PRESIDÊNCIA DO CONSELHO DE MINISTROS

Decreto-Lei n.º 65/2021

de 30 de julho

Sumário: Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019.

Através da Lei n.º 46/2018, de 13 de agosto, que aprovou o regime jurídico da segurança do ciberespaço, foi transposta para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

A referida lei remete para legislação complementar a definição, por um lado, dos requisitos de segurança das redes e sistemas de informação e, por outro lado, das regras para a notificação de incidentes, que devem ser cumpridos pela Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais. O presente decreto-lei procede, assim, à regulamentação destes aspetos.

Os requisitos previstos no presente decreto-lei constituem um mínimo a assegurar pelas entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, não prejudicando as regras que, em função da natureza das entidades, de aspetos específicos da atividade desenvolvida ou do contexto em que esta se desenvolva, possam vir a ser estabelecidas por outras autoridades, nomeadamente pelo Ministério Público, pela Autoridade Nacional de Emergência e Proteção Civil, pelo Conselho Nacional de Planeamento Civil de Emergência, pela Autoridade Nacional de Comunicações, pela Comissão Nacional de Proteção de Dados, ou por outras autoridades setoriais.

Tendo presente que o ciberespaço é uma realidade dinâmica e fluida, em permanente mutação, colocando desafios de alcance transnacional e que atravessa vários setores de atividade, o presente decreto-lei reconhece a necessidade de articular as disposições legais aqui consagradas com a aplicação de normativos complementares setoriais. Para este efeito, o Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, nos casos em que se considere necessário e em articulação com as entidades reguladoras e de supervisão setoriais, procede a uma avaliação de equivalência, conferindo, assim, segurança jurídica aos requisitos constantes de legislação setorial que sejam considerados equivalentes aos consagrados no presente decreto-lei.

Adicionalmente à regulamentação do regime jurídico aprovado pela Lei n.º 46/2018, de 13 de agosto, e considerando a complementaridade que a certificação de produtos, serviços e processos de tecnologias de informação e comunicação assume para a promoção de um ciberespaço mais seguro, assegura-se a implementação, na ordem jurídica nacional, das obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, permitindo a implementação de um quadro nacional de certificação da cibersegurança pela Autoridade Nacional de Certificação da Cibersegurança.

O caráter transfronteiriço da cibersegurança e o esforço de cooperação internacional que lhe está subjacente permitem a produção de conhecimento em permanente atualização e o desenvolvimento contínuo de um conjunto de boas práticas, vertidas para o plano nacional através do Quadro Nacional de Referência para a Cibersegurança, com o qual é estabelecida uma relação para efeitos de análise dos riscos a realizar pelas respetivas entidades abrangidas, sem prejuízo da natureza transversal deste documento enquanto referencial para um fortalecimento da resiliência de cada organização face às ameaças que afetam o ciberespaço.

Em alinhamento com o Programa do XXII Governo Constitucional, que reconhece a importância de promover políticas e melhores práticas de cibersegurança, o decreto-lei que ora se aprova procura dar resposta ao papel cada vez mais determinante que as tecnologias de informação assumem na forma como se desenvolve a vida em sociedade, seja na atividade dos agentes económicos e dos serviços públicos, seja nas próprias relações entre as pessoas e entre os cidadãos e a Administração Pública. O desafio da transição digital, de alcance transversal, e a emergência de novas tecnologias

disruptivas, como a inteligência artificial, a realidade virtual e aumentada e a Internet das coisas, sublinham a necessidade de assegurar um nível elevado de segurança das redes e dos sistemas de informação que sustentam o uso destas tecnologias, para que decorra num ambiente de confiança e protegido de ameaças que podem ter efeitos desestabilizadores de considerável alcance na vida em sociedade, especialmente em contextos de crise, que tendem a agravar a exploração de vulnerabilidades por parte de agentes de ameaça com motivações diversas.

Foram ouvidas a Entidade Reguladora dos Serviços Energéticos, a Autoridade Nacional da Aviação Civil, a Autoridade da Mobilidade e dos Transportes, o Conselho Nacional de Supervisores Financeiros, a Entidade Reguladora dos Serviços de Águas e Resíduos, a Autoridade Nacional de Comunicações, a Autoridade Nacional de Emergência e Proteção Civil, a Comissão Nacional de Proteção de Dados, os órgãos de governo próprio da Região Autónoma dos Açores, a Associação Nacional de Municípios Portugueses e a Associação Nacional de Freguesias.

