridades e partes interessadas envolvidas na execução da ENCS;

g) Um quadro político para o reforço da cooperação entre as autoridades competentes nos termos do presente decreto-lei e as autoridades competentes que resultem da transposição da Diretiva (UE) 2022/2557, do Parlamento Europeu e do Conselho, de 14 de dezembro, para efeitos de partilha de informações sobre riscos, ciberameaças e incidentes, bem como riscos, ameaças e incidentes não cibernéticos, e do exercício de funções de supervisão;

h) Um plano, incluindo as medidas necessárias, para reforçar o nível geral de educação, formação e sensibilização dos cidadãos para a cibersegurança e ciber-higiene;

i) Um plano, incluindo as medidas necessárias, adequado às necessidades específicas em matéria de cibersegurança das pequenas e médias empresas, qualificadas nos termos do artigo 2.º do anexo III ao presente decreto-lei, correspondentes aos da Recomendação 2003/361/CE, da Comissão, de 6 de maio;

j) A promoção do desenvolvimento, investigação e integração de tecnologias avançadas que visem a aplicação de medidas, boas práticas e controlos inovadores, incluindo o recurso a inteligência artificial, em matéria de gestão dos

{A139886346-9910-4EFC-B182-85FA24028071}

riscos de cibersegurança e da deteção e prevenção de ciberataques.

3 - A ENSC é aprovada por resolução do Conselho de Ministros, sob proposta do CNCS, ouvidos a Assembleia da República e o Conselho Superior de Segurança do Ciberespaço (CSSC), decorrido um período de consulta pública não inferior a 30 dias.

4 - A ENCS é revista e atualizada a cada 5 anos, após um processo de avaliação baseado em indicadores-chave de impacto e desempenho, podendo este período ser reduzido por decisão do membro do Governo responsável pela área da cibersegurança mediante proposta fundamentada do CNCS.

5 - A ENSC não prejudica a aprovação pelas entidades competentes, quando necessário, de instrumentos que estabeleçam estratégias setoriais de cibersegurança, que devem ser revistas e atualizadas nos mesmos termos aplicáveis à ENCS.

Artigo 13.º

Plano nacional de resposta a crises e incidentes de cibersegurança em grande escala

1 - O plano nacional de resposta a crises e incidentes de cibersegurança em grande escala estabelece os objetivos e modalidades de gestão deste tipo de crises e incidentes.

2 - O plano nacional de resposta a crises e incidentes de cibersegurança em grande escala é aprovado por resolução do Conselho de Ministros, por proposta conjunta do Secretário-Geral do Sistema de Segurança Interna, da Polícia Judiciária, do Serviço de Informações de Segurança, do Serviço de Informações Estratégicas de Defesa, do Comando de Operações de Ciberdefesa e do CNCS, cabendo a este último a sua implementação, acompanhamento e monitorização, em colaboração estreita com as entidades que compõe o gabinete de crise previsto no n.º 4 do artigo 16.º da Lei 53/2008, de 29 de agosto, na redação que lhe é atribuída pelo presente decreto-lei, e ouvido o CSSC.

3 - O plano nacional de resposta a crises e incidentes de cibersegurança em grande escala deve garantir a coerência com os quadros existentes de gestão geral de crises a nível nacional.

Artigo 14.º

Quadro Nacional de Referência para a Cibersegurança

1 - O QNRCS é o instrumento nacional de referência para a identificação das normas, padrões e boas práticas existentes em matéria de gestão da cibersegurança e da segurança da informação.

2 - O QNRCS é aprovado por regulamento do CNCS, ouvido o CSSC, devendo ser regularmente atualizado, pelo menos de cinco em cinco anos.

3 - As entidades essenciais e importantes devem ter em conta o QNRCS no âmbito da adoção de medidas de cibersegurança previstas nos artigos 27.º e seguintes.

4 - As autoridades nacionais setoriais de cibersegurança referidas na alínea a) do n.º 2 do artigo 15.º podem adotar normas complementares ao QNRCS, através de regulamento próprio, em articulação com o CNCS.

5 - Sem prejuízo dos números anteriores, a aplicação do QNRCS pelas entidades essenciais, importantes e públicas relevantes é objeto de regulamento a aprovar pelo CNCS, prevendo medidas de cibersegurança específicas e níveis de conformidade.

Capítulo III

Quadro institucional da segurança do ciberespaço

Artigo 15.º

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Organização

1 - O quadro institucional da segurança do ciberespaço é composto pelas seguintes entidades:

a) O CSSC, na qualidade de órgão consultivo do Primeiro-Ministro no domínio da cibersegurança;

b) O CNCS, na qualidade de:

i) Autoridade nacional de cibersegurança;

ii) Ponto de contacto único para efeitos de cooperação no âmbito da União Europeia e ao nível internacional, sem prejuízo das competências atribuídas a outras entidades em matéria de cooperação internacional;

iii) Autoridade nacional de certificação de cibersegurança;

iv) Entidade que integra a equipa de resposta a incidentes de cbersegurança nacional.

c) O Secretário-Geral do Sistema de Segurança Interna, na qualidade de autoridade nacional de gestão de crises e incidentes de cibersegurança em grande escala.

2 - Integram ainda o quadro institucional da segurança do ciberespaço:

a) Na qualidade de autoridades nacionais setoriais de cibersegurança:

i) O Gabinete Nacional de Segurança (GNS), no que respeita aos serviços de confiança nas transações eletrónicas no mercado interno;

ii) A Autoridade Nacional de Comunicações (ANACOM), no que respeita à matéria das comunicações eletrónicas e dos serviços postais.

b) Na qualidade de autoridades nacionais especiais de cibersegurança, no que respeita à matéria da resiliência operacional digital do setor financeiro:

Proposta de Lei n.º .....

i) A Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF);

ii) A Comissão do Mercado de Valores Mobiliários (CMVM);

iii) O Banco de Portugal.

c) A Comissão de Avaliação de Segurança do Ciberespaço;

d) A Polícia Judiciária;

e) O Serviço de Informações de Segurança;

f) O Serviço de Informações Estratégicas de Defesa;

g) O Comando de Operações de Ciberdefesa.

3 - A organização do quadro institucional da segurança do ciberespaço não prejudica a articulação informal das autoridades referidas no presente artigo, nomeadamente mediante a participação em instâncias multilaterais de coordenação no que respeita à defesa da segurança do ciberespaço, como o Gabinete de Oficiais de Ligação do Ciberespaço para a cooperação tático-operacional (G5).

Artigo 16.º

Conselho Superior de Segurança do Ciberespaço

1 - O CSSC é o órgão de coordenação estratégica que apoia o Primeiro-Ministro em matéria de segurança do ciberespaço.

2 - O CSSC é composto por:

a) O Primeiro-Ministro, que preside, ou o membro do Governo responsável pela área da cibersegurança com competência delegada;

b) Dois Deputados designados pela Assembleia da República através do método de Hondt;

c) O Secretário-Geral do Sistema de Segurança Interna;

Proposta de Lei n.º .....

d) O Secretário-Geral do Sistema de Informações da República Portuguesa;

e) O Diretor do Serviço de Informações de Segurança;

f) O Diretor do Serviço de Informações Estratégicas de Defesa;

g) O Diretor-geral do Gabinete Nacional de Segurança;

h) O Coordenador do CNCS;

i) O Embaixador para a ciberdiplomacia;

j) O Chefe do Centro de Comunicações e Informação, Ciberespaço e Espaço do Estado-Maior-General das Forças Armada;

k) O Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária;

l) Um representante do Ministério Público, designado pelo Procurador-Geral da República;

m) O Presidente do Conselho Nacional de Planeamento Civil de Emergência;

n) Um representante da Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática;

o) O dirigente máximo das autoridades nacionais setoriais e especiais de cibersegurança, referidas no n.º 2 do artigo 15.º, não constantes nas alíneas anteriores.

3 - O CSSC é ainda composto por um representante do Governo Regional dos Açores e um representante do Governo Regional da Madeira.

4 - O presidente, por sua iniciativa ou a pedido de qualquer dos membros do CSSC, pode convocar outros titulares de órgãos públicos ou convidar outras entidades e personalidades de reconhecido mérito para participar em reuniões.

5 - O presidente é substituído nas suas ausências e impedimentos pelo membro do

Proposta de Lei n.º .....

Governo que designar.

Artigo 17.º

Competências do Conselho Superior de Segurança do Ciberespaço

1 - São competências do CSSC:

a) Assegurar a coordenação estratégica para a segurança do ciberespaço;

b) Emitir parecer prévio sobre a ENSC, bem como acompanhar a sua execução e elaborar anualmente, ou sempre que necessário, relatório de avaliação da mesma;

c) Emitir parecer prévio sobre o plano nacional de resposta a crises e incidentes de cibersegurança em grande escala;

d) Emitir parecer sobre matérias relativas à segurança do ciberespaço, a pedido do Primeiro-Ministro, ou do membro do Governo em quem este delegar, no âmbito das suas competências;

e) Responder a solicitações do Primeiro-Ministro, ou do membro do Governo em quem este delegar, no âmbito das suas competências;

f) Propor ao membro do Governo responsável pela área de cibersegurança a realização de avaliações de segurança, nos termos do disposto no artigo seguinte.

2 - O relatório anual de avaliação da execução da Estratégia Nacional da Segurança do Ciberespaço é enviado à Assembleia da República até 30 de junho do ano posterior àquele a que se reporta.

3 - Os Serviços de Informações instruem o Conselho Superior de Segurança do Ciberespaço a respeito da avaliação da ameaça vigente para o ciberespaço nacional e para o ciberespaço internacional, sempre que for conveniente ou revisto o grau de ameaça atribuído pelo Serviço de Informações de Segurança.

Artigo 18.º

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Comissão de Avaliação de Segurança do Ciberespaço

1 - A Comissão de Avaliação de Segurança do Ciberespaço funciona junto do CSSC e é responsável pela realização de avaliações de segurança de equipamentos, componentes ou serviços de tecnologias de informação e comunicação, utilizados em redes e sistemas de informação públicos ou privados, de fabricantes ou fornecedores que possam ser considerados de elevado risco para a segurança do ciberespaço de interesse nacional, designadamente nos contextos da segurança interna e externa, da defesa nacional, da integridade do processo democrático e de outras funções de soberania, e ainda da operação de infraestruturas críticas e da prestação de serviços essenciais.

2 - A Comissão de Avaliação de Segurança do Ciberespaço tem a seguinte composição:

a) O Diretor-geral do Gabinete Nacional de Segurança, que preside;

b) O coordenador do CNCS;

c) Um representante da ANACOM;

d) Um representante do Sistema de Segurança Interna;

e) Um representante do Sistema de Informações da República Portuguesa;

f) O Embaixador para a ciberdiplomacia;

g) Um representante da Polícia Judiciária;

h) Um representante do Serviço de Informações de Segurança;

i) Um representante do Serviço de Informações Estratégicas de Defesa;

j) Um representante do Comando de Operações de Ciberdefesa;

k) Um representante da Direção-Geral de Política Externa;

l) Um representante da Direção-Geral da Política de Defesa;

m) Um representante da Autoridade da Concorrência.

Proposta de Lei n.º .....

3 - O membro do Governo responsável pela área da cibersegurança pode determinar a aplicação de restrições provisórias à utilização, a cessação de utilização ou exclusão de equipamentos, componentes ou serviços de tecnologias de informação e comunicação, utilizados em redes e sistemas de informação públicos ou privados, considerados de elevado risco para a segurança do ciberespaço de interesse nacional, mediante proposta da Comissão de Avaliação de Segurança do Ciberespaço, fundamentada em avaliação de segurança realizada nos termos do disposto nos números seguintes.

4 - A avaliação de segurança deve ser devidamente fundamentada, tendo em conta os riscos técnicos dos equipamentos, componentes ou serviços, o seu contexto de utilização e a exposição dos seus fabricantes ou fornecedores à influência indevida de países estrangeiros, para tal considerando, designadamente, informação relevante emitida pelas entidades competentes nacionais e da União Europeia ou constante das avaliações nacionais ou europeias de risco para a segurança das redes e sistemas de informação, bem como outros riscos securitários relevantes.

5 - Para avaliar o nível de exposição dos fabricantes ou fornecedores à influência indevida de um país estrangeiro, podem ser considerados os seguintes elementos:

a) O fabricante ou fornecedor estar sujeito, direta ou indiretamente, à interferência do governo ou administração de um país estrangeiro;

b) O fabricante ou fornecedor estar domiciliado em, ou de qualquer forma relevantemente vinculado a países reconhecidos por Portugal, pela União Europeia, pela Organização para a Cooperação e Desenvolvimento Económico (OCDE) ou pela OTAN, como responsáveis ou envolvidos em ações hostis à segurança interna e defesa nacional de Portugal ou dos seus aliados, designadamente atos de espionagem ou de sabotagem;

c) O fabricante ou fornecedor estar domiciliado em, ou de qualquer forma relevantemente vinculado a países que não dispõem de legislação ou

Proposta de Lei n.º .....

acordos diplomáticos com Portugal ou com a União Europeia em matéria de proteção de dados, de cibersegurança e de proteção de propriedade intelectual.

d) O fabricante ou fornecedor estar associado a práticas de introdução de vulnerabilidades ou acessos ocultos;

e) O fabricante ou fornecedor adotar modelos de governação corporativa que não esclareçam sobre o grau de influência ou vinculação a países estrangeiros nas condições das alíneas anteriores;

f) As cadeias de produção e fornecimento do fabricante ou fornecedor evidenciarem falhas sistémicas de controlo e segurança.

6 - As avaliações de segurança podem ser realizadas ou revistas a pedido do membro do Governo responsável pela área da cibersegurança, bem como, em aplicação do mecanismo português de salvaguarda de ativos estratégicos essenciais, a pedido do membro do Governo responsável pela área em que o ativo estratégico em causa esteja integrado.

7 - A proposta da Comissão de Avaliação de Segurança do Ciberespaço realizada na sequência da avaliação de segurança deve, no seu teor, abrangência e intensidade, respeitar o princípio da proporcionalidade, considerando, designadamente, o grau de risco apurado, o grau de incidência, global e específica, sobre cada equipamento, componente ou serviço em causa, o prejuízo sofrido pelo fabricante e fornecedor afetado, e ainda os prejuízos económicos e sociais potencialmente decorrentes da decisão.

8 - A Comissão de Avaliação de Segurança do Ciberespaço pode solicitar a qualquer entidade, pública ou privada, a prestação de qualquer informação necessária à elaboração de avaliações de segurança.

9 - A decisão do membro do Governo responsável pela área da cibersegurança prevista no n.º 3 define os prazos razoáveis e, quando aplicável, o âmbito geográfico da

medida a aplicar, de forma que as entidades públicas ou privadas em causa procedam à sua implementação.

10 - Os documentos ou informações produzidas no âmbito dos trabalhos da Comissão de Avaliação de Segurança do Ciberespaço são considerados como informação classificada no grau de segurança reservado, salvo se o presidente da Comissão considerar necessário atribuir um grau de classificação de segurança superior, e sem prejuízo destes documentos ou informações poderem ser classificadas como segredo de Estado nos termos da Lei Orgânica n.º 2/2014, de 6 de agosto, na sua redação atual.

