NOVO ARTIGO 8º-A DA LEI DO CIBERCRIME

Nota Prática nº 32/2026

16 de setembro de 2026

ÍNDICE

NOTA PRÁTICA nº 32/2026
16 de setembro de 2026

O NOVO ARTIGO 8º-A DA LEI DO CIBERCRIME

Esta Nota Prática tem como propósito ser um auxiliar dos magistrados do Ministério Público na interpretação da alteração, operada em dezembro de 2025, à Lei Cibercrime, com a introdução de um novo artigo 8º-A (“atos não puníveis por interesse público de cibersegurança”).

A – A ALTERAÇÃO À LEI DO CIBERCRIME

1. A Lei do Cibercrime (Lei nº 109/2009, de 15 de setembro) sofreu uma pequena, mas muito significativa, alteração legislativa no final do ano de 2025, por via do Decreto-Lei nº 125/2025, de 4 de dezembro, que aprovou o regime jurídico da cibersegurança.
O objeto principal deste diploma foi o de rever o quadro normativo em matéria de segurança nacional e internacional, no funcionamento do Estado e dos agentes económicos, transpondo para o direito interno a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022.

2. Porém, além disso, lateralmente, também introduziu um novo artigo 8º-A à Lei do Cibercrime. Esta nova norma determina a não punição de factos suscetíveis de consubstanciar os crimes de acesso ilegítimo e de interceção ilegítima, por razões de interesse público de cibersegurança, se verificadas algumas circunstâncias específicas.
Este novo quadro legal entrou em vigor 120 dias após a sua publicação, a 4 de abril de 2026 (artigo 11º do Decreto-Lei nº 125/2025).

3. O novo regime jurídico da cibersegurança determina também (alínea h) do nº 1 do artigo 20º) que o Centro Nacional de Cibersegurança emita “*ordens, orientações, recomendações e instruções técnicas em matéria de divulgação coordenada de vulnerabilidades*”, que permitam tornar operativo o mecanismo de isenção de responsabilidade do novo artigo 8º-A.
Em cumprimento desta determinação legal, o Centro Nacional de Cibersegurança aprovou, a 24 de junho de 2026, a Instrução Técnica nº 1/2026[1] (*Divulgação Coordenada de Vulnerabilidades*).

4. Em termos gerais, pode dizer-se que este novo regime legal isenta de responsabilidade penal os chamados *white hat hackers*, também conhecidos como *hackers éticos*. Sob a epígrafe “atos não puníveis por interesse público de cibersegurança”, o novo Artigo 8º-A introduz uma exceção à

[1] https://www.cncs.gov.pt/docs/1782487642.pdf

incriminação de factos ou ações que, se esta norma não existisse, fariam incorrer os seus autores em responsabilidade criminal. Estão abrangidos por este regime os factos constitutivos dos tipos de crimes de acesso ilegítimo e de interceção ilegítima previstos nos artigos 6º e 7º da Lei do Cibercrime.
O propósito deste regime de exceção é o de isentar de responsabilidade penal os especialistas em segurança informática que se dediquem à procura de falhas ou de vulnerabilidades de segurança em sistemas informáticos. Portanto, este regime protege quem se dedica a este tipo de investigação com o intuito de corrigir debilidades de segurança, assim contribuindo para tornar os sistemas mais seguros. Por ser de exceção, vem acompanhado de um conjunto de regras de procedimento e dos limites jurídicos que mais abaixo se descreverão. Entre eles, é por exemplo instituída a obrigação de rápida comunicação das vulnerabilidades descobertas, designadamente ao proprietário do sistema informático em causa e ao Centro Nacional de Cibersegurança.
Esta atividade de identificação ou descoberta de vulnerabilidades é extremamente importante na perspetiva da segurança digital, uma vez que permite identificar possíveis falhas antes que os agentes criminosos as explorem. É essa a razão última desta opção legislativa, que já ocorreu também noutros países europeus.

B – O CONTEXTO LEGAL

5. É vulnerabilidade a "*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*". Este conceito resulta da alínea h) do artigo 2º da Lei do Cibercrime, na nova redação, também introduzida pelo Decreto-Lei nº 125/2025.
Como se referiu, o artigo 8º-A foi introduzido no tecido legal por via de uma iniciativa legislativa de âmbito muito mais vasto, que redefiniu o quadro normativo da cibersegurança. Esta nova norma, de natureza penal, é uma das peças da nova estratégia jurídica da cibersegurança, que privilegia a prevenção e, dentro dela, a identificação e divulgação coordenada de vulnerabilidades em sistemas informáticos.