Foi promovida a audição da Entidade Reguladora da Saúde e dos órgãos de governo próprio da Região Autónoma da Madeira.

O presente decreto-lei foi submetido a consulta pública entre 12 de abril e 5 de maio de 2021.

Assim:

Ao abrigo do disposto no artigo 31.º da Lei n.º 46/2018, de 13 de agosto, e nos termos da alínea *c*) do n.º 1 do artigo 198.º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

1 — O presente decreto-lei procede à:

a) Regulamentação da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço (Regime Jurídico da Segurança do Ciberespaço), transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União;

b) Execução, na ordem jurídica nacional, das obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, permitindo a implementação de um quadro nacional de certificação da cibersegurança.

2 — Para efeitos do disposto na alínea *a*) do número anterior são estabelecidos:

a) Os requisitos de segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas e pelos operadores de serviços essenciais, nos termos dos artigos 12.º, 14.º e 16.º do Regime Jurídico da Segurança do Ciberespaço;

b) Os requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação que devem ser cumpridos pela Administração Pública, pelos operadores de infraestruturas críticas, pelos operadores de serviços essenciais e pelos prestadores de serviços digitais, nos termos dos artigos 13.º, 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço, prevendo as circunstâncias, o prazo, o formato e os procedimentos aplicáveis.

Artigo 2.º

Âmbito de aplicação

1 — O presente decreto-lei aplica-se às entidades previstas nas alíneas *a*) a *d*) do n.º 1 do artigo 2.º do Regime Jurídico da Segurança do Ciberespaço, sem prejuízo do disposto nos números seguintes.

2 — Os requisitos de segurança das redes e dos sistemas de informação constantes do presente decreto-lei não se aplicam às empresas e aos prestadores de serviços referidos no n.º 2 do artigo 12.º do Regime Jurídico da Segurança do Ciberespaço.

3 — Os requisitos de notificação de incidentes que afetem a segurança das redes e dos sistemas de informação constantes do presente decreto-lei não se aplicam:

a) Às empresas e aos prestadores de serviços referidos no n.º 2 do artigo 13.º do Regime Jurídico da Segurança do Ciberespaço;

b) Aos prestadores de serviços digitais que sejam microempresas ou pequenas empresas, tal como definidas pelo Decreto-Lei n.º 372/2007, de 6 de novembro, na sua redação atual.

4 — Para efeito do cumprimento do Regime Jurídico da Segurança do Ciberespaço e do presente decreto-lei, a identificação dos operadores de serviços essenciais nos termos do n.º 1 do artigo 29.º do Regime Jurídico da Segurança do Ciberespaço, bem como a atualização anual prevista no n.º 2 do mesmo artigo, é comunicada pelo Centro Nacional de Cibersegurança (CNCS) aos operadores.

CAPÍTULO II

Disposições comuns

Artigo 3.º

Princípios e regras gerais

1 — A adoção das medidas técnicas e organizativas destinadas ao cumprimento dos requisitos de segurança previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei obedece ao princípio da adequação e da proporcionalidade, devendo ter em consideração:

a) As condições normais de funcionamento das redes e dos sistemas de informação;

b) As situações extraordinárias, designadamente:

i) A ocorrência de incidentes, nos termos da alínea *c*) do artigo 3.º do Regime Jurídico da Segurança do Ciberespaço;

ii) A ocorrência de acidente grave ou catástrofe, nos termos previstos nas disposições legais e regulamentares aplicáveis em matéria de proteção civil ou a eventual ativação de planos de emergência de proteção civil;

iii) A declaração do estado de emergência, de sítio ou de guerra, nos termos previstos na Constituição ou em outras disposições legais e regulamentares aplicáveis;

iv) A ativação de planos no âmbito do planeamento civil de emergência no setor da cibersegurança, nos termos do Decreto-Lei n.º 43/2020, de 21 de julho;

v) A ocorrência de grave ameaça à segurança interna, incluindo as situações de ataques terroristas, nos termos previstos nas disposições legais e regulamentares aplicáveis em matéria de segurança interna.

2 — O cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei deve ser efetuado em conformidade com as disposições respeitantes à segurança de matérias classificadas no âmbito nacional e no âmbito das organizações internacionais de que Portugal seja parte.