11 - No exercício das suas competências, o CNCS ou, quando aplicável, a autoridade nacional setorial ou nacional especial, procede à fiscalização do cumprimento das solicitações da Comissão de Avaliação de Segurança do Ciberespaço e da decisão do membro do Governo responsável pela área da cibersegurança previstas no presente artigo, sancionando o seu incumprimento nos termos da alínea d) do n.º 1 do artigo 63.º e da alínea a) do n.º 1 do artigo 61.º, respetivamente.

12 - O apoio técnico, administrativo e logístico da Comissão de Avaliação de Segurança do Ciberespaço, assim como os respetivos encargos associados, são prestados e suportados pelo GNS.

Artigo 19.º

Centro Nacional de Cibersegurança

1 - O CNCS é a autoridade nacional de cibersegurança, tendo por missão garantir que o país alcança e mantém um nível elevado de cibersegurança, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento das entidades

essenciais, entidades importantes e entidades públicas relevantes.

2 - O CNCS é ainda o ponto de contacto único para efeitos de cooperação ao nível da União Europeia, bem como ao nível internacional em matéria de cibersegurança, sem prejuízo das competências atribuídas a outras autoridades em matéria de cooperação em matéria penal, designadamente as competências da Polícia Judiciária para a cooperação internacional que lhe são conferidas pelo disposto nos artigos 20º a 26º e artigo 29º da Lei do Cibercrime, e em matéria de produção de informações referentes a segurança interna e externa do Estado Português e dos seus aliados.

3 - O CNCS integra o «CERT.PT», previsto no artigo 22.º, que atua como equipa de resposta a incidentes de cibersegurança nacional.

4 - O CNCS é igualmente a autoridade nacional de certificação de cibersegurança, nomeadamente para efeitos do disposto no artigo 58.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril, sem prejuízo das competências do GNS no que diz respeito à certificação e acreditação dos sistemas de informação e comunicação que tratam informação classificada, nos termos do Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual.

Artigo 20.º

Competências do CNCS

1 - O CNCS, no âmbito das responsabilidades atribuídas nos n.ºs 1 e 2 do artigo 19.º, prossegue as atribuições e exerce as competências descritas nas alíneas seguintes:

a) Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança, a ciberataques, e a ciberameaças;

Proposta de Lei n.º .....

b) Cooperar com as entidades competentes no âmbito da segurança do ciberespaço no âmbito das respetivas atribuições;

c) Comunicar, no prazo de 24 horas, à Polícia Judiciária todos os factos com relevância criminal de que tenha conhecimento no decurso da sua atividade;

d) Comunicar, no prazo de 24 horas, ao Serviço de Informações de Segurança todos os factos referentes a ameaças à segurança interna, à ciberespionagem e à cibersabotagem, de que tenha conhecimento no decurso da sua atividade;

e) Adotar regulamentos e emitir as orientações, recomendações e instruções técnicas relativas à cibersegurança;

f) Propor ao membro do Governo responsável pela área da cibersegurança a definição do nível nacional de alerta de cibersegurança, desenvolvido através de regulamento próprio do CNCS e difundido em coordenação com as entidades competentes no âmbito da segurança do ciberespaço, e emitir ordens e instruções adequadas à gravidade da situação;

g) Informar o Secretário-Geral do Sistema de Segurança Interna sobre a verificação de uma ciberameaça significativa ou sobre a ocorrência de uma crise ou incidente de cibersegurança em grande escala, nos termos das alíneas d) e k) do artigo 2.º, respetivamente e sem prejuízo do disposto no n.º 2 do artigo 21.º;

h) Emitir ordens, orientações, recomendações e instruções técnicas em matéria de divulgação coordenada de vulnerabilidades;

i) Prevenir e minorar o impacto de incidentes de cibersegurança, designadamente pela deteção e divulgação de vulnerabilidades em redes e sistemas de informação, em colaboração com entidades públicas e privadas, pessoas singulares e coletivas;

j) Aplicar as medidas de supervisão e de execução nos termos do disposto no Capítulo VI;

k) Emitir avisos, designadamente sobre vulnerabilidades, relativos a *malware* ou outros riscos de cibersegurança em produtos, componentes ou serviços TIC;

Proposta de Lei n.º .....

l) Assegurar a cooperação transfronteiriça com as autoridades competentes dos Estados-Membros da União Europeia, com a Comissão Europeia, com a Agência da União Europeia para a Cibersegurança (ENISA) e outras instituições, organismos e agências da União Europeia que desenvolvam atividades no âmbito da cibersegurança e das competências que lhe são cometidas pelo presente artigo, nomeadamente a participação e a representação nacional em fóruns multilaterais e bilaterais com as suas congéneres, sem prejuízo do disposto nos artigos 20.º a 26.º e 29.º da Lei do Cibercrime, incluindo a participação e representação nacional:

i) No Grupo de Cooperação, previsto no artigo 14.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro;

ii) Na Rede Europeia de CSIRTs (*Computer Security Incident Response Team*, na expressão e sigla de língua inglesa), prevista no artigo 15.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro; e

iii) Na Rede de Organizações de Coordenação de Cibercrises (UE-CyCLONe) prevista no artigo 16.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro.

m) Emitir parecer não vinculativo, quando solicitado, sobre qualquer medida legislativa relativa à cibersegurança;

n) Promover a sensibilização, formação e qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança e ciber-higiene;

o) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;

p) Publicar estudos e relatórios na área da cibersegurança;

q) Aprovar os formulários que se mostrem necessários adequados ao exercício das suas atribuições.

.....

Proposta de Lei n.º .....

2 - O CNCS tem, no exercício das responsabilidades atribuídas pelo n.º 4 do artigo 19.º, prossegue as atribuições e exerce as competências descritas nas alíneas seguintes:

a) Solicitar aos organismos de avaliação da conformidade, aos titulares de certificados de cibersegurança e aos emitentes de declarações de conformidade, as informações de que necessite para o exercício das suas competências;

b) Tomar as medidas adequadas a garantir que os organismos de avaliação da conformidade, os titulares de certificados nacionais ou europeus de cibersegurança, e os emitentes de declarações de conformidade cumprem o disposto na legislação aplicável em matéria de certificação da cibersegurança;

c) Exercer as demais competências legalmente estabelecidas para as autoridades de certificação da cibersegurança, designadamente as decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril, sem prejuízo das competências do GNS no que diz respeito à certificação e acreditação dos sistemas de informação e comunicação que tratam informação classificada, nos termos do Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual;

d) Implementar um quadro nacional de certificação da cibersegurança, estabelecendo as disposições necessárias à elaboração, implementação e execução dos esquemas de certificação, aos quais são aplicáveis, com as necessárias adaptações, as disposições constantes do título III do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril;

e) Avaliar os esquemas de certificação específicos, designadamente sobre a respetiva adequação, articulação com o Instituto Português de Acreditação, I. P., na qualidade de organismo nacional de acreditação, bem como com o Instituto Português da Qualidade, I. P., na qualidade de organismo nacional de normalização, e com as demais entidades públicas com competências no âmbito da matéria abrangida pela certificação;

Proposta de Lei n.º .....

f) Desenvolver e implementar esquemas específicos de certificação da cibersegurança relativos a entidades, produtos, serviços e processos de tecnologias de informação e comunicação que não sejam ainda abrangidos por um esquema europeu, sempre que a especificidade do objeto da certificação o justifique;

g) Promover a formação de auditores no âmbito da cibersegurança, em colaboração com o Instituto Português de Acreditação, I. P.

3 - Qualquer disposição regulamentar de cibersegurança emitida pelas autoridades nacionais setoriais ou especiais de cibersegurança é precedida de parecer do CNCS.

4 - As entidades públicas e privadas prestam a sua colaboração ao CNCS para o exercício das respetivas atribuições e competências ao abrigo do presente decreto-lei, no respeito pelo princípio da proporcionalidade.

5 - O dever de cooperação previsto no número anterior pode incluir o acesso físico às instalações das entidades para a realização de diligências integradas em ações de supervisão ou de resposta a incidentes, sem prejuízo do cumprimento de requisitos de acesso previstos noutros regimes especiais de segurança da informação e respeitadas as exigências previstas no Código do Procedimento Administrativo.

6 - O CNCS atua em estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo.

Artigo 21.º

Autoridade de gestão de crises de cibersegurança

1 - O Secretário-Geral do Sistema de Segurança Interna é a autoridade nacional de gestão de crises e incidentes de cibersegurança em grande escala, também designada por autoridade de gestão de crises de cibersegurança.

Proposta de Lei n.º .....

2 - A declaração de crises e incidentes de cibersegurança em grande escala, depende da atribuição de um grau de ameaça elevado pelo Serviço de Informações de Segurança, nos termos previstos no plano de coordenação, controlo e comando operacional das Forças e Serviços de Segurança, aprovado pela Deliberação do Conselho de Ministros n.º DB 14/2010, de 5 de março, ou da comunicação, pelo CNCS, da ocorrência de uma crise ou incidente de cibersegurança em grande escala, nos termos da alínea g) do n.º 1 do artigo 20.º.

3 - O Secretário-Geral do Sistema de Segurança Interna convoca o gabinete de crise de cibersegurança, nos termos do n.º 4 do artigo 16.º da Lei n.º 53/2008, de 29 de agosto, na sua redação atual.

Artigo 22.º

Equipa de Resposta a Incidentes de Cibersegurança

1 - O «CERT.PT» é a equipa nacional de resposta a incidentes de cibersegurança.

2 - O «CERT.PT» está integrado no CNCS e dispõe de autonomia técnica e operacional.

3 - O «CERT.PT» exerce as seguintes competências:

a) Garantir a resposta operacional a incidentes;

b) Monitorizar e analisar ciberameaças, vulnerabilidades e incidentes a nível nacional e, mediante pedido, prestar assistência a entidades essenciais, importantes e públicas relevantes relativamente à monitorização em tempo real ou quase real dos seus sistemas em rede e informação;

c) Ativar os mecanismos de alerta rápido, enviar mensagens de alerta, fazer comunicações e divulgar informações às entidades essenciais, importantes e públicas relevantes, a autoridades competentes, e a outras partes interessadas,

Proposta de Lei n.º .....

sobre ciberameaças, vulnerabilidades e incidentes, incluindo em tempo real;

d) Intervir em caso de incidentes e prestar assistência às entidades essenciais, importantes e públicas relevantes, nomeadamente, quando aplicável, propondo ao CNCS a emissão de ordens, instruções e orientações operacionais quanto a medidas que devem ser adotadas para conter, mitigar e resolver os incidentes, bem como os prazos adequados para a sua implementação;

e) Em situações de grave e comprovado risco, propor à autoridade de cibersegurança competente a adoção de medidas de execução necessárias para uma resposta imediata à ciberameaça, incidente ou crise, nos termos do n.º 3 do artigo 52.º, caso a entidade essencial, importante ou pública relevante em causa não o faça de forma voluntária;

f) Recolher e analisar dados forenses, determinar a sua preservação e proceder à análise dinâmica dos riscos e dos incidentes e desenvolver o conhecimento situacional em matéria de cibersegurança;

g) Realizar, a pedido de uma entidade essencial, importante ou pública relevante, uma análise proativa das respetivas redes e sistemas de informação da entidade, a fim de detetar vulnerabilidades com um potencial impacto significativo;

h) Implementar ferramentas e funcionalidades que permitam uma partilha segura de informação com as entidades essenciais, importantes e públicas relevantes, bem como com outras partes interessadas;

i) Realizar, por sua iniciativa, análises proativas e não intrusivas de redes e sistemas de informação acessíveis ao público de entidades essenciais, importantes e públicas relevantes, com o objetivo de detetar redes e sistemas de informação vulneráveis ou inseguros e informar as entidades em causa, na

Proposta de Lei n.º .....

medida em que não tenham qualquer impacto negativo no funcionamento dos serviços destas;

j) Promover a adoção e a utilização de práticas comuns ou normalizadas;

k) Assegurar a representação nacional na rede de equipas de resposta a incidentes de cibersegurança nacionais nos termos da subalínea ii), da alínea l) do n.º 1 do artigo 20.º e restantes fóruns internacionais de cooperação de equipas de resposta a incidentes de cibersegurança;

l) Participar nos fóruns nacionais de cooperação de equipas de resposta a incidentes de segurança informática;

m) Participar em eventos e ações de formação nacionais e internacionais;

n) Colaborar e articular a sua atuação com as redes de CSIRTs setoriais, nacionais e europeias, sempre que necessário ou conveniente;

o) Cooperar com as entidades competentes no âmbito da segurança do ciberespaço.

4 - No exercício das suas competências, o «CERT.PT» pode determinar a priorização de certas tarefas através de uma abordagem baseada no risco, considerando, designadamente, a avaliação de ameaça vigente e produzida pelo Serviço de Informações de Segurança.

5 - As entidades públicas e privadas prestam a sua colaboração ao «CERT.PT» para o exercício das respetivas atribuições e competências ao abrigo do presente decreto-lei.

6 - A colaboração referida no número anterior pode incluir o acesso físico às instalações e a partilha de informação entre as entidades que prestam serviços de resposta a incidentes a terceiros e o «CERT.PT», e ações conjuntas, por iniciativa deste, para efeitos da alínea e) do n.º 3.

Proposta de Lei n.º .....

Artigo 23.º

Cooperação entre autoridades nacionais

1 - O CNCS, o Secretário-Geral do Sistema de Segurança Interna e as autoridades nacionais setoriais de cibersegurança, no exercício das suas atribuições e competências ao abrigo do presente decreto-lei, atuam em cooperação estreita com:

a) A Comissão Nacional de Proteção de Dados, sempre que estejam em causa incidentes que tenham dado origem à violação de dados pessoais, nos termos do artigo 79.º;

b) O Ministério Público, os tribunais e a Polícia Judiciária, sempre que estejam em causa incidentes que possam ter dado origem à prática de cibercrimes, nomeadamente através:

i) Da comunicação, logo que possível, de factos relativos à preparação e execução de cibercrimes de que tenham tido conhecimento no exercício das suas funções, sem prejuízo do disposto no artigo 38.º;

ii) Da prática dos atos cautelares necessários e urgentes para assegurar a conservação de provas e da partilha, nos termos legais, de outros elementos probatórios necessários para o estrito exercício das competências previstas nas alíneas a) a e) do n.º 3 do artigo anterior;

iii) Do desempenho da função de perito prevista no artigo 153.º do Código do Processo Penal.

c) O Comando de Operações de Ciberdefesa, nomeadamente quando estejam em causa prevenção de incidentes, monitorização, deteção, reação, análise e correção no âmbito da ciberdefesa e da cibersegurança das Forças Armadas;

d) O Serviço de Informações de Segurança, nomeadamente na partilha de

Proposta de Lei n.º .....

informações necessárias à preservação da segurança do ciberespaço de interesse nacional, designadamente no que respeita à espionagem, à sabotagem, ao terrorismo e à criminalidade organizada.

2 - A obtenção de informação ao abrigo da cooperação prevista no número anterior deve respeitar a legislação aplicável em matéria de proteção de dados pessoais, designadamente, o RGPD, a Lei n.º 26/2016, de 22 de agosto, na sua redação atual, a Lei n.º 58/2019, de 8 de agosto e a Lei n.º 59/2019, de 8 de agosto.

3 - A cooperação prevista na alínea b) do n.º 1 não põe em causa o segredo de justiça.