6. Ao encontro desta estratégia, a lei conferiu ao Centro Nacional de Cibersegurança novas responsabilidades em matéria de *divulgação coordenada de vulnerabilidades*. Assim, o artigo 20º do novo regime da cibersegurança conferiu ao CNCS competência para "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" (alínea i) do nº 1). Por outro lado, a lei acomete ao «CERT.PT», equipa de resposta a incidentes de cibersegurança nacional, integrada no CNCS, ser 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" (artigo 38º, nº 1).
Neste quadro, é natural que a lei confira ao CNCS a tarefa de "emitir ordens, orientações, recomendações e instruções técnicas" nesta matéria (alínea h do nº 1 do artigo 20º), da mesma forma que confere ao «CERT.PT» diversas funções operativas no processo de identificação, notificação e divulgação de vulnerabilidades.

C – A NÃO PUNIBILIDADE DE FACTOS SUSCETÍVEIS DE CONSUBSTANCIAR CRIME

7. No regime jurídico-penal português punem-se como crimes os atos típicos que igualmente sejam ilícitos, culposos e puníveis. Por outro lado, não existe responsabilidade penal caso se verifiquem causas de exclusão da ilicitude, causas de exclusão da culpa ou causas de exclusão da punibilidade.
O novo artigo 8º-A da Lei do Cibercrime introduziu uma nova causa de exclusão da responsabilidade penal desta última categoria. Portanto, reconhecendo que eventuais factos possam preencher tipos de crime e sejam ilícitos e culposos, determina que tais factos não sejam puníveis.

8. Como consideração liminar, importa delimitar o âmbito de aplicação deste regime de exceção: aplica-se somente a factos que possam consubstanciar dois dos vários tipos de crimes previstos na Lei do Cibercrime, o crime de acesso ilegítimo (previsto no artigo 6º) e o crime de interceção ilegítima (previsto no artigo 7º).
Depois, para que este novo regime se aplique, tem que verificar-se, no caso concreto, um complexo conjunto de condições, designadamente decorrentes da própria atuação do agente do crime. Importa sublinhar que todas estas condições requeridas pela lei são cumulativas. Isto é, por força do nº 1 do artigo 8º-A da Lei do Cibercrime o atuação do agente tem que preencher todas elas, sob pena de, não o fazendo, não poder beneficiar da exclusão da punibilidade.

D – AS CIRCUNSTÂNCIAS REQUERIDAS

9. O primeiro dos requisitos legais (descrito na alínea a) do nº1) respeita ao intuito de quem descobre as vulnerabilidades: o agente que as descobre e divulga tem que ser exclusivamente movido pela intenção de identificar a existência de vulnerabilidades, como o fim de, por via da respetiva divulgação, contribuir para a segurança do ciberespaço.
Porém, este regime de exceção não se aplicará se as vulnerabilidades em causa tiverem sido criadas pelo agente.

10. O segundo requisito (alínea b)) é o do altruísmo do agente na ação: isto é, exige-se que o agente não vise qualquer vantagem ao descobrir a vulnerabilidade. Com esta exigência pretendem excluir-se da aplicação deste regime de exceção os chamados *caçadores de recompensas* (ou "*bug bounties*") que, à revelia dos proprietários dos sistemas, procuram falhas nos mesmos.
Note-se que não está aqui em causa a situação em que o agente atua em conformidade ou a pedido do dono do sistema, por exemplo, porque foi contratado por ele para esse mesmo efeito, de verificação de segurança, mesmo sendo pago por este serviço. Neste tipo de situação não se preencherão os elementos objetivos dos tipos de crime em causa (que são crimes dolosos). Não estando preenchidos os elementos do tipo nem se colocará, desde logo liminarmente, a questão da exclusão da punibilidade.
Aliás, isto mesmo é afirmado pelo nº 5 do artigo 8º-A, de forma talvez desnecessária.
Não obstante, esta norma acaba por ter uma finalidade útil, já que contém uma imposição legal adicional. Nos seus termos, também é aplicável a quem seja contratado pelo dono de um sistema para identificar vulnerabilidades a obrigação de comunicar as mesmas ao Centro Nacional de Cibersegurança, se de facto forem efetivamente identificadas vulnerabilidades.