3 — O cumprimento dos requisitos de segurança e das obrigações de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei não prejudica:

a) O cumprimento dos requisitos específicos de segurança e das obrigações específicas de notificação de incidentes nos termos definidos pelas autoridades competentes, nomeadamente pelo Ministério Público, pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC), pela

Autoridade Nacional de Comunicações (ANACOM), pela Comissão Nacional de Proteção de Dados (CNPD) e por outras autoridades setoriais, nos termos das disposições legais e regulamentares aplicáveis;

b) O cumprimento de legislação da União Europeia.

4 — Aos prestadores de serviços digitais aplica-se o disposto no Regulamento de Execução (UE) 2018/151, da Comissão, de 30 de janeiro de 2018, em matéria de requisitos de segurança e de notificação de incidentes.

5 — As entidades referidas no n.º 1 do artigo anterior podem estabelecer formas de colaboração com vista ao cumprimento das obrigações em matéria de requisitos de segurança e de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço, e no presente decreto-lei, numa lógica de partilha de recursos, desde que seja assegurada a efetiva operacionalização das mesmas em cada entidade.

6 — O disposto no número anterior não prejudica a responsabilização de cada entidade individualmente considerada a que haja lugar pela infração a qualquer disposição do presente decreto-lei.

7 — O CNCS pode, através da regulamentação complementar prevista no artigo 18.º, estabelecer condições específicas para o cumprimento dos requisitos de segurança e de notificação de incidentes previstos no presente decreto-lei por parte das entidades da Administração Pública, em termos proporcionais e adequados à sua dimensão ou complexidade organizacional.

Artigo 4.º

Ponto de contacto permanente

1 — As entidades devem indicar, pelo menos, um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS, nomeadamente:

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

b) A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetida pela mesma ou outra entidade;

c) A obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;

d) A partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias;

e) 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 do ciberespaço;

f) A receção das instruções técnicas emitidas ao abrigo do disposto no n.º 5 do artigo 7.º do Regime Jurídico da Segurança do Ciberespaço e no artigo 18.º;

g) A operacionalização dos procedimentos fixados no âmbito dos planos de segurança previstos no artigo 7.º

2 — As entidades devem assegurar a função de 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 do CNCS.

3 — As entidades devem indicar ao CNCS, no prazo de 20 dias úteis a contar do início da respetiva atividade, a pessoa ou pessoas responsáveis por assegurar as funções de ponto de contacto permanente, bem como os respetivos meios de contacto principal e alternativos.

4 — As entidades 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 do prazo previsto no n.º 2 do artigo 23.º

5 — As entidades devem comunicar imediatamente ao CNCS qualquer alteração à informação prevista no n.º 3.

6 — As entidades devem assegurar que o ponto de contacto permanente dispõe de meios de contacto principais e alternativos para a comunicação com o CNCS.

Artigo 5.º

Responsável de segurança

1 — As entidades devem designar um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do presente decreto-lei.

2 — As entidades devem indicar ao CNCS, no prazo de 20 dias úteis a contar do início da respetiva atividade, a pessoa designada para as funções de responsável de segurança.

3 — As entidades 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 do prazo previsto no n.º 2 do artigo 23.º

4 — As entidades devem comunicar imediatamente ao CNCS a substituição do responsável de segurança.

Artigo 6.º

Inventário de ativos

1 — As entidades devem elaborar e manter atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços, devendo o mesmo ser assinado pelo responsável de segurança.

2 — No inventário de ativos deve constar, para cada ativo, a informação definida em instruções técnicas emitidas pelo CNCS.

3 — As entidades devem comunicar ao CNCS a lista dos ativos constantes do inventário, com a informação que venha a ser determinada nos termos do número anterior, com a seguinte periodicidade:

a) Na sua versão inicial, no prazo de 20 dias úteis a contar da data de início de atividade;

b) Numa versão atualizada, anualmente, a ser entregue em conjunto com o relatório anual a que se refere o artigo 8.º

Artigo 7.º

Plano de segurança

1 — As entidades devem elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, que contenha:

a) A política de segurança, incluindo a descrição das medidas organizativas e a formação de recursos humanos;

b) A descrição de todas as medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes;

c) A identificação do responsável de segurança;

d) A identificação do ponto de contacto permanente.

2 — Para efeitos do cumprimento do disposto no número anterior, os operadores de infraestruturas críticas podem utilizar o plano previsto no artigo 10.º do Decreto-Lei n.º 62/2011, de 9 de maio, desde que o mesmo inclua medidas relativas à segurança das redes e da informação.

Artigo 8.º

Relatório anual

1 — As entidades devem elaborar um relatório