4 - O acesso a informação nos termos da cooperação prevista, designadamente, nas subalíneas i) e ii) da alínea b) do n.º 1, relativa a processos que estejam a ser objeto de investigação, pode ser recusado com os fundamentos previstos no n.º 1 do artigo 89.º do Código de Processo Penal.

5 - A Polícia Judiciária e o Serviço de Informações de Segurança designam um elemento de ligação permanente junto do CNCS.

6 - Os termos da cooperação técnica e operacional entre o CNCS, o Comando de Operações de Ciberdefesa, a Polícia Judiciária, o Serviço de Informações de Segurança e o Serviço de Informações Estratégicas de Defesa, são definidos por mútuo acordo no âmbito do G5.

7 - As autoridades referidas neste artigo devem responder aos pedidos de informação no prazo de 5 dias após a data em que as informações tiverem sido solicitadas, salvo motivo devidamente justificado.

Artigo 24.º

Cooperação com o setor privado

1 - As entidades que integrem o quadro institucional da segurança do ciberespaço, nos

termos do artigo 15.º, devem estabelecer relações de cooperação com as entidades abrangidas pelo presente decreto-lei e, quando pertinente, com outras entidades interessadas do setor privado, com vista a alcançar os objetivos do regime jurídico da cibersegurança.

2 - As relações de cooperação devem abranger, pelo menos, os seguintes aspetos relativos à partilha de informação, adoção de boas práticas, desenvolvimento ou melhoria de sistemas de classificação e de taxonomias comuns ou normalizadas quanto a:

a) Medidas de gestão dos riscos de cibersegurança;

b) Indicadores de exposição a riscos ou ciberameaças;

c) Procedimentos de tratamento de incidentes;

d) Gestão de crises; e

e) Divulgação coordenada de vulnerabilidades, nos termos do artigo 38.º.

3 - A fim de promover a troca de conhecimento, a partilha de boas práticas e a mobilização de conhecimentos especializados de entidades do setor privado no apoio à autoridade de cibersegurança competente, podem ser adotadas parcerias público-privadas para a cibersegurança, definindo o âmbito e as partes envolvidas, o modelo de governação, as opções de financiamento disponíveis e a interação entre as partes participantes.

4 - Podem ser celebrados, entre as entidades referidas no n.º 1 bem como, quando pertinente, com os seus fornecedores ou prestadores de serviços, acordos de partilha de informações sobre cibersegurança, para os seguintes fins:

a) Evitar, detetar, responder e recuperar de incidentes ou atenuar o seu impacto;

b) Reforçar o nível de cibersegurança, em especial ao sensibilizar para as ciberameaças, limitar ou impedir a sua capacidade de disseminação, apoiar um

leque de capacidades defensivas, a correção e divulgação de vulnerabilidades, as técnicas de deteção, contenção e prevenção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação, ou promover a investigação colaborativa de ciberameaças entre entidades públicas e privadas.

5 - As partes signatárias dos acordos de partilha de informação, quando necessário, tomam medidas para proteger a natureza sensível das informações partilhadas e limitar a sua distribuição, em conformidade com o designado TLP (*Traffic Light Protocol,* na expressão e sigla de língua inglesa).

6 - As entidades essenciais e importantes são obrigadas a notificar a autoridade de cibersegurança competente da sua participação nos acordos referidos no n.º 4, aquando da sua celebração, ou, quando aplicável, da sua retirada de tais acordos, assim que esta produza efeitos.

7 - Os acordos referidos no n.º 4, quando celebrados por entidades essenciais e importantes abrangidas pelo Regulamento (UE) 2022/2554, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro, são comunicados às respetivas autoridades nacionais especiais de cibersegurança.

8 - O CNCS assegura e gere uma plataforma em linha para a partilha de informações.

Capítulo IV

Gestão dos riscos de cibersegurança e outros deveres

Secção I

Gestão da cibersegurança e da segurança da informação

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Artigo 25.º

Obrigações dos órgãos de gestão, direção e administração

1 - Os órgãos de gestão, direção e administração das entidades essenciais e importantes:

a) Aprovam as medidas de gestão dos riscos de cibersegurança, adotadas em conformidade com o artigo 27.º;

b) Supervisionam a aplicação das medidas de gestão dos riscos de cibersegurança;

c) Asseguram o cumprimento das medidas de supervisão e de execução, a que se refere o Capítulo VI do presente decreto-lei;

d) Asseguram a realização, com uma periodicidade regular, de ações de formação em cibersegurança, de forma a promover uma cultura de gestão interna sobre práticas de gestão dos riscos de cibersegurança.

2 - Os titulares dos órgãos de gestão, direção e administração podem responder por ação ou omissão, com dolo ou culpa grave, nos termos da legislação aplicável, pelas infrações previstas no presente decreto-lei.

3 - A responsabilidade e poderes necessários para o cumprimento das obrigações referidas no presente artigo não podem ser delegados, exceto num dos titulares dos órgãos de gestão, direção e administração.

Artigo 26.º

Sistema de gestão de riscos de cibersegurança

1 - As entidades essenciais e importantes são responsáveis por garantir a segurança das redes e dos sistemas de informação, tomando as medidas técnicas, operacionais e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e para impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros

Proposta de Lei n.º .....

serviços.

2 - As medidas de cibersegurança adotadas devem basear-se numa abordagem sistémica que abranja todos os riscos para as entidades essenciais e importantes e que vise proteger todos os ativos que garantam a continuidade do funcionamento das redes e os sistemas de informação que suportam os serviços essenciais, incluindo o seu ambiente físico, contra incidentes.

3 - As medidas devem ainda:

a) Garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes e, se aplicáveis, as normas europeias e internacionais pertinentes, bem como os custos de execução e a viabilidade financeira destes; e

b) Ser proporcionais ao grau de exposição da entidade aos riscos, a dimensão da entidade e a probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico, segundo os critérios técnicos que venham a ser definidos pelo CNCS.

4 - De forma a orientar a política de gestão de riscos de cibersegurança por parte das entidades essenciais e importantes, o CNCS pode emitir instruções técnicas de harmonização e, sempre que necessário, elaborar e atualizar a matriz de risco aplicável àquelas entidades.

5 - Considerando o setor de atividade e a dimensão da entidade e a matriz de risco definida, o CNCS, através de regulamento a aprovar pelo CNCS, define medidas de cibersegurança mínimas e específicas e níveis de conformidade a adotar pelas entidades essenciais e entidades importantes.

6 - As medidas de cibersegurança mínimas não prejudicam a adoção de outras medidas que sejam necessárias e proporcionais, em resultado da análise e gestão dos riscos residuais de cibersegurança, nos termos do artigo seguinte.

7 - As entidades públicas relevantes devem adotar as medidas técnicas, operacionais e organizativas adequadas que sejam determinadas pelo CNCS, de acordo com o grupo a que pertençam, nos termos do artigo 33.º.

Artigo 27.º

Medidas de cibersegurança

1 - As medidas de cibersegurança a adotar pelas entidades essenciais e importantes, tendo em consideração a matriz de risco em que estiverem inseridas nos termos do artigo 26.º, abrangem, designadamente, as seguintes áreas:

a) Tratamento de incidentes;

b) Continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises;

c) Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos;

d) Segurança na aquisição, desenvolvimento e manutenção das redes e sistemas de informação, incluindo o tratamento e a divulgação de vulnerabilidades;

e) Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;

f) Práticas básicas de ciber-higiene e formação em cibersegurança, incluindo os titulares de órgãos máximos de gestão e trabalhadores;

g) Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem, sem prejuízo das competências conferidas a outras entidades em matéria de criptografia no âmbito nacional ou perante outras organizações internacionais de que Portugal seja membro;

h) Segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos;

i) Utilização de autenticação multifator ou de autenticação contínua, comunicações seguras e sistemas seguros de comunicações de emergência no seio da entidade.

2 - As entidades essenciais e importantes devem adotar ainda, sem demora injustificada, todas as medidas de cibersegurança corretivas necessárias, adequadas e proporcionais, que sejam indispensáveis ao suprimento de falhas ou omissões no cumprimento das medidas previstas no número anterior.

3 - As autoridades nacionais setoriais de cibersegurança podem emitir disposições regulamentares para adoção de medidas de cibersegurança específicas do sector, sem prejuízo do disposto no n.º 3 do artigo 20.º.

Artigo 28.º

Cadeia de abastecimento

As medidas de cibersegurança relativas à segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos, devem considerar, designadamente:

a) As vulnerabilidades específicas de cada fornecedor direto e cada prestador de serviços;

b) A qualidade global dos produtos na componente de cibersegurança;

c) As práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro;

d) As avaliações coordenadas dos riscos de segurança de cadeias de abastecimento de produtos de TIC, sistemas de TIC ou serviços de TIC críticos que sejam realizadas nos termos do artigo 22.º da Diretiva (EU) 2022/2555, do Parlamento Europeu e do

Proposta de Lei n.º .....

Conselho, de 14 de dezembro;

e) As decisões relativas à aplicação de restrições à utilização, a cessação de utilização ou exclusão de equipamentos, componentes ou serviços de tecnologias de informação e comunicação, ao abrigo do disposto no n.º 3 do artigo 18.º.

Artigo 29.º

Gestão do risco residual

1 - As entidades essenciais e importantes devem realizar uma análise e gestão de riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e sistemas de informação que utilizam, incluindo aos ativos que garantam a prestação dos serviços essenciais, com a periodicidade e os elementos técnicos e documentais a definir por regulamento da autoridade de cibersegurança competente, para além do cumprimento das medidas de cibersegurança mínimas nos termos do n.º 5 do artigo 26.º.

2 - Com base na análise e gestão de riscos referida no número anterior, as entidades essenciais e importantes devem adotar as medidas de cibersegurança adequadas e proporcionais de forma a gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, incluindo os riscos residuais, tendo em conta o QNRCS, os progressos técnicos mais recentes e, se aplicáveis, as normas europeias e internacionais pertinentes.

3 - As entidades essenciais e importantes devem documentar a preparação, a execução e a apresentação dos resultados da análise dos riscos.

Artigo 30.º

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Relatório anual

1 - As entidades essenciais e importantes devem elaborar e manter um relatório anual que contenha os seguintes elementos em relação ao ano civil a que se reportam:

a) Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação;

b) Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;

c) Análise agregada dos incidentes com impacto significativo, com informação sobre:

i) Número de utilizadores afetados pela perturbação serviço;

ii) Duração dos incidentes;

iii) Distribuição geográfica, no que se refere à zona afetada pelos incidentes, incluindo a indicação de impacto transfronteiriço.

d) Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação;

e) Problemas identificados e medidas implementadas na sequência dos incidentes;

f) Qualquer outra informação que se considere relevante.

2 - As entidades essenciais remetem o relatório anual à autoridade de cibersegurança competente, devidamente assinado pelo responsável de cibersegurança, nos seguintes termos:

a) O primeiro relatório anual é submetido:

i) Até ao último dia útil do mês de janeiro do ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha tido início no primeiro semestre;

Proposta de Lei n.º .....

ii) Até ao último dia útil do mês de janeiro do segundo ano civil seguinte ao primeiro ano civil de atividade, quando esta tenha tido início no segundo semestre.

b) Os relatórios anuais subsequentes são submetidos até ao último dia útil do mês de janeiro do ano civil seguinte aos quais os mesmos se reportam.

3 - Para efeitos do disposto na subalínea ii) da alínea a) do número anterior, o relatório anual deve abranger também o período entre a data de início de atividade e o final do ano civil anterior ao que se reporta.

4 - As entidades importantes devem comunicar o relatório anual ao CNCS sempre que solicitado.

5 - O CNCS, ouvidas as autoridades nacionais setoriais de cibersegurança, pode adotar modelos para a apresentação do relatório referido nos números anteriores.

Artigo 31.º

Responsável de cibersegurança

1 - As entidades essenciais e importantes designam um responsável de cibersegurança para a gestão da cibersegurança e da segurança da informação, que seja titular dos órgãos de gestão, direção ou administração ou lhes responda organicamente e de forma direta.

2 - O responsável de cibersegurança tem, pelo menos, as seguintes funções:

a) Propor as medidas de gestão dos riscos de cibersegurança, incluindo ao nível da cadeia de abastecimento, que devem ser aprovadas nos termos da alínea a) do n.º 1 do artigo 25.º;

b) Prestar informações relativas às medidas de gestão dos riscos de cibersegurança aos órgãos da entidade responsável pela sua supervisão nos termos da alínea b)

Proposta de Lei n.º .....

do n.º 1 do artigo 25.º;

c) Auxiliar os órgãos da entidade no cumprimento das medidas de supervisão e de execução nos termos da alínea c) do n.º 1 do artigo 25.º;

d) Contribuir para a promoção de uma cultura de cibersegurança na entidade, propondo, nomeadamente, as ações de formação em cibersegurança previstas na alínea d) do n.º 1 do artigo 25.º;

e) Assegurar a gestão de riscos prevista no artigo 29.º;

f) Assegurar o cumprimento das obrigações referentes à elaboração do relatório anual nos termos do artigo 30.º;

g) Coordenar as ações do ponto de contacto permanente, previstas no artigo 32.º, quando esta função não seja assegurada por si;

3 - As entidades essenciais e importantes comunicam à autoridade de cibersegurança competente, no prazo de 20 dias úteis a contar do início de funções, a pessoa designada para exercer as funções de responsável de cibersegurança, incluindo a informação referida em regulamento a aprovar pelo CNCS.

4 - As entidades essenciais e importantes que tenham iniciado atividade antes da data de entrada em vigor do presente decreto-lei, efetuam a comunicação prevista no número anterior no prazo de 20 dias úteis, a contar desta data.

5 - As entidades essenciais e importantes comunicam, sem demora injustificada, às autoridades de cibersegurança competentes, a substituição do responsável de cibersegurança.

6 - Relativamente às entidades essenciais e importantes que pertençam à administração direta, pode ser designado o mesmo responsável de cibersegurança para vários ministérios, áreas governativas ou secretarias regionais.

7 - Relativamente às entidades essenciais e importantes inseridas no mesmo grupo

empresarial, pode cada empresa estabelecer um elemento que funcione como ponto de contacto para a cibersegurança sob coordenação de um responsável de segurança comum ao grupo.

8 - O exercício das funções de responsável de cibersegurança é compatível com a acumulações de outras funções dentro da mesma entidade, sem prejuízo do disposto no presente artigo.

Artigo 32.º

Ponto de contacto permanente

1 - As entidades essenciais e importantes asseguram a função do ponto de contacto permanente com uma disponibilidade contínua de 24 horas por dia e de sete dias por semana, limitada a períodos de ativação, iniciados e terminados mediante comunicação da autoridade de cibersegurança competentes.

2 - As entidades essenciais e importantes comunicam ao CNCS, pelo menos, um ponto de contacto permanente, que pode ser assegurado por um elemento ou uma equipa, de modo a assegurar:

a) Os fluxos de informação de nível operacional e técnico com a autoridade de cibersegurança competente, nomeadamente:

i) A articulação intersectorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores;

ii) A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto significativo submetida pela mesma ou por outra entidade;

iii) A obtenção e atualização de informação de situação integrada no contexto de um incidente significativo.