11. Esta comunicação de descoberta da vulnerabilidade é uma das mais importantes circunstâncias exigidas para que opere a não punição: exige a alínea c) do nº 1 do artigo 8º-A que o agente comunique a identificação das vulnerabilidades "*imediatamente após a ação*".
Tal comunicação deve ser primordialmente efetuada ao proprietário do sistema de informação (ou a pessoa por ele designada para o gerir). O mesmo sucede se a vulnerabilidade respeitar a um produto (por exemplo *software*) ou a um serviço das tecnologias de informação e comunicação (por exemplo uma rede social, ou um serviço de *webmail*), cujo proprietário deve igualmente ser informado.
Caso a vulnerabilidade permita o acesso a dados pessoais, deve ainda ser feita a comunicação da mesma ao titular desses dados.
Por último (em resultado da imposição do nº 2 do artigo 8º-A), a vulnerabilidade tem também sempre que ser comunicada ao Centro Nacional de Cibersegurança.

12. Do nº 4 do artigo 8º-A resulta uma regra prática importante, relacionada com esta comunicação: todo o processo que a envolve deve ser secreto, de forma a permitir ao dono do sistema que corrija, de forma recatada e atempada, a vulnerabilidade identificada, minorando assim o seu efeito. Mas por outro lado, esta norma impõe também a obrigação de que todos os dados (informáticos) que sejam objeto de comunicação sejam eliminados, após a vulnerabilidade ser corrigida pelo dono do sistema. Anote-se, porém, que estas concretas regras de procedimento foram deixadas pelo legislador de fora do conjunto de requisitos exigidos para a exclusão da punibilidade do agente.

13. Para que opere a exclusão da punibilidade, é ainda requerido que o agente atue com proporcionalidade. Isto é, a sua concreta atuação tem que ser proporcional aos seus propósitos e limitada pelos mesmos. Daqui decorre que o agente não pode praticar atos que vão para além daqueles que sejam estritamente necessários à identificação das vulnerabilidades.
Além desta limitação, decorrente da alínea d) do nº 1 do artigo 8º-A, o nº 3 do mesmo artigo aponta critérios para aferir a proporcionalidade da conduta do agente: que esta tenha sido necessária à deteção da vulnerabilidade, por um lado; por outro, que a extensão dos sistemas ou dados informáticos acedidos, consultados e/ou copiados fosse imposta pelo interesse em contribuir para a segurança do ciberespaço.

14. Concretizando atuações que ficam de fora da esfera da proporcionalidade, quer a alínea d)[2] do nº 1 do artigo 8º-A, quer o nº 3[3] do artigo 8º-A, descrevem algumas das modalidades de ação que

[2] i) perturbar ou interromper o funcionamento do sistema ou serviço;
ii) eliminar ou deteriorar dados informáticos ou copiar os mesmos sem autorização;
iii) produzir um 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, os que resultariam da própria vulnerabilidade detetada ou da sua exploração.
[3] 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 ao sistema de informação;
g) instalação e distribuição de software malicioso.

expressamente são proibidas a quem queira beneficiar deste estatuto de exclusão da punibilidade. Afigura-se que estes exemplos detalhadamente descritos pelo texto legal, embora pedagógicos, são pouco úteis e nada acrescentam ao juízo que o julgador terá que fazer a este respeito: é que as atividades proibidas, de uma forma ou outra, acabam por se enquadrar noutros tipos de ilícito da Lei do Cibercrime (designadamente no dano informático, na sabotagem informática ou na falsidade informática), os quais não são suscetíveis de beneficiar da exclusão da punibilidade.

É também expressamente proibido (alínea e) do artigo 8º-A, nº 1) que o agente, com a sua atuação "consubstancie violação de dados pessoais protegidos ao abrigo da legislação aplicável em matéria de proteção de dados pessoais". Esta proibição não está especificamente densificada, não se alcançando se pretende ir mais além do regime geral de proteção de dados – sendo certo que este artigo 8º-A apenas permite a exclusão da punibilidade quanto a dois dos crimes previstos na Lei do Cibercrime e não quanto aos ilícitos criminais da área da proteção de dados pessoais.

E – A INSTRUÇÃO TÉCNICA DO CENTRO NACIONAL DE CIBERSEGURANÇA

15. Uma última nota para referir a Instrução Técnica nº 1/2026 do Centro Nacional de Cibersegurança sobre divulgação coordenada de vulnerabilidades. Trata-se de uma fonte normativa infra legal, de natureza técnica, que não colide com a interpretação do artigo 8º-A.

É seu propósito criar regras e definir os procedimentos daqueles que se dediquem à identificação de vulnerabilidades: via, forma da comunicação e conteúdo da mesma, obrigações dos "donos" dos sistemas e das entidades públicas com responsabilidade nesta matéria, entre outras.

A observação destas regras técnicas, de natureza prática, será apenas um indicador quanto ao resto da factualidade a apurar, no momento da determinação desta causa de exclusão da punibilidade.

Uma das normas relevantes a este respeito será porventura a do artigo 5º da Instrução Técnica, que, identificando a obrigação de comunicação imediata da vulnerabilidade, também refere que, aquele que a identificar, deve "fornecer todos os elementos e informações relevantes relativas à vulnerabilidade identificada" (alínea b) do nº 1) e, além disso, "cumprir com o prazo previamente definido e/ou acordado, antes de tornar pública a vulnerabilidade" (alínea c) do nº 1).

F – QUADRO DE SÍNTESE

<table>
<tr><td>âmbito de aplicação</td><td colspan="3">acesso ilegítimo (artigo 6º da Lei do Cibercrime)
interceção ilegítima (artigo 7º da Lei do Cibercrime)</td></tr>
<tr><td rowspan="3">propósito do agente</td><td colspan="3">exclusiva intenção de identificar a existência de vulnerabilidades (como o fim de, por via da respetiva divulgação, contribuir para a segurança do ciberespaço)</td></tr>
<tr><td rowspan="2">não pode visar qualquer vantagem económica</td><td colspan="2">exclui os chamados caçadores de recompensas</td></tr>
<tr><td>não abrange os profissionais contratados para o efeito pelo dono do sistema</td><td>que ainda assim, têm obrigação de as comunicar as vulnerabilidades que identifiquem</td></tr>
<tr><td rowspan="4">obrigação de comunicação</td><td>proprietário</td><td colspan="2">sempre e imediatamente</td></tr>
<tr><td>CNCS</td><td colspan="2">sempre e imediatamente</td></tr>
<tr><td>titular dos dados pessoais</td><td colspan="2">se for identificada vulnerabilidade de dados pessoais</td></tr>
<tr><td colspan="3">a comunicação é secreta</td></tr>
<tr><td rowspan="3">proporcionalidade na ação</td><td rowspan="2">atuação tem que ser proporcional aos seus propósitos e limitada pelos mesmos</td><td colspan="2">conduta do agente tem que ser necessária à deteção da vulnerabilidade</td></tr>
<tr><td colspan="2">extensão dos sistemas ou dados informáticos acedidos, consultados e/ou copiados foi imposta pelo interesse em contribuir para a segurança do ciberespaço</td></tr>
<tr><td colspan="3">o agente não pode praticar atos que vão para além daqueles que sejam estritamente necessários</td></tr>
<tr><td>outros atos proibidos</td><td colspan="3">• perturbar ou interromper o funcionamento do sistema ou serviço
• eliminar ou deteriorar dados informáticos ou copiar os mesmos sem autorização
• produzir um 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, os que resultariam da própria vulnerabilidade detetada ou da sua exploração
• executar mecanismos de negação de serviço (DoS) ou negação de serviço distribuída (DDoS)
• engenharia social, definida como o facto de enganar responsáveis ou utilizadores dos sistemas de informação com vista à disponibilização de informação sensível ou sigilosa
• ‘phishing’ e variantes
• roubo ou furto de palavras-passe ou outras informações sensíveis
• eliminar ou alterar dolosa de dados informáticos
• inflição dolosa de danos ao sistema de informação
• instalar e distribuir software malicioso
• violação de dados pessoais</td></tr>
</table>

ANEXO 1

LEI DO CIBERCRIME – *extrato*

Artigo 8º-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 contra partida 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, 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 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 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 ao 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.