Proposta de Lei n.º .....

b) A partilha de informação com a autoridade de cibersegurança competente, quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da cibersegurança bem como de planos no âmbito do planeamento civil de emergência da cibersegurança, dos planos de segurança das infraestruturas críticas nacionais ou europeias, ou dos planos de resiliência das entidades críticas nacionais ou europeias;

c) A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência da cibersegurança;

d) A receção das orientações, recomendações, instruções técnicas e ordens emitidas pela autoridade de cibersegurança competente.

3 - As entidades essenciais e importantes devem indicar à autoridade de cibersegurança competente, no prazo de 20 dias úteis a contar do início de funções, a pessoa ou pessoas que compõem a equipa que asseguram as funções de ponto de contacto permanente, bem como os respetivos meios de contacto principal e alternativos contendo a informação referida em regulamento a aprovar pelo CNCS.

4 - As entidades essenciais e importantes que tenham iniciado atividade antes da data de entrada em vigor do presente decreto-lei devem efetuar a comunicação prevista no número anterior no prazo de 20 dias úteis a contar desta data.

5 - As entidades essenciais e importantes devem comunicar imediatamente à autoridade de cibersegurança competente, qualquer alteração à informação prevista no n.º 3.

6 - As entidades essenciais e importantes devem assegurar que o ponto de contacto permanente dispõe de meios de contacto principais e alternativos para a comunicação com a autoridade de cibersegurança competente.

.....

Proposta de Lei n.º .....

Artigo 33.º

Medidas de cibersegurança aplicáveis às entidades públicas relevantes

1 - As entidades públicas relevantes devem cumprir com as medidas de cibersegurança estabelecidas pelo CNCS nos termos do número seguinte.

2 - O CNCS estabelece, através de regulamento, as medidas de cibersegurança que devem ser cumpridas por parte das entidades públicas relevantes, considerando os critérios previstos no disposto nos n.ºs 2 e 3 do artigo 26.º e em termos proporcionais e adequados ao grupo a que pertencem, de acordo com o disposto no artigo 7.º.

3 - As entidades públicas relevantes estão sujeitas às medidas de supervisão e de execução previstas nos artigos 55.º e 56.º, respetivamente.

Artigo 34.º

Certificação da cibersegurança

1 - O CNCS pode exigir às entidades essenciais, importantes e públicas relevantes, a obtenção de certificação, nacional, europeia ou internacional, que ateste o cumprimento das medidas de cibersegurança do presente decreto-lei, nomeadamente em conformidade com esquemas de certificação elaborados a partir do Documento Normativo Português - Especificação Técnica (DNP TS) 4577-1, Maturidade Digital - Selo Digital e do Quadro Nacional de Referência para a Cibersegurança, assegurando, em todo caso, uma matriz de equivalência com esquemas de certificação de referência existentes.

2 - O CNCS pode ainda exigir às entidades essenciais, importantes e públicas relevantes, nos termos do n.º 1 do artigo 24.º da Diretiva (UE) 2022/2555, do Parlamento e do Conselho, de 14 de dezembro, a utilização de produtos, serviços e processos, todos

Proposta de Lei n.º .....

de TIC, desenvolvidos pela entidade ou fornecidos por terceiros, certificados no âmbito de sistemas nacionais e europeus de certificação da cibersegurança, adotados nos termos do artigo 49.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

Secção II

Outros deveres

Artigo 35.º

Dever de registo

1 - Para efeitos de registo, as entidades essenciais, importantes e públicas relevantes têm o dever de inscrever na plataforma eletrónica referida no n.º 7 do artigo 8.º os elementos que permitam a sua identificação completa, designadamente:

a) Nome da entidade em causa;

b) Número de identificação fiscal;

c) Endereço e dados de contacto atualizados, incluindo os endereços de correio eletrónico, as gamas de endereços IP e os números de telefone;

d) Se aplicável, o setor e subsetor pertinentes referidos nos anexos I ou II ao presente decreto-lei, que dela fazem parte integrante; e

e) Se aplicável, uma lista dos Estados-Membros da União Europeia em que prestam serviços abrangidos pelo âmbito de aplicação do presente decreto-lei.

2 - Além dos dados referidos no número anterior, o registo de nomes de domínio de topo, bem como as entidades que sejam prestadores de serviços de DNS, prestadores

Proposta de Lei n.º .....

serviços de registo de nomes de domínio, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados, fornecedores de redes de distribuição de conteúdos, prestadores de serviços geridos, prestadores de serviços de segurança geridos, bem como dos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, têm o dever de inscrever na plataforma eletrónica referida no n.º 7 do artigo 8.º os seguintes elementos:

a) O endereço do respetivo estabelecimento principal e dos outros estabelecimentos legais que possui na União Europeia ou, caso não esteja estabelecida na União, do representante designado;

b) Contactos atualizados, incluindo endereços de correio eletrónico e números de telefone da entidade e, se aplicável, do seu representante designado;

c) Os Estados-Membros onde presta serviços; e

d) As gamas de endereços IP.

3 - As entidades essenciais, importantes, públicas relevantes e os prestadores de serviços de registos de nomes de domínio notificam o CNCS de qualquer alteração aos dados referidos nos números anteriores, no prazo de 30 dias úteis a contar da alteração.

4 - No caso do registo de nomes de TLD, bem como as entidades que sejam prestadores de serviços de DNS, prestadores serviços de registo de nomes de domínio, prestadores de serviços de computação em nuvem, prestadores de serviços de centro de dados, fornecedores de redes de distribuição de conteúdos, prestadores de serviços geridos, prestadores de serviços de segurança geridos, bem como dos prestadores de serviços de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais, a alteração aos dados referidos nos n.ºs 1 e 2 é notificada no prazo de 3 meses a contar da alteração.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Artigo 36.º

Base de dados relativos ao registo de nomes de domínio

1 - O registo de nomes de domínio de topo e as entidades que prestam serviços de registo de nomes de domínio devem recolher e manter os dados exatos e completos relativos ao registo de nomes de domínio em bases de dados criadas especificamente para o efeito.

2 - A recolha e manutenção dos dados referidos no número anterior constitui uma obrigação jurídica nos termos e para os efeitos do artigo 6.º, n.º 1, alínea c), do RGPD.

3 - A base de dados referida no n.º 1 contém a seguinte informação:

a) O nome de domínio;

b) A data de registo;

c) O nome, o endereço de correio eletrónico de contato e o número de telefone do titular de registo;

d) O endereço de contacto e o número de telefone de contacto que administra o nome de domínio, caso sejam diferentes do titular de registo.

4 - O registo de nomes de domínio de topo e as entidades que prestam serviços de domínio adotam políticas e procedimentos, incluindo de verificação, para assegurar que as respetivas bases de dados, nos termos do n.º 1, contêm informações exatas e completas.

5 - Os dados relativos ao registo de nomes de domínio e as políticas e procedimentos referidos nos números anteriores devem ser acessíveis ao público, quando não sejam dados pessoais e não se encontrem protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais, designadamente, o RGPD, a Lei n.º 26/2016,

Proposta de Lei n.º .....

de 22 de agosto, na sua redação atual, a Lei n.º 58/2019, de 8 de agosto e a Lei n.º 59/2019, de 8 de agosto.

Artigo 37.º

Acesso ao registo de nomes de domínio

1 - O registo de nomes de domínio de topo e as entidades que prestam serviços de registo de nomes de domínio garantem o acesso a dados específicos relativos ao registo de nomes de domínio a quem apresente um pedido de acesso lícito e devidamente fundamentado, em conformidade com a legislação aplicável em matéria de proteção de dados pessoais, designadamente, o RGPD, a Lei n.º 26/2016, de 22 de agosto, na sua redação atual, a Lei n.º 58/2019, de 8 de agosto, e a Lei n.º 59/2019, de 8 de agosto.

2 - Os pedidos de acesso referidos no número anterior são concedidos no prazo de 72 horas a contar da receção do mesmo.

Capítulo V

Prevenção e tratamento de incidentes

Secção I

Prevenção e acompanhamento de vulnerabilidades

Artigo 38.º

Vulnerabilidades em sistemas de informação

1 - O «CERT.PT» é a entidade coordenadora nacional para efeitos da divulgação

coordenada de vulnerabilidades que afetem redes e sistemas de informação, produtos, componentes e serviços de tecnologias de informação e comunicação.

2 - O «CERT.PT» desempenha o papel de intermediário de confiança, facilitando a interação entre a pessoa singular ou coletiva notificadora e o fabricante ou fornecedor de produtos de TIC ou prestador de serviços de TIC que sejam potencialmente vulneráveis, a pedido de qualquer uma das partes.

3 - As funções da «CERT.PT» incluem, designadamente:

a) A identificação e o contacto das entidades referidas no número anterior;

b) A prestação de apoio às pessoas singulares ou coletivas que notifiquem vulnerabilidades;

c) A negociação do calendário de divulgação e a gestão das vulnerabilidades que afetem várias entidades.

4 - O «CERT.PT» preserva o anonimato de qualquer pessoa singular ou coletiva que comunique uma vulnerabilidade, caso esta lho solicite, sem prejuízo do disposto na Lei do Cibercrime, aprovada pela Lei n.º 109/2009, de 15 de setembro, na redação introduzida pelo presente decreto-lei.

5 - Os dados incluídos nas comunicações realizadas ao abrigo do presente artigo devem ser eliminados no prazo de 10 dias, contados a partir do momento em que a vulnerabilidade seja corrigida, devendo garantir-se a confidencialidade dos mesmos durante todo o procedimento.

Artigo 39.º

Comunicação de vulnerabilidades

Quando a vulnerabilidade possa ter impacto importante sobre entidades em mais do que um Estado-Membro da União Europeia, o «CERT.PT» coopera com as suas congéneres, quer

.....

Proposta de Lei n.º .....

no âmbito da Rede Europeia de CSIRTs, quer no âmbito da UE-CyCLONe.

Secção II

Notificação de incidentes

Artigo 40.º

Notificação obrigatória

1 - As entidades essenciais, importantes e públicas relevantes notificam qualquer incidente significativo à autoridade de cibersegurança competente.

2 - O cumprimento da mera notificação não gera responsabilidade acrescida para a entidade notificante.

3 - A fim de determinar se um incidente tem impacto significativo nos termos do n.º 1, as entidades em causa devem ter em consideração, designadamente, os seguintes parâmetros:

a) Número de utilizadores afetados pela perturbação do serviço;

b) A duração do incidente;

c) O nível da gravidade da perturbação do funcionamento do serviço;

d) A dimensão do impacto nas atividades económicas e sociais.

4 - As entidades devem ainda ter em consideração os parâmetros e limiares definidos, quando aplicável, por instrução técnica do CNCS e pelos atos de execução da Comissão, previstos no n.º 11 do artigo 23.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro.

Proposta de Lei n.º .....

5 - O cumprimento do disposto no presente decreto-lei não dispensa o respeito pelas obrigações específicas de notificação de incidentes nos termos definidos pelas autoridades com competência para o efeito, nomeadamente o Ministério Público, a Polícia Judiciária, a Comissão Nacional de Proteção de Dados (CNPD), a Entidade Fiscalizadora do Segredo de Estado e o GNS, de acordo com as disposições legais e regulamentares aplicáveis.

6 - As notificações devem ser submetidas na plataforma eletrónica referida no n.º 7 do artigo 8.º.

7 - Às entidades essenciais, importantes e públicas relevantes é assegurada a possibilidade de notificar um incidente, simultaneamente, à autoridade de cibersegurança competente, às autoridades especiais de cibersegurança, bem como às entidades previstas no n.º 5, através da plataforma prevista no n.º 7 do artigo 8.º, nos termos a definir por protocolo outorgado entre as referidas autoridades.

Artigo 41.º

Tipos de notificações

1 - Por cada incidente sujeito a notificação obrigatória, as entidades essenciais, importantes e públicas relevantes submetem:

a) Uma notificação inicial, nos termos do artigo 42.º;

b) Uma notificação de fim do impacto significativo, nos termos do artigo 43.º;

c) Um relatório final, nos termos dos artigos 44.º.

2 - Nos casos em que o incidente é resolvido nas duas horas após a sua deteção, as entidades referidas ficam apenas obrigadas ao envio da notificação do fim de impacto significativo.

3 - Sem prejuízo do disposto no número anterior, as entidades essenciais, importantes e

públicas relevantes poderão ainda ser notificadas para apresentar um relatório intercalar, nos termos do artigo 44.º.

4 - O formato e procedimento de notificação de incidentes e a taxonomia dos incidentes, incluindo as categorias de causas dos incidentes e os seus efeitos, são definidos por instrução técnica do CNCS, sem prejuízo dos atos de execução adotados pela Comissão previstos no n.º 11 do artigo 23.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro.

Artigo 42.º

Notificação inicial

1 - A notificação inicial deve ser enviada à autoridade de cibersegurança competente, assim que a entidade essencial, importante ou pública relevante concluir que existe, ou possa vir a existir, um incidente significativo, sem demora injustificada e até 24 horas após essa verificação, salvo quando tal for incompatível com a mitigação ou a resolução do incidente.

2 - A notificação inicial deve incluir, pelo menos, a seguinte informação:

a) Nome, número de telefone e endereço de correio eletrónico de um representante da entidade, quando diferente do ponto de contacto permanente a que se refere o artigo 32.º, para efeito de um eventual contacto pela autoridade de cibersegurança competente;

b) Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção do incidente;

c) Breve descrição do incidente, incluindo a indicação da categoria da causa e dos efeitos produzidos, de acordo com a taxonomia definida pelo CNCS, sempre que possível, o respetivo detalhe;

d) Estimativa possível do impacto, considerando:

i) Número de utilizadores afetados pela perturbação do serviço;

ii) Duração do incidente;

iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação do impacto transfronteiriço;

iv) Outra informação que a entidade essencial e importante considere relevante.

3 - Quando necessário, a entidade essencial, importante ou pública relevante envia à autoridade de cibersegurança competente uma atualização da notificação inicial até 72 horas após a verificação do incidente significativo, revendo a informação referida no número anterior e fornecendo uma avaliação inicial do incidente significativo, incluindo da sua gravidade e do seu impacto, bem como, se disponíveis, dos indicadores de exposição a riscos.

Artigo 43.º

Notificação do fim de impacto significativo

1 - A notificação do fim de impacto significativo do incidente deve ser submetida à autoridade de cibersegurança competente, sem demora injustificada e dentro do prazo de 24 horas após o fim do impacto.

2 - A notificação do fim de impacto significativo deve incluir a seguinte informação, pelo menos:

a) Atualização da informação transmitida na notificação inicial, caso exista;

b) Breve descrição das medidas adotadas para a resolução do incidente;

c) Descrição da situação de impacto existente no momento da perda de impacto

Proposta de Lei n.º .....

significativo, nomeadamente:

i) Número de utilizadores afetados pela perturbação do serviço;

ii) Duração do incidente;

iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;

iv) Tempo estimado para a recuperação total dos serviços.

Artigo 44.º

Relatórios final e intercalar

1 - O relatório final deve ser submetido à autoridade de cibersegurança competente, no prazo de 30 dias úteis a contar da data da notificação do fim de impacto significativo do incidente.

2 - O relatório final deve incluir a seguinte informação:

a) Data e hora em que o incidente assumiu o impacto significativo;

b) Data e hora em que o incidente perdeu o impacto significativo;

c) Impacto do incidente, considerando:

i) Número de utilizadores afetados pela perturbação do serviço;

ii) Duração do incidente;

iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;

iv) Descrição do incidente, com a indicação da categoria da causa e dos efeitos produzidos, de acordo com a taxonomia definida pelo CNCS, e o respetivo detalhe;

Proposta de Lei n.º .....

d) Indicação das medidas adotadas para mitigar o incidente;

e) Descrição da situação residual do impacto existente à data da notificação final, nomeadamente:

i) Número de utilizadores afetados pela perturbação do serviço;

ii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;

iii) Tempo estimado para a recuperação total dos serviços ainda afetados;

iv) Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente ao Ministério Público ou à CNPD e a outras autoridades setoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis;

v) Outra informação que a entidade essencial e importante considere relevante.

3 - Na hipótese de, decorrido o prazo para apresentação do relatório final, o incidente ainda se encontrar em curso, a entidade essencial, importante ou pública relevante em causa deve apresentar relatório intercalar a autoridade de cibersegurança competente, a pedido destas entidades e com periodicidade semanal até ao momento da apresentação do relatório final.

4 - O relatório intercalar deve incluir a seguinte informação:

a) Atualização da informação transmitida na notificação inicial, caso exista;

b) Breve descrição das medidas adotadas para a resolução do incidente;

c) Descrição da situação de impacto existente no momento da perda de impacto significativo, nomeadamente:

i) Número de utilizadores afetados pela perturbação do serviço;

ii) Duração do incidente;

iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;

iv) Tempo estimado para a recuperação total dos serviços.

Artigo 45.º

Notificações voluntárias de informações pertinentes

1 - Sem prejuízo da obrigação de notificação de incidentes prevista no presente decreto-lei, qualquer pessoa singular ou coletiva pode notificar, a título voluntário, a ocorrência de incidentes, ciberameaças, quase incidentes ou vulnerabilidades.

2 - As notificações voluntárias não geram obrigações adicionais para a entidade notificante.

3 - O disposto nos artigos 42.º a 44.º aplica-se, com as devidas adaptações, às notificações voluntárias, sem prejuízo da prioridade a dar ao tratamento das notificações obrigatórias.

Artigo 46.º

Pedidos de informação

A autoridade de cibersegurança competente pode solicitar às entidades essenciais, importantes ou públicas relevantes, as informações relevantes ou determinar as ações necessárias, nos termos legalmente aplicáveis, quando tenha conhecimento, por qualquer meio, de um potencial incidente, aplicando-se, com as devidas adaptações, o disposto nos artigos 42.º a 44.º.

Proposta de Lei n.º .....

Artigo 47.º

Proteção da informação

1 - O envio de informações pelo CNCS ou, quando aplicável, pelas autoridades nacionais setoriais de cibersegurança, ao abrigo do presente decreto-lei, para autoridades ou entidades competentes nacionais, da União Europeia ou de outro Estado-Membro limita-se ao necessário e proporcional, em conformidade com a legislação aplicável em matéria de proteção de dados pessoais, designadamente, o RGPD, a Lei n.º 26/2016, de 22 de agosto, na sua redação atual, a Lei n.º 58/2019, de 8 de agosto e a Lei n.º 59/2019, de 8 de agosto.

2 - A autoridade de cibersegurança competente garante a proteção adequada das informações e dados, qualquer que seja a sua natureza, transmitidos pelas entidades essenciais, importantes e públicas relevantes em matéria de confidencialidade e segredo comercial.

3 - O n.º 2 aplica-se, com as devidas adaptações, às informações fornecidas pelas pessoas singulares e coletivas que procedam a uma notificação ao abrigo do artigo anterior.

Artigo 48.º

Comunicação aos destinatários dos serviços

1 - As entidades essenciais, importantes e públicas relevantes comunicam aos destinatários dos seus serviços, sem demora injustificada, quaisquer incidentes com impacto significativo que sejam suscetíveis de os afetar negativamente.

2 - As entidades essenciais, importantes e públicas relevantes comunicam aos destinatários dos seus serviços potencialmente afetados por uma ciberameaça significativa, sem demora injustificada, as medidas ou soluções que estes podem adotar para responder à ameaça e, quando apropriado, comunicam aos mesmos a

ciberameaça em causa.

3 - A comunicação referida no número anterior não dispensa as entidades em causa do dever de, a expensas suas, adotarem as medidas adequadas e imediatas para prevenir ou remediar quaisquer ameaças e restabelecer o nível normal de segurança do serviço que prestam.

4 - A informação referida nos números anteriores deve ser prestada de forma gratuita e em linguagem facilmente compreensível.

Secção III

Comunicação de incidentes, informação ao público e resposta

Artigo 49.º

Comunicação entre autoridades

1 - As autoridades nacionais setoriais e especiais de cibersegurança comunicam ao CNCS todos os incidentes de que são notificados nos termos do disposto no artigo 40.º, e informam aquela autoridade da respetiva evolução.

2 - Para efeitos do artigo 21.º, o CNCS comunica ao Secretário-Geral do Sistema de Segurança Interna, sem demora injustificada, os incidentes de que são notificados nos termos do disposto no artigo 40.º, que sejam suscetíveis de ser qualificados como de grande escala.

3 - O CNCS informa, quando entenda ser necessário, as autoridades nacionais setoriais e especiais de cibersegurança das notificações voluntárias nos termos do artigo 45.º.

4 - O disposto no presente artigo aplica-se, com as devidas adaptações, às notificações efetuadas nos termos do artigo 42.º.

5 - As comunicações referidas nos números anteriores são feitas de forma imediata, através de meios eletrónicos.

Artigo 50.º

Comunicação a entidades no âmbito da União Europeia ou dos seus Estados-Membros

1 - Sempre que se justificar, nomeadamente quando um incidente significativo envolver pelo menos outro Estado-Membro da União Europeia, o CNCS deve informar os outros Estados-Membros afetados, designados ao abrigo do artigo 8.º da Diretiva (EU) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, e a ENISA da ocorrência do mesmo, com envolvimento dos canais de cooperação em matéria de cooperação policial e em matéria de serviços de informações.

2 - A comunicação referida no número anterior inclui as informações recebidas através das notificações feitas nos termos dos artigos 42.º e seguintes.

3 - Compete ao CNCS, na qualidade de ponto de contacto único, apresentar trimestralmente à ENISA um relatório de síntese que inclua dados anonimizados e agregados sobre os incidentes significativos, os incidentes, as ciberameaças e os quase incidentes notificados nos termos dos artigos 40.º e 45.º.

Artigo 51.º

Informação ao público

1 - A autoridade de cibersegurança competente deve informar o público da ocorrência de um incidente significativo, após consulta com a entidade em causa, quando:

a) For necessário esclarecer o público para evitar o incidente ou para responder a um incidente em curso;

b) A divulgação do incidente significativo seja de interesse público.

Proposta de Lei n.º .....

2 - A autoridade de cibersegurança competente deve também exigir que a entidade em causa proceda à divulgação ao público do incidente significativo, quando estejam em causa as situações referidas no número anterior.

3 - A autoridade de cibersegurança competente deve informar o público de um incidente significativo, perante pedido de uma autoridade competente de outro Estado-Membro da União Europeia.

4 - A comunicação ao público prevista no presente artigo não prejudica a cooperação em sede de investigações criminais em curso, ou que estejam abrangidas pelos regimes de segredo de justiça e de segredo de Estado.

Artigo 52.º

Resposta a notificações

1 - A autoridade de cibersegurança competente responde à entidade notificante, sem demora injustificada e, se possível, no prazo de 24 horas após a receção da notificação inicial prevista no artigo 42.º.

2 - A autoridade de cibersegurança competente fornece, na sua resposta, designadamente, as suas observações iniciais sobre o incidente significativo e, a pedido da entidade, orientações ou aconselhamento operacional sobre a aplicação de possíveis medidas de atenuação.

3 - Em situações de grave e comprovado risco do impacto do incidente notificado nos termos do artigo 40.º, a autoridade de cibersegurança competente pode impor, como medida de execução imediata, a interrupção da prestação de serviço à entidade essencial, importante ou pública relevante em causa, ou a cessação de uma conduta que infringe o presente decreto-lei, caso esta não o faça de forma voluntária.

4 - Nos casos de suspeita fundada da natureza criminosa do incidente significativo, a

autoridade de cibersegurança competente deve fornecer igualmente orientações sobre a notificação do incidente significativo às autoridades policiais.

5 - O disposto nos números anteriores aplica-se, com as necessárias adaptações, aos incidentes, quase incidentes ou ciberameaças que tenham sido notificados, de forma voluntária, ao abrigo do artigo 45.º.

Capítulo VI

Supervisão e execução

Secção I

Medidas de supervisão e execução

Artigo 53.º

Princípios

1 - A autoridade de cibersegurança competente, na qualidade de autoridade de supervisão e de execução, fiscaliza e supervisiona o cumprimento do presente decreto-lei e adota as medidas necessárias para garantir esse cumprimento.

2 - As atividades de supervisão e de execução são orientadas, designadamente, pelos princípios da prossecução do interesse público, da legalidade, da eficiência, da eficácia e da proporcionalidade, devendo minimizar, sempre que possível, o seu impacto nas atividades públicas, sociais e empresariais das entidades supervisionadas.

3 - A atividade de supervisão assenta em metodologias de avaliação de risco e, com fundamento nessa avaliação e nos princípios referidos no número anterior, pode determinar a afetação prioritária de recursos e as medidas a adotar em função da

matriz de risco aplicável à entidade em causa, nomeadamente no que respeita à realização, frequência ou tipo de inspeções no local, às auditorias de segurança direcionadas ou verificações de segurança e ao tipo de informações a solicitar.

4 - As atividades de supervisão e de execução são exercidas com autonomia operacional, incluindo as que visam as entidades públicas relevantes.

5 - As atividades de supervisão e de execução respeitam as garantias dos particulares legal e constitucionalmente previstas.

Artigo 54.º

Medidas de supervisão relativas a entidades essenciais

1 - A autoridade de cibersegurança competente dispõe, relativamente a entidades essenciais, de poderes para as submeter às seguintes medidas:

a) Inspeções no local e a supervisão remota, incluindo controlos aleatórios efetuados por profissionais qualificados;

b) Auditorias de segurança, regulares ou direcionadas, realizadas pela própria autoridade competente ou, quando tal se justifique, por uma entidade devidamente qualificada para o efeito que ofereça garantias de independência;

c) Auditorias *ad hoc*, designadamente com fundamento na verificação de incidente significativo, incumprimento de ordens, instruções e orientações da autoridade de cibersegurança competente ou infração ao presente decreto-lei por parte da entidade em causa;

d) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes, se necessário em cooperação com a entidade em causa;

e) Pedidos de informações necessários para avaliar o cumprimento das medidas de

Proposta de Lei n.º .....

cibersegurança referidas nos artigos 27.º e seguintes, adotadas pela entidade em causa;

f) Pedidos de acesso a dados, documentos e informações necessários ao desempenho das suas funções de supervisão;

g) Pedidos de apresentação das provas demonstrativas da aplicação das políticas e procedimentos de cibersegurança.

2 - As auditorias direcionadas referidas na alínea b) do n.º 1 baseiam-se na análise de risco realizada pela autoridade de cibersegurança competente, na análise de risco realizada pela entidade auditada ou noutras informações disponíveis relacionadas com os riscos, nomeadamente as constantes das instruções técnicas de harmonização e as matrizes de risco elaboradas pelo CNCS, nos termos do n.º 4 do artigo 26.º, bem como das ordens, instruções e orientações da autoridade de cibersegurança competente.

3 - Os custos das auditorias direcionadas referidas nas alíneas b) do n.º 1, são suportados pela entidade auditada, salvo decisão contrária fundamentada da autoridade de cibersegurança competente.

4 - Os pedidos de informação e de prova referidos nas alíneas e) a g) no n.º 1 devem indicar a respetiva finalidade, especificar a informação solicitada e fixar um prazo adequado e razoável para a entidade essencial lhes dar resposta.

Artigo 55.º

Medidas de supervisão relativas a entidades importantes e públicas relevantes

1 - Sempre que obtenha provas, indícios ou informações de que uma entidade importante ou pública relevante não está a cumprir o presente decreto-lei, a autoridade de cibersegurança competente aplica as medidas de supervisão *ex post*

previstas nos números seguintes.

2 - A autoridade de cibersegurança competente dispõe, relativamente a entidades importantes, de poderes para as submeter às seguintes medidas:

a) Inspeções no local e supervisão *ex post* remota efetuadas por profissionais qualificados;

b) Auditorias de segurança direcionadas realizadas pela própria autoridade competente ou, quando tal se justifique, por uma entidade devidamente qualificada para o efeito que ofereça garantias de independência;

c) Auditorias *ad hoc*, designadamente com fundamento na verificação de incidente significativo, incumprimento de ordens, instruções e orientações da autoridade de cibersegurança competente ou infração ao presente decreto-lei por parte da entidade em causa;

d) Verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes, se necessário em cooperação com a entidade em causa;

e) Pedidos de informações necessários para avaliar o cumprimento das medidas de cibersegurança referidas nos artigos 27.º e seguintes, adotadas pela entidade em causa;

f) Pedidos de acesso a dados, documentos e quaisquer informações necessárias para o desempenho das suas funções de supervisão;

g) Pedidos de apresentação das provas demonstrativas da aplicação das políticas e procedimentos de cibersegurança.

3 - As auditorias direcionadas referidas na alínea b) do n.º 2 baseiam-se na análise de risco realizada pela autoridade de cibersegurança competente, na análise de risco realizada pela entidade auditada ou noutras informações disponíveis relacionadas

com os riscos, nomeadamente as constantes das instruções técnicas de harmonização e as matrizes de risco elaboradas pelo CNCS, nos termos do n.º 4 do artigo 26.º, bem como das ordens, instruções e orientações da autoridade de cibersegurança competente.

4 - Os custos das auditorias direcionadas referidas na alínea b) do n.º 2 são suportados pela entidade auditada, salvo decisão contrária fundamentada da autoridade de cibersegurança competente.

5 - Os pedidos de informação e de prova referidos nas alíneas e) a g) do n.º 2 devem indicar a respetiva finalidade, especificar a informação solicitada e fixar um prazo adequado e razoável para a entidade essencial lhes dar resposta.

Artigo 56.º

Medidas de execução

1 - A autoridade de cibersegurança competente pode, relativamente a entidades essenciais, importantes e públicas relevantes, adotar medidas que incluam o seguinte:

a) Advertências sobre infrações dos deveres decorrentes do presente decreto-lei e do respetivo regime regulamentar aplicável;

b) Ordens ou instruções vinculativas com vista à adoção de medidas necessárias para prevenir, impedir ou corrigir um incidente, determinando os prazos para a sua execução e respetiva informação;

c) Ordens ou instruções vinculativas com vista à correção de deficiências ou infrações ao presente decreto-lei;

d) Ordens ou instruções vinculativas com vista ao cumprimento do disposto no artigo 26.º e seguintes ou, quando se trate de uma entidade pública relevante, do disposto no artigo 33.º, ou ainda com vista ao cumprimento

Proposta de Lei n.º .....

do disposto nos artigos 40.º e seguintes;

e) Ordens para que as entidades em causa informem as pessoas singulares ou coletivas a quem prestam serviços ou que realizam atividades potencialmente afetadas por ciberameaça significativa da natureza desta, bem como de quaisquer medidas de proteção ou corretivas que possam ser adotadas em resposta a essa ciberameaça;

f) Ordens para que a entidade em causa aplique, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança;

g) Designação de um supervisor com funções adequadamente circunscritas, durante um período limitado, para supervisionar o cumprimento das obrigações previstas nos artigos 26.º e seguintes, e previstas nos artigos 40.º e seguintes, pela entidade em causa;

h) Ordens para que entidade em causa publicite os aspetos das infrações ao presente decreto-lei de uma forma específica;

i) Aplicação de coimas nos termos do capítulo seguinte.