ANEXO 2

Centro Nacional de Ciber Segurança

Instrução Técnica nº 01/2026
Divulgação Coordenada de Vulnerabilidades

SUMÁRIO

No âmbito da competência atribuída ao Centro Nacional de Cibersegurança de emitir ordens, orientações, recomendações e instruções em matéria de divulgação coordenada de vulnerabilidades, de acordo com a al. h) do n.º 1 do artigo 20.º e do artigo 38.º do Decreto-Lei n.º 125/2025, de 4 de dezembro, aprovou 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, serve a presente Instrução para estabelecer os requisitos aplicáveis à divulgação coordenada de vulnerabilidades.

24 de junho de 2026 – O Coordenador do Centro Nacional de Cibersegurança, José Lino Alves dos Santos.

SECÇÃO I

Artigo 1.º

Objeto

A presente instrução técnica estabelece os requisitos aplicáveis à identificação de vulnerabilidades e à sua divulgação coordenada, nos termos do disposto na alínea h), número 1 do artigo 20.º e do artigo 38.º do Decreto-Lei n.º 125/2025, de 4 de dezembro, que aprova o Regime Jurídico da Cibersegurança.

Artigo 2.º

Âmbito de aplicação

Quem identificar vulnerabilidades que afetem redes e sistema de informação procede da forma descrita nesta instrução técnica e, designadamente procede à sua notificação ao Centro Nacional de Cibersegurança, nos termos aqui previstos.

São abrangidas pelo disposto nesta instrução técnica, as pessoas singulares ou coletivas que tiverem identificado vulnerabilidades que afetem redes e sistemas de informação, produtos, componentes e serviços de tecnologia de informação e comunicação, nos termos do artigo 2º, alínea h) da Lei do Cibercrime (Lei nº 109/2009).

A execução da presente instrução técnica é assegurada pelo CERT.PT, nos termos do artigo 22.º e 38.º do Regime Jurídico da Cibersegurança e na alínea b) do artigo 3.º desta instrução técnica, sem prejuízo da política interna de divulgação coordenada de vulnerabilidades do fabricante, fornecedor ou entidade vulnerável em causa.

Artigo 3.º

Definições

Para efeitos do disposto na presente instrução técnica, entende-se por:

a. «Regime Jurídico da Cibersegurança», aprovado em anexo ao Decreto-Lei n.º 125/2025, de 04 de dezembro;
b. «CERT.PT» - é a equipa nacional de resposta a incidentes de cibersegurança e está integrado no CNCS, nos termos do artigo 22.º do Regime Jurídico da Cibersegurança.
c. «Produto de TIC» - um elemento ou grupo de elementos de uma rede ou um sistema de informação, nos termos do ponto 12 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019;
d. «Serviço de TIC» - um serviço que consiste total ou principalmente na transmissão, no armazenamento, na extração ou no tratamento de informações através de redes e sistemas de

informação, nos termos do ponto 13 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019;

e. «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, definida na aceção do ponto n.º 8 do artigo 2.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho de 17 de abril de 2019;
f. «Divulgação coordenada de vulnerabilidades» - especifica um processo estruturado mediante o qual as vulnerabilidades são notificadas aos fabricantes ou fornecedores de produtos de TIC ou aos prestadores de serviços de TIC potencialmente vulneráveis de uma forma que lhes permite diagnosticar e corrigir as vulnerabilidades antes de serem divulgadas informações pormenorizadas sobre as mesmas a terceiros ou ao público;
g. «Divulgação pública de vulnerabilidades» - ato de tornar pública a informação relativa a uma vulnerabilidade identificada.

SECÇÃO II

Divulgação coordenada de vulnerabilidades

Artigo 4.º

Princípios orientadores da divulgação coordenada de vulnerabilidades

A divulgação coordenada de vulnerabilidades rege-se pelos seguintes princípios orientadores:

a. Princípio da legalidade;
b. Princípio da responsabilidade – a divulgação de vulnerabilidades deve ser realizada de forma responsável, priorizando a segurança e a mitigação das vulnerabilidades identificadas;
c. Princípio da cooperação – todas as partes no processo devem cooperar para a resolução das vulnerabilidades identificadas;
d. Princípio da boa-fé;
e. Princípio da proporcionalidade.

Artigo 5.º

Obrigações das partes no âmbito da divulgação coordenada de vulnerabilidades

1. Quem identificar vulnerabilidades, aquando dessa identificação, deve:
   a. Comunicar, imediatamente, ao fabricante, fornecedor ou entidade vulnerável e, sem demora, ao CERT.PT;
   b. Fornecer todos os elementos e informações relevantes relativas à vulnerabilidade identificada.
   c. Cumprir com o prazo previamente definido e/ou acordado, antes de tornar pública(s) a(s) vulnerabilidade(s).
2. O fabricante, fornecedor ou entidade vulnerável, após o conhecimento de uma vulnerabilidade, deve:
   a. Validar a(s) vulnerabilidade(s) reportada(s) através de uma prova de conceito criada internamente ou cedida por quem identificou a vulnerabilidade;
   b. Comunicar os resultados da sua investigação e análise ao CERT.PT e, caso seja possível, a quem identificou a vulnerabilidade
   c. Caso se confirme a existência da(s) vulnerabilidade(s), desenvolver as ações de mitigação e correção necessárias.
   d. Quando aplicável, comunicar às partes interessadas as medidas de mitigação e correção das a(s) vulnerabilidade(s) identificada(s).
3. O CERT.PT deve:
   a. Receber e analisar a informação comunicada por quem identificar vulnerabilidades;
   b. Acompanhar as comunicações entre aquele e o fabricante, fornecedor ou entidade vulnerável;
   c. Preservar o anonimato, quando solicitado, de quem identificar vulnerabilidades, nos termos do n.º 4 do artigo 38.º do Regime Jurídico da Cibersegurança;

d. Determinar e acordar entre as partes o prazo de resolução e de divulgação das vulnerabilidades identificadas;
e. Monitorizar o processo de comunicação e de resolução das vulnerabilidades.

Artigo 6.º
Comunicação de vulnerabilidades

1. A comunicação de vulnerabilidades é feita através de um email disponibilizado para o efeito ou de outro meio seguro, ambos indicados pelo CERT.PT.
2. O CERT.PT assegura o tratamento das comunicações que reportam vulnerabilidades, bem como, e se possível, a confirmação da sua receção à pessoa singular ou coletiva notificadora no prazo máximo de 72 horas.
3. A referida comunicação contém, se aplicável, pelo menos, os seguintes elementos, nos termos do n.º 2 do artigo 12.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022:
   a. A identificação do fabricante, fornecedor ou entidade vulnerável;
   b. A identificação dos produtos de TIC ou os serviços de TIC afetados pela vulnerabilidade;
   c. As informações relevantes que descrevam a vulnerabilidade;
   d. A gravidade da vulnerabilidade, tendo em conta as circunstâncias em que pode ser explorada;
4. O CERT.PT, após validar a comunicação de vulnerabilidades realizada nos termos dos números anteriores, procede às diligências necessárias à concretização do disposto no n.º 2 do artigo 38.º do Regime Jurídico da Cibersegurança.
5. Sem prejuízo do disposto número anterior, o CERT.PT pode solicitar informações ou elementos adicionais.
6. Nos casos em que a comunicação de vulnerabilidades se revista de relevância criminal, o CERT.PT comunica à Polícia Judiciária, nos termos no n.º 2 do artigo
8.º-A da Lei 109/2009, de 15 de setembro.

SECÇÃO III
Divulgação coordenada de vulnerabilidades
Artigo 7.º
Divulgação coordenada de vulnerabilidades

As vulnerabilidades identificadas e comunicadas nos termos do artigo anterior, só podem ser divulgadas publicamente de acordo com as indicações do CERT.PT, nos termos do artigo 38.º do Regime Jurídico da Cibersegurança e do artigo 8.º da presente instrução técnica, sem prejuízo das normas legais aplicáveis à investigação e ação penais.

Artigo 8.º
Prazos de resolução e divulgação da vulnerabilidade identificada

1. Quem identificar uma vulnerabilidade pode divulgá-la após 90 dias, caso se trate de uma vulnerabilidade que respeite a SOFTWARE, ou 180 dias, caso se trate de uma vulnerabilidade que respeite a HARDWARE, a contar da data da notificação da vulnerabilidade ao fabricante, fornecedor ou entidade vulnerável e ao CERT.PT, em conformidade com o disposto na alínea c), do n.º 3 do artigo 38.º do Decreto-Lei n.º 125/2025, de 4 de dezembro.
2. Os prazos previstos no número anterior podem ser alterados por acordo entre as partes ou por decisão fundamentada do CERT.PT.