2 - Em caso de incumprimento, por qualquer entidade essencial, das medidas referidas nas alíneas a) a d) e f) no prazo determinado pela autoridade de cibersegurança competente, esta pode, na medida do estritamente necessário:

a) Suspender uma certificação, autorização ou licença relativa a uma parte ou à totalidade dos serviços relevantes prestados ou das atividades realizadas pela entidade, ou ordenar a um organismo de certificação a sua suspensão;

b) Solicitar ao órgão competente a suspensão da autorização ou da licença relativa a uma parte ou à totalidade dos serviços relevantes prestados ou das atividades realizadas pela entidade;

3 - As suspensões ou inibições temporárias referidas no número anterior mantêm-se até

ao momento em que a entidade corrija as deficiências ou cumpra as medidas referidas no n.º 1.

4 - As medidas referidas no n.º 2 não se aplicam às entidades públicas abrangidas pelo presente decreto-lei, sem prejuízo do exercício dos poderes de direção e tutela, nos termos gerais.

Artigo 57.º

Medidas de bloqueio e redirecionamento

1 - A autoridade de cibersegurança competente pode emitir ordens ou instruções com vista a neutralizar uma ciberameaça, ciberataque ou incidente para as redes e sistemas de informação das entidades essenciais, importantes ou públicas relevantes que resulte da utilização abusiva de nomes de domínio ou endereço de protocolo IP, nos termos dos números seguintes.

2 - Os tipos de abusos referidos no número anterior incluem, designadamente:

a) Ataques de negação de serviço distribuída (DDoS);

b) Servidores maliciosos (Comando e Controlo);

c) Equipamentos infetados (comunicação com Comando e Controlo);

d) Distribuição de código malicioso;

e) Utilização ilegítima de nome de terceiros;

f) Correio eletrónico não solicitado (SPAM).

3 - Na medida do estritamente necessário para cessar a utilização abusiva de nomes de domínio, a autoridade de cibersegurança competente pode ordenar, de forma devidamente fundamentada:

a) Ao registo de nomes de TLD, que solicite ao titular de um registo de um

nome de domínio a adoção de medidas adequadas, dentro de um prazo determinado, para reprimir uma ciberameaça ou responder a um ciberataque ou a um incidente;

b) Ao registo de nomes de TLD ou aos prestadores de serviços de DNS, o bloqueio ou redireccionamento de nomes de domínio para um servidor seguro do CNCS, quando estes estejam manifestamente dedicados a ou envolvidos em ciberataques ou incidentes e não estejam disponíveis outros meios eficazes para fazer cessar o ciberataque ou incidente.

4 - Na medida do estritamente necessário para cessar a utilização abusiva de endereços de protocolo IP, o CNCS pode ordenar às empresas que oferecem redes e serviços de comunicações eletrónicas o bloqueio ou redireccionamento de endereço de protocolo IP, dinâmico ou estático, para um servidor seguro do CNCS, quando estes endereços estejam manifestamente dedicados ou envolvidos nos tipos de ciberataques ou incidentes previstos nas alíneas a) a d) do n.º 2.

5 - As medidas referidas nos n.ºs 3 e 4 não podem exceder o período de 60 dias, podendo este ser renovado por igual período quando haja forte probabilidade, aferida mediante uma avaliação fundamentada, de os ciberataques ou incidentes com origem nos mesmos endereços persistirem ou serem retomados.

6 - O disposto no presente artigo aplica-se igualmente aos prestadores de serviços de registo de nomes de domínio.

Artigo 58.º

Garantias procedimentais

1 - A autoridade de cibersegurança competente apresenta uma fundamentação adequada das suas decisões de aplicação das medidas de execução, devendo também, nos termos gerais, proceder à audiência prévia da entidade em causa dentro de um prazo

razoável, não inferior a 10 dias.

2 - Dispensa-se a audiência prévia referida no número anterior sempre que houver necessidade, devidamente fundamentada, de aplicação de medidas imediatas para prevenir ou responder a incidentes ou ciberameaças significativas.

3 - Ao aplicar qualquer uma das medidas de execução referidas nos números anteriores, a autoridade de cibersegurança competente deve respeitar as garantias procedimentais da entidade, atendendo às circunstâncias do caso concreto, e ponderar, designadamente:

a) A gravidade da infração e a importância das disposições violadas;

b) A duração da infração;

c) Quaisquer anteriores infrações relevantes cometidas pela entidade em causa:

d) Quaisquer danos materiais ou imateriais causados, incluindo quaisquer prejuízos financeiros ou económicos, os efeitos noutros serviços e o número de utilizadores afetados;

e) Quaisquer medidas tomadas pela entidade para prevenir ou atenuar os danos materais ou imaterais;

f) A culpa do agente;

g) O nível de cooperação das pessoas singulares ou coletivas responsáveis com a autoridade de cibersegurança competente.

4 - Para efeitos da alínea a) do número anterior, presumem-se graves:

a) Violações repetidas do presente decreto-lei;

b) Incumprimento do dever de notificação de incidentes nos termos dos artigos 40.º e seguintes;

c) Incumprimento do dever de correção de incidentes significativos;

d) Incumprimento do dever de correção de deficiências na sequência de instruções vinculativas da autoridade de cibersegurança competente;

e) Obstrução de auditorias ou atividades de acompanhamento ordenadas pela autoridade de cibersegurança competente, na sequência da verificação de uma infração ao presente decreto-lei;

f) Prestação de informações falsas ou grosseiramente inexatas em relação às medidas de cibersegurança previstas nos artigos 26.º e seguintes, ou das obrigações de notificação, previstas nos artigos 40.º e seguintes.

Secção II

Cooperação entre autoridades com competências de supervisão

Artigo 59.º

Comunicação de incidentes e aplicação de medidas

1 - As autoridades nacionais setoriais de cibersegurança e as autoridades nacionais especiais de cibersegurança informam o CNCS da ocorrência de incidentes ou ciberameaças significativas, bem como da aplicação de medidas de supervisão e de execução em matéria de cibersegurança, nos termos do regime aplicável.

2 - A aplicação das medidas de supervisão e de execução em matéria de cibersegurança, nos termos do regime aplicável, pelas autoridades nacionais setoriais de cibersegurança e pelas autoridades nacionais especiais de cibersegurança é precedida de parecer não vinculativo do CNCS, com exceção, para as autoridades nacionais setoriais de cibersegurança, das medidas previstas na alínea i) do n.º 1 do artigo 56.º.

3 - As autoridades nacionais setoriais de cibersegurança e as autoridades nacionais especiais de cibersegurança estão dispensadas de solicitar parecer ao CNCS nos termos do

número anterior, quando esteja em causa o cumprimento de medidas de execução num prazo inferior a 24h, sem prejuízo de as medidas serem imediatamente comunicadas ao CNCS.

4 - A autoridade de cibersegurança competente informa as autoridades nacionais especiais de cibersegurança dos incidentes significativos ocorridos que possam afetar as entidades do setor financeiro.

5 - A transmissão da informação acima referida deve ser realizada através da plataforma mencionada no n.º 7 do artigo 8.º.

Artigo 60.º

Cooperação no âmbito da segurança das infraestruturas críticas

1 - Sempre que o CNCS, as autoridades nacionais setoriais de cibersegurança ou as autoridades nacionais especiais de cibersegurança, consoante o caso, exerçam os seus poderes de supervisão relativamente a uma entidade referida no n.º 5 do artigo 3.º, devem informar as autoridades competentes que resultem da transposição da Diretiva (UE) 2022/2557, do Parlamento Europeu e o Conselho, de 14 de dezembro.

2 - As autoridades competentes que resultem da transposição da Diretiva (UE) 2022/2557, do Parlamento Europeu e o Conselho, de 14 de dezembro, podem, se for necessário, solicitar que o CNCS, as autoridades nacionais setoriais de cibersegurança ou as autoridades nacionais especiais de cibersegurança, consoante o caso, exerçam os seus poderes de supervisão, relativamente a uma entidade referida no n.º 5 do artigo 3.º.

Capítulo VII

Regime Sancionatório

.....

Proposta de Lei n.º .....

Artigo 61.º

Contraordenações muito graves

1 - Constituem contraordenações muito graves ao abrigo do presente decreto-lei:

a) O incumprimento das decisões do membro do Governo responsável pela área da cibersegurança, previstas no n.º 3 do artigo 18.º;

b) O incumprimento do dever de adoção das medidas de cibersegurança nos termos dos artigos 27.º a 29.º;

c) O incumprimento dos deveres previstos no artigo 30.º;

d) O incumprimento dos deveres previstos no artigo 31.º;

e) O incumprimento dos deveres previstos no artigo 32.º;

f) O incumprimento do dever de adoção das medidas de cibersegurança estabelecidas pelo CNCS nos termos do artigo 33.º;

g) O incumprimento dos deveres previstos no artigo 34.º;

h) O incumprimento dos deveres previstos nos n.ºs 1 e 2 do artigo 36.º;

i) O incumprimento dos deveres previstos no artigo 37.º;

j) O incumprimento do dever de notificação nos termos do artigo 40.º a 44.º;

k) O incumprimento do dever de comunicação nos termos do disposto no artigo 48.º;

2 - As contraordenações referidas no número anterior são punidas com as seguintes coimas:

a) Quando se trate de uma entidade essencial:

i) De €2 500,00 a €10 000 000,00 ou a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da entidade

{A139886346-9910-4EFC-B182-85FA24028071}

essencial em causa, consoante o montante que for mais elevado, se praticadas por uma pessoa coletiva;

ii) De €500,00 a €250 000,00, se praticadas por uma pessoa singular.

b) Quando se trate de uma entidade importante:

i) De €1 750,00 a €7 000 000,00 ou num montante máximo não inferior a 1,4 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da entidade importante em causa, consoante o montante que for mais elevado, se praticada por pessoa coletiva;

ii) De €500,00 a €250 000,00, se praticadas por uma pessoa singular.

c) Quando se trate de uma entidade pública relevante integrada no Grupo A previsto no n.º 2 do artigo 7.º:

i) De €20 000,00 a €5 000 000,00, se praticadas por pessoa coletiva;

ii) De €750,00 a €20 000,00, se praticadas por pessoa singular.

d) Quando se trate de uma entidade pública relevante integrada no Grupo B previsto no n.º 3 do artigo 7.º:

i) De €10 000,00 a €450 000,00, se praticadas por pessoa coletiva;

ii) De €750,00 a €20 000,00, se praticadas por pessoa singular.

Artigo 62.º

Contraordenações graves

1 - Constituem contraordenações graves ao abrigo do presente decreto-lei:

a) O incumprimento dos deveres previstos no artigo 8.º;

b) O incumprimento dos deveres previstos no artigo 35.º;

Proposta de Lei n.º .....

c) O incumprimento dos deveres previstos nos n.ºs 4 e 5 do artigo 36.º;

d) O incumprimento dos deveres previstos no artigo 46.º;

e) O incumprimento da obrigação prevista no n.º 2 do artigo 51.º;

f) O incumprimento da medida de execução imediata prevista no n.º 3 do artigo 52.º;

g) O incumprimento das advertências, ordens ou instruções vinculativas dadas pela autoridade de cibersegurança competente, ao abrigo das alíneas a) a g) do n.º 1 do artigo 56.º;

h) A violação da suspensão determinada ao abrigo do disposto na alínea a) do n.º 2 do artigo 56.º;

i) A violação da suspensão determinada ao abrigo do disposto na alínea b) do n.º 2 do artigo 56.º;

j) O incumprimento das ordens ou instruções previstas no artigo 57.º;

2 - As contraordenações referidas no número anterior são punidas com as seguintes coimas:

a) Quando se trate de uma entidade essencial:

i) De €1 250,00 a €5 000 000,00 ou a 1 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da entidade essencial em causa, consoante o montante que for mais elevado, se praticadas por uma pessoa coletiva;

ii) De €250,00 a €125 000,00, se praticadas por uma pessoa singular.

b) Quando se trate de uma entidade importante:

i) De €875,00 a €3 500 000,00 ou num montante máximo não inferior a 0,7 % do volume de negócios anual a nível mundial, no exercício

Proposta de Lei n.º .....

financeiro anterior, da entidade importante em causa, consoante o montante que for mais elevado, se praticada por pessoa coletiva;

ii) De €250,00 a €125 000,00, se praticadas por uma pessoa singular.

c) Quando se trate de uma entidade pública relevante integrada no «Grupo A» previsto no n.º 2 do artigo 7.º:

i) De €10 000,00 a €2 500 000,00, se praticadas por pessoa coletiva;

ii) De €375,00 a €10 000,00, se praticadas por pessoa singular.

d) Quando se trate de uma entidade pública relevante integrada no «Grupo B» previsto no n.º 3 do artigo 7.º:

i) De €5 000,00 a €225 000,00, se praticadas por pessoa coletiva;

ii) De €375,00 a €10 000,00, se praticadas por pessoa singular.

Artigo 63.º

Contraordenações leves

1 - São contraordenações leves:

a) A utilização, pelas entidades, de marca de certificação da cibersegurança inválida, caducada ou revogada;

b) A utilização de expressão ou grafismo que expressa ou tacitamente sugira a certificação da cibersegurança de produto, serviço ou processo que não seja certificado;

c) A omissão dolosa de informação ou a prestação de falsa informação que seja relevante para o processo de certificação da cibersegurança que se encontre em curso, nos termos definidos em cada esquema de certificação;

d) O incumprimento das solicitações da Comissão de Avaliação de Segurança do

Ciberespaço, previstas no n.º 8 do artigo 18.º;

2 - As contraordenações referidas no número anterior são punidas com as seguintes coimas:

a) De €875,00 a €45 000,00, se praticadas por uma pessoa coletiva;

b) De €250,00 a €3 750,00, se praticadas por uma pessoa singular.

Artigo 64.º

Negligência

As contraordenações referidas no n.º 1 do artigo 61.º, no n.º 1 do artigo 62.º e nas alíneas a) e b) do n.º 1 do artigo 63.º, são igualmente puníveis a título negligente, sendo os limites mínimos e máximos das coimas reduzidos a metade.

Artigo 65.º

Dispensa de aplicação das coimas

Todas as entidades essenciais, importantes e públicas relevantes podem, mediante pedido devidamente fundamentado, solicitar à autoridade de cibersegurança competente a dispensa da aplicação de coimas referidas no n.º 2 do artigo 61.º e no n.º 2 do artigo 62.º, com fundamento na inexistência de um procedimento interno de adaptação dessas entidades ao novo regime jurídico, durante 12 meses a contar da entrada em vigor do presente decreto-lei.

Artigo 66.º

Determinação da medida da coima

1 - A determinação da coima concreta faz-se em função da gravidade da ilicitude

concreta do facto, da culpa do agente, da sua situação económica e do benefício económico que este retirou da prática da contraordenação.

2 - Na determinação da ilicitude concreta do facto e da culpa do agente atende-se às seguintes circunstâncias:

a) A gravidade da infração,

b) A duração da infração;

c) O caráter ocasional ou reiterado da infração;

d) Os danos causados, incluindo quaisquer prejuízos financeiros ou económicos, os efeitos noutros serviços e o número de utilizadores afetados;

e) As medidas tomadas pela entidade para prevenir ou atenuar os danos referidos na alínea anterior;

f) O nível de cooperação das pessoas singulares ou coletivas responsáveis com a autoridade de cibersegurança competente.

3 - Para efeitos da alínea a) do número anterior, presumem-se graves:

a) As violações repetidas do presente decreto-lei;

b) A ausência de notificação de incidentes nos termos dos artigos 40.º e seguintes;

c) A ausência de correção de incidentes significativos;

d) A ausência de correção de deficiências na sequência de instruções vinculativas das autoridades competentes;

e) A obstrução de auditorias ou atividades de acompanhamento ordenadas pela autoridade de cibersegurança competente, na sequência da verificação de uma infração ao presente decreto-lei;

f) A prestação de informações falsas ou grosseiramente inexatas em relação às medidas de cibersegurança e deveres relativos às medidas de cibersegurança, nos

termos do disposto nos artigos 27.º e seguintes, ou das obrigações de notificação, nos termos do disposto nos artigos 40.º e seguintes.

4 - O disposto na alínea f) do número anterior não prejudica a responsabilidade nos termos do Código Penal.

5 - Exceto em caso de dolo, a instauração de processo de contraordenação depende de prévia advertência do agente, por parte da autoridade de cibersegurança competente, para cumprimento da obrigação omitida ou reintegração da proibição violada em prazo razoável.

Artigo 67.º

Sanções acessórias e outras determinações

Caso a gravidade da infração e a culpa do infrator o justifiquem, a autoridade de cibersegurança competente pode determinar, em simultâneo com a coima:

a) A publicação no Diário da República e num dos jornais de maior circulação nacional, regional ou local, consoante o mercado geográfico relevante, a expensas do infrator, de extrato da decisão de condenação ou, pelo menos, da parte decisória da decisão de condenação proferida no âmbito de um processo instaurado ao abrigo do presente decreto-lei, após o trânsito em julgado;

b) A proibição de participação em procedimentos de contratação pública, quando aplicável;

c) A adoção e execução de um plano de formação em cibersegurança, a executar no prazo de 6 meses;

d) A adoção ou alteração de um plano de segurança, a executar no prazo de 6 meses;

e) A suspensão da prestação do serviço até ao cumprimento dos deveres omitidos;

f) A interdição temporária dos titulares dos órgãos de gestão, direção e

administração, do exercício das respetivas funções.

Artigo 68.º

Sanções compulsórias

1 - Os destinatários de uma decisão da autoridade de cibersegurança competente ficam sujeitos ao pagamento de uma quantia pecuniária a pagar por cada dia de atraso no cumprimento, contado da data da respetiva notificação.

2 - Para efeitos do disposto no número anterior, considera-se sanção pecuniária compulsória a imposição ao agente do pagamento de uma quantia pecuniária por cada dia de incumprimento que se verifique para além do prazo fixado para o cumprimento da obrigação.

3 - A sanção pecuniária compulsória é fixada segundo critérios de razoabilidade e proporcionalidade, sendo o valor diário da sanção prevista no número anterior fixado em €500,00, quando cometida por pessoa coletiva, e em €100,00, quando cometida por pessoa singular.

4 - Os montantes diários fixados podem aumentar para cada dia de incumprimento, não podendo, em caso algum, ultrapassar a duração máxima de 30 dias.

Artigo 69.º

Prescrição do procedimento

1 - O procedimento pelas contraordenações graves e muito graves extingue-se por efeito da prescrição logo que sobre a prática da contraordenação haja decorrido o prazo de cinco anos, sem prejuízo das causas de interrupção e suspensão previstas nos termos gerais.

2 - O procedimento pelas contraordenações leves extingue-se por efeito da prescrição

logo que sobre a prática da contraordenação haja decorrido o prazo de três anos, sem prejuízo das causas de interrupção e suspensão previstas nos termos gerais.

Artigo 70.º

Prescrição da coima e sanções acessórias

1 - O prazo de prescrição da coima e sanções acessórias é de:

a) Três anos, no caso das contraordenações graves e muito graves;

b) Dois anos, no caso de contraordenações leves.

2 - O prazo conta-se a partir do carácter definitivo ou do trânsito em julgado da decisão condenatória.

Artigo 71.º

Regra da competência das autoridades competentes

A instauração e instrução dos processos de contraordenação, bem como a aplicação das coimas, é da competência da autoridade de cibersegurança competente.

Artigo 72.º

Notificações

1 - As notificações realizadas pelas autoridades de cibersegurança competentes são feitas por via eletrónica, ou, a pedido fundamentado da entidade, por carta registada ou pessoalmente.

2 - A notificação por via eletrónica faz-se por meio de disponibilização da mesma em área digital de acesso reservado ao destinatário, integrada na plataforma prevista no

n.º 7 do artigo 8.º e associada ao endereço de correio eletrónico nela registado pelo destinatário, e ainda, cumulativamente, através do serviço público de notificações eletrónicas (SPNE), sempre que se verifique que o destinatário a ele tenha aderido, nos termos do Decreto-Lei n.º 93/2017, de 1 de agosto, na sua redação atual.

3 - A disponibilização é acompanhada de envio de aviso ao destinatário para o endereço de correio eletrónico registado na plataforma prevista no n.º 7 do artigo 8.º, indicando-se a autoridade remetente e a forma de acesso à área reservada do destinatário.

4 - A notificação por via eletrónica considera-se feita na data da consulta eletrónica da área digital de acesso reservado da plataforma prevista no n.º 7 do artigo 8.º ou, se esta não ocorrer nos primeiros três dias a contar da receção, no termo desse prazo.

5 - A notificação postal presume-se feita no terceiro dia útil posterior ao do registo.

Artigo 73.º

Produto das coimas

O produto das coimas reverte em:

a) 60 % para o Estado;

b) 40 % para o CNCS ou para a autoridade nacional setorial de cibersegurança competente, consoante a entidade que tenha instaurado e instruído o processo.

Artigo 74.º

Custas

1 - Pelos processos de contraordenação são, ainda, devidas custas relativas aos encargos com a sua tramitação, arquivo e disponibilização.

.....

Proposta de Lei n.º .....

2 - As decisões da autoridade de cibersegurança competente sobre a matéria do processo devem fixar o montante das custas.

3 - As custas destinam-se a cobrir as despesas efetuadas no processo.

4 - O reembolso pelas despesas com notificações e comunicações, meios audiovisuais e materiais utilizados no processo é calculado:

a) Sendo o processo tramitado, total ou parcialmente, em papel, à razão de metade de 0,5 UC nas primeiras 50 folhas ou fração do processado e de um décimo de UC por cada conjunto subsequente de 25 folhas ou fração do processado, sem prejuízo do disposto nos números seguintes;

b) Sendo o processo tramitado, a título principal, de forma digital, até a um máximo de 5 UC, atendendo à complexidade do processo e atos praticados.

5 - As custas compreendem, ainda, os seguintes encargos:

a) A remuneração de peritos, tradutores, intérpretes e consultores técnicos;

b) O pagamento devido por deslocações ou pagamentos a qualquer entidade pelo custo de serviços técnicos, de certidões ou outros elementos de informação e de prova.

6 - Caso sejam facultadas cópias ou certidões do processo ou de partes deste, em suporte físico ou digital, a pedido do arguido, acresce ao valor referido nos números anteriores uma quantia calculada nos termos previstos nos mesmos números.

7 - As custas são suportadas pelo arguido e corresponsáveis nos termos do presente decreto-lei, em caso de aplicação de uma sanção de admoestação, de uma coima ou de uma sanção acessória.

8 - As custas revertem para o CNCS ou para a autoridade nacional setorial de cibersegurança, consoante a competência para a tramitação do processo de contraordenação.

.....

Proposta de Lei n.º .....

Artigo 75.º

Cumprimento de dever omitido

Sempre que a contraordenação resulte da omissão de um dever, a aplicação da sanção e o pagamento da coima não dispensam o infrator do seu cumprimento se este ainda for possível.

Artigo 76.º

Suspensão da execução da coima

1 - A autoridade de cibersegurança competente suspende a execução da coima aplicada, atendendo à natureza não reiterada da conduta ilícita do agente, às circunstâncias do cometimento da infração e à sua conduta anterior e posterior ao crime, sempre que conclua que a simples censura do facto, a sujeição a sanções acessórias e a ameaça de coima realizam de forma adequada e suficiente as finalidades preventivas e corretivas da sanção.

2 - A autoridade de cibersegurança competente, se julgar conveniente à realização das finalidades da punição, subordina a suspensão da execução da coima ao cumprimento das sanções e determinações previstas no artigo 67.º, ou de outros deveres que considere relevantes.

3 - A decisão condenatória especifica sempre os fundamentos da suspensão e das suas condições, incluindo o respetivo prazo de duração.

4 - O período de suspensão é fixado entre 1 e 3 anos a contar da notificação da decisão condenatória ou da decisão judicial transitada em julgado que dela conhecer.

Artigo 77.º

{A139886346-9910-4EFC-B182-85FA24028071}

.....

Proposta de Lei n.º .....

Revogação da suspensão da execução da coima

1 - Se, durante o período da suspensão, o condenado deixar de cumprir qualquer das sanções ou determinações previstas no artigo 67.º ou cometer uma contraordenação muito grave ou grave, a autoridade de cibersegurança competente, após o devido procedimento, revoga a decisão de suspensão da execução da coima.

2 - A revogação determina o dever de pagamento imediato da coima, sem que o arguido possa exigir a reparação de quaisquer prestações efetuadas ou despesas suportadas, durante o cumprimento anterior das sanções acessórias que lhe foram aplicadas.

Artigo 78.º

Extinção da coima

A coima é declarada extinta se, decorrido o período da sua suspensão, não houver motivos que possam conduzir à sua revogação.

Artigo 79.º

Violação de dados pessoais

1 - Sempre que a autoridade de cibersegurança competente obtiver um grau razoável de certeza, no decurso de uma ação de supervisão ou da imposição de medida de execução, de que a infração das obrigações estabelecidas nos artigos 27.º a 29.º e dos artigos 40.º a 43.º por parte de uma entidade essencial ou importante pode implicar uma violação de dados pessoais, nos termos do artigo 4.º, ponto 12, do RGPD, a qual deve ser notificada nos termos do artigo 33.º do mesmo RGPD, aquela autoridade deve, sem demora injustificada, informar a CNPD.

2 - No caso de a CNPD aplicar uma coima, nos termos do artigo 58.º, n.º 2, alínea i) do RGPD e restante direito nacional aplicável, a autoridade de cibersegurança

competente fica impedida de aplicar uma coima em resultado da prática da mesma infração nos termos do presente decreto-lei, sem prejuízo do disposto no número seguinte.

3 - A autoridade de cibersegurança competente pode impor as medidas de execução, previstas no artigo 56.º, n.º 1, alíneas a) a h), às entidades essenciais e importantes cuja violação das obrigações decorrentes do presente decreto-lei resulte num incidente de violação de dados pessoais.

Artigo 80.º

Impugnação das decisões da autoridade de cibersegurança competente

1 - Sem prejuízo do disposto no n.º 3, impugnada a decisão proferida pela autoridade de cibersegurança competente no âmbito de um processo de contraordenação, aquela remete os autos respetivos ao Ministério Público, preferencialmente por via eletrónica, no prazo de 20 dias úteis, podendo juntar alegações, bem como outros elementos ou informações que considere relevantes para a decisão da causa, e ainda oferecer meios de prova.

2 - A remessa dos autos por via eletrónica dispensa o envio dos respetivos originais, sem prejuízo do dever de exibição das peças processuais em suporte de papel e dos originais dos documentos dele constantes, quando existentes, sempre que o Ministério Público ou o juiz o determine.

3 - As decisões ou quaisquer medidas adotadas e aplicadas pela autoridade de cibersegurança competente no âmbito de processos de contraordenação são impugnáveis para os tribunais judiciais, devendo o recurso ser apresentado à autoridade de cibersegurança competente.

4 - A impugnação de quaisquer decisões proferidas pela autoridade de cibersegurança competente que, no âmbito de processos de contraordenação, determinem a

Proposta de Lei n.º .....

aplicação de coimas ou de sanções acessórias tem efeito suspensivo.

5 - A impugnação das demais decisões ou medidas da autoridade de cibersegurança competente, incluindo as decisões de aplicação de sanções pecuniárias compulsórias, adotados no âmbito de processos de contraordenação, tem efeito meramente devolutivo e obedece às regras previstas no presente artigo.

6 - A autoridade de cibersegurança competente, o Ministério Público e os arguidos podem opor-se a que o tribunal decida por despacho, sem audiência de julgamento.

7 - Em sede de recurso de decisão proferida em processo de contraordenação, a desistência da acusação pelo Ministério Público depende da concordância da autoridade de cibersegurança competente.

8 - A autoridade de cibersegurança competente tem legitimidade para recorrer autonomamente de quaisquer sentenças e despachos que não sejam de mero expediente, incluindo os que versem sobre nulidades e outras questões prévias ou incidentais, ou sobre a aplicação de medidas cautelares, bem como para responder a recursos interpostos.

9 - As decisões dos tribunais judiciais que admitam recurso, nos termos previstos no regime do ilícito de mera ordenação social, aprovado pelo Decreto-Lei n.º 433/82, de 27 de outubro, na sua redação atual, são impugnáveis junto do Tribunal da Relação de Lisboa.

10 - O Tribunal da Relação, no âmbito da competência prevista no número anterior, decide em última instância, não cabendo recurso ordinário dos seus acórdãos.

Artigo 81.º

Direito Subsidiário

Em matéria contraordenacional, em tudo que não estiver previsto do presente decreto-lei,

aplica-se, subsidiariamente, o disposto no regime do ilícito de mera ordenação social, aprovado pelo Decreto-Lei n.º 433/82, de 27 de outubro, na sua redação atual.

Capítulo VIII

Disposições complementares

Secção I

Outras disposições

Artigo 82.º

Taxa de supervisão

1 - Pode ser cobrada às entidades essenciais e importantes uma taxa de supervisão por contrapartida dos atos de supervisão praticados, a fixar em função dos custos necessários à prestação de serviços de supervisão.

2 - As taxas de supervisão obedecem ao princípio da proporcionalidade e são fixadas de acordo com critérios objetivos e transparentes.

3 - O regime que regula as taxas referidas nos números anteriores é fixado por portaria dos membros do Governo responsáveis pelas áreas das finanças e da cibersegurança.

Artigo 83.º

Comunicações

1 - As comunicações entre as entidades com o CNCS, ou com as autoridades nacionais setoriais de cibersegurança referidas na alínea a) do n.º 2 no 15.º, incluindo as

notificações de incidentes nos termos dos artigos 40.º e seguintes, devem seguir o formato e o procedimento definido pelo CNCS em regulamento a aprovar pelo CNCS.

2 - Na ausência de disposição regulamentar aplicável, todas as comunicações dirigidas à autoridade de cibersegurança competente, no âmbito do presente decreto-lei, bem como o envio de informação, devem ser realizadas por meios eletrónicos.

3 - Nos casos em que a entidade não tenha temporariamente capacidade operacional para assegurar a comunicação prevista nos números anteriores, ou nos casos em que o sítio na *Internet* da autoridade de cibersegurança competente, esteja indisponível, em resultado do incidente ou por outro motivo de natureza eminentemente técnica devidamente justificado, a notificação pode ser efetuada, a título excecional, através de correio eletrónico ou telefonicamente.

4 - O formato e procedimento referido no n.º 1 é adotado pelo CNCS, mediante prévia audição das autoridades nacionais setoriais de cibersegurança competentes, que também podem adotar formatos e procedimentos próprios, adaptados às suas especificidades, conforme referido no n.º 1.

5 - Os casos referidos no n.º 3 são objeto de instruções técnicas do CNCS, adotadas em articulação com as autoridades nacionais setoriais de cibersegurança.

Artigo 84.º

Segurança e integridade da informação

1 - O CNCS e as autoridades nacionais setoriais de cibersegurança competentes nos termos do disposto na alínea a) do n.º 2 no artigo 15.º mantêm e gerem a informação em matéria de segurança e integridade num sistema de informação seguro, em conformidade com as disposições respeitantes à segurança de informação classificada no âmbito nacional e no âmbito das organizações internacionais de que Portugal é

parte.

2 - O acesso aos sistemas eletrónicos e sítios de *Internet* para tratamento das notificações previstas no presente decreto-lei deve ser efetuado preferencialmente com recurso a sistema de identificação eletrónico com nível de garantia elevado, nos termos definidos pelos artigos 8.º e 9.º do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho, relativo à identificação eletrónica e aos serviços de confiança, designadamente através do Cartão de Cidadão e da Chave Móvel Digital, conforme alterado pela Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro, e pelo Regulamento (UE) n.º 2024/1183, do Parlamento Europeu e do Conselho, de 11 de abril.

Capítulo IX

Disposições finais

Artigo 85.º

Aprovação do plano nacional de resposta a crises e incidentes de cibersegurança em grande escala

O plano referido no artigo 13.º é aprovado no prazo de 6 meses após a entrada em vigor do presente decreto-lei.

Artigo 86.º

Dotação de meios e independência operacional do CNCS

Por forma a prosseguir atribuições e a exercer as competências previstas no presente decreto-lei, o CNCS deverá ser dotado dos meios necessários e beneficia de independência operacional em relação às entidades supervisionadas.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

Artigo 87.º

Interoperabilidade e acesso a informação

1 - O CNCS acede gratuitamente às bases de dados e registos nacionais relevantes para a concretização das atribuições e exercício das competências previstas no presente decreto-lei e demais legislação em matéria de cibersegurança, em especial para a atribuição ou confirmação da qualificação das entidades.

2 - As entidades públicas responsáveis pelas bases de dados e registos nacionais previstos no número anterior disponibilizam o acesso às mesmas, mediante uma solução de interoperabilidade estipulada em protocolo e adequada para o efeito.

3 - A falta de assinatura dos protocolos referidos no número anterior não obsta ao acesso às informações relevantes pelo CNCS, devendo as entidades públicas responsáveis pelas bases de dados e registos nacionais prestar todas as informações necessárias sempre que solicitadas pelo CNCS.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

ANEXO I

(a que se refere os artigos 3.º, 6.º, 12.º e 35.º)

Setores de importância crítica

Setor	Subsetor	Tipo de entidade
1. Energia	a) Eletricidade	Empresas de eletricidade na aceção do artigo 2.º, ponto 57, da Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho, que exercem a atividade de «comercialização» na aceção do artigo 2.º, ponto 12, da mesma diretiva
		Operadores da rede de distribuição na aceção do artigo 2.º, ponto 29, da Diretiva (UE) 2019/944
		Operadores da rede de transporte na aceção do artigo 2.º, ponto 35, da Diretiva (UE) 2019/944
		Produtores na aceção do artigo 2.º,

.....

Proposta de Lei n.º .....

		ponto 38, da Diretiva (UE) 2019/944
		Operadores nomeados do mercado da eletricidade na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho
		Participantes no mercado na aceção do artigo 2.º, ponto 25, do Regulamento (UE) 2019/943, que prestam serviços de agregação, resposta da procura ou armazenamento de energia na aceção do artigo 2.º, pontos 18, 20 e 59, da Diretiva (UE) 2019/944
		Os operadores de um ponto de carregamento que são responsáveis pela gestão e operação

		de um ponto de carregamento que presta um serviço de carregamento aos utilizadores finais, incluindo em nome e por conta de um prestador de serviços de mobilidade
	b) Sistemas de aquecimento e arrefecimento urbano	Operadores de sistemas de aquecimento urbano ou sistemas de arrefecimento urbano na aceção do artigo 2.º, ponto 19, da Diretiva (UE) 2018/2001 do Parlamento Europeu e do Conselho
	c) Petróleo	Operadores de oleodutos de petróleo
		Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo
		Entidades centrais de armazenagem na aceção do artigo 2.º, alínea f), da Diretiva

.....

Proposta de Lei n.º .....

		2009/119/CE do Conselho
	c) Gás	Empresas de comercialização na aceção do artigo 2.º, ponto 8, da Diretiva 2009/73/CE do Parlamento Europeu e do Conselho
		Operadores da rede de distribuição na aceção do artigo 2.º, ponto 6, da Diretiva 2009/73/CE
		Operadores da rede de transporte na aceção do artigo 2.º, ponto 4, da Diretiva 2009/73/CE
		Operadores do sistema de armazenamento na aceção do artigo 2.º, ponto 10, da Diretiva 2009/73/CE
		Operadores da rede de GNL na aceção do artigo 2.º, ponto 12, da Diretiva 2009/73/CE

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

		Empresas de gás natural na aceção do artigo 2.º, ponto 1, da Diretiva 2009/73/CE
		Operadores de instalações de refinamento e tratamento de gás natural
	e) Hidrogénio	Operadores de produção, armazenamento e transporte de hidrogénio
2. Transportes	a) Transporte aéreo	Transportadoras aéreas na aceção do artigo 3.º, ponto 4, do Regulamento (CE) n.o 300/2008 utilizadas para fins comerciais
		Entidades gestoras aeroportuárias na aceção do artigo 2.º, ponto 2, da Diretiva 2009/12/CE do Parlamento Europeu e do Conselho, aeroportos na aceção do artigo 2.º, ponto 1 da mesma diretiva, incluindo os aeroportos principais enumerados

.....

Proposta de Lei n.º .....

		no anexo II, secção 2, do Regulamento (UE) n.º 1315/2013 do Parlamento Europeu e do Conselho, e as entidades que exploram instalações auxiliares existentes dentro dos aeroportos
		Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo (CTA) na aceção do artigo 2.º, ponto 1, do Regulamento (CE) n.º 549/2004 do Parlamento Europeu e do Conselho
	b) Transporte ferroviário	Gestores de infraestrutura na aceção do artigo 3.º, ponto 2, da Diretiva 2012/34/UE do Parlamento Europeu e do Conselho
		Empresas ferroviárias na aceção do artigo 3.º, ponto 1, da Diretiva 2012/34/UE,

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

		incluindo os operadores das instalações de serviço na aceção do artigo 3.º, ponto 12, dessa diretiva
	c) Transporte aquático	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, tal como definidas para o transporte marítimo no anexo I do Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho, não incluindo os navios explorados por essas companhias
		Entidades gestoras dos portos na aceção do artigo 3.º, ponto 1, da Diretiva 2005/65/CE do Parlamento Europeu e do Conselho, incluindo as respetivas instalações portuárias na

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

		aceção do artigo 2.º, ponto 11, do Regulamento (CE) n.º 725/2004, e as entidades que gerem as obras e o equipamento existentes dentro dos portos
		Operadores de serviços de tráfego marítimo (VTS, do inglês, vessel traffic services) na aceção do artigo 3.º, alínea o), da Diretiva 2002/59/CE do Parlamento Europeu e do Conselho
	d) Transporte rodoviário	Autoridades rodoviárias na aceção do artigo 2.º, ponto 12, do Regulamento Delegado (UE) 2015/962 da Comissão, responsáveis pelo controlo da gestão do tráfego, com exceção das entidades públicas nas quais a gestão do

.....

Proposta de Lei n.º .....

		tráfego ou a gestão de sistemas de transporte inteligentes constituem uma parte não essencial da sua atividade geral
		Operadores de sistemas de transporte inteligentes na aceção do artigo 4.º, ponto 1, da Diretiva 2010/40/UE do Parlamento Europeu e do Conselho
3. Setor bancário		Instituições de crédito, tal como definidas no artigo 4.º, ponto 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho
4. Infraestruturas do mercado financeiro		Operadores de plataformas de negociação na aceção do artigo 4.º, ponto 24, da Diretiva 2014/65/UE do Parlamento Europeu e do Conselho
		Contrapartes centrais (CCP) na aceção

.....

Proposta de Lei n.º .....

		do artigo 2.º, ponto 1, do Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho
5. Saúde		Prestadores de cuidados de saúde na aceção do artigo 3.º, alínea g), da Diretiva 2011/24/UE do Parlamento Europeu e do Conselho
		Laboratórios de referência da UE referidas no artigo 15.º do Regulamento (UE) 2022/2371 do Parlamento Europeu e do Conselho
		Entidades que realizam atividades de investigação e desenvolvimento de medicamentos na aceção do artigo 1.º, ponto 2, da Diretiva 2001/83/ CE do Parlamento Europeu e do Conselho
6. Água potável		Fornecedores e distribuidores de água

		destinada ao consumo humano na aceção do artigo 2.º, ponto 1, alínea a), da Diretiva (UE) 2020/2184 do Parlamento Europeu e do Conselho, excluindo os distribuidores para os quais a distribuição de água para consumo humano constitui uma parte não essencial da sua atividade geral de distribuição de outros produtos de base e mercadorias
7. Águas residuais		Empresas que recolhem, eliminam ou tratam águas residuais urbanas, domésticas ou industriais na aceção do artigo 2.º, pontos 1, 2 e 3, da Diretiva 91/271/CEE do Conselho, excluindo as empresas para as quais a recolha,

.....

Proposta de Lei n.º .....

		eliminação ou tratamento de águas residuais urbanas, domésticas ou industriais constitui uma parte não essencial da sua atividade geral
8. Infraestruturas digitais		Fornecedores de pontos de troca de tráfego
		Prestadores de serviços de DNS, excluindo operadores de servidores de nomes raiz
		Registos de nomes de TLD
		Prestadores de serviços de computação em nuvem
		Prestadores de serviços de centro de dados
		Fornecedores de redes de distribuição de conteúdos
		Prestadores de serviços de confiança
		Fornecedores de redes públicas de comunicações eletrónicas
		Prestadores de serviços de

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

		comunicações eletrónicas acessíveis ao público
9. Gestão de serviços TIC (entre empresas)		Prestadores de serviços geridos
		Prestadores de serviços de segurança geridos
10. Espaço		Operadores de infraestruturas terrestres, detidas, geridas e operadas por Estados-Membros ou entidades privadas, que apoiam a prestação de serviços espaciais, excluindo os fornecedores de redes públicas de comunicações eletrónicas

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

ANEXO II

(a que se refere os artigos 3.º, 6.º, 12.º e 35.º)

Outros setores críticos

Setor	Subsetor	Tipo de entidade
1. Serviços postais e de estafeta		Prestadores de serviços postais na aceção da Lei n.º 17/2012, de 26 de abril, na sua redação atual, incluindo prestadores de serviços de estafeta
2. Gestão de resíduos		Empresas que realizam a gestão de resíduos na aceção do artigo 3.º, ponto 9, da Diretiva 2008/98/CE do Parlamento Europeu e do Conselho, mas excluindo as empresas para as quais a gestão de resíduos não constitui a atividade económica principal
3. Produção, fabrico e distribuição de produtos químicos		Empresas que realizam a produção de substâncias e a distribuição de substâncias ou misturas, referidas no artigo 3.º, pontos 9 e 14, do Regulamento (CE) n.º 1907/2006 do Parlamento Europeu e do Conselho e empresas que realizam a produção de «artigos» na aceção do artigo 3.º, ponto 3, do

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

		mesmo regulamento, de substâncias ou misturas
4. Produção, transformação e distribuição de produtos alimentares		Empresas do setor alimentar, na aceção do artigo 3.º, ponto 2, do Regulamento (CE) n.º 178/2002 do Parlamento Europeu e do Conselho, que se dedicam à distribuição por grosso e à produção e transformação industriais
5. Indústria transformadora	a) Fabrico de dispositivos médicos e dispositivos médicos para diagnóstico in vitro	Entidades que fabricam dispositivos médicos na aceção do artigo 2.º, ponto 1, do Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, e entidades que fabricam dispositivos médicos para diagnóstico in vitro na aceção do artigo 2.º, ponto 2, do Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, com exceção das entidades que fabricam dispositivos médicos referidas no anexo I, ponto 5, quinto travessão, da presente diretiva
	b) Fabricação de equipamentos informáticos, equipamentos	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 26, da NACE Rev. 2

.....

Proposta de Lei n.º .....

	para comunicação, produtos eletrónicos e óticos	
	c) Fabricação de equipamento elétrico	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 27, da NACE Rev. 2
	d) Fabricação de máquinas e equipamentos (não especificados)	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 28, da NACE Rev. 2
	e) Fabricação de veículos automóveis, reboques e semirreboques	Empresas que exercem qualquer uma das atividades económicas referidas na secção C, divisão 29, da NACE Rev. 2
	f) Fabricação de outro	Empresas que exercem qualquer uma das atividades

.....

Proposta de Lei n.º .....

	equipamento de transporte	económicas referidas na secção C, divisão 30, da NACE Rev. 2
6. Prestação de serviços digitais		Prestadores de serviço de mercados em linha
		Prestadores de serviço de motores de pesquisa em linha
		Prestadores de serviço de plataformas de serviços de redes sociais
7. Investigação		Organismos de investigação

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....

ANEXO III

(a que se refere os artigos 3.º, 6.º, 7.º e 12.º)

Artigo 1º.

Empresa

Entende-se por empresa qualquer entidade que, independentemente da sua forma jurídica, exerce uma atividade económica. São, nomeadamente, consideradas como tal as entidades que exercem uma atividade artesanal ou outras atividades a título individual ou familiar, as sociedades de pessoas ou as associações que exercem regularmente uma atividade económica.

Artigo 2º.

Categorias

1 - A categoria das micro, pequenas e médias empresas (PME) é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros.

2 - Na categoria das PME, uma pequena empresa é definida como uma empresa que emprega menos de 50 pessoas e cujo volume de negócios anual ou balanço total anual não excede 10 milhões de euros.

3 - Na categoria das PME, uma microempresa é definida como uma empresa que emprega menos de 10 pessoas e cujo volume de negócios anual ou balanço total anual não excede 2 milhões de euros.

PRESIDÊNCIA DO CONSELHO DE MINISTROS

.....

Proposta de Lei n.º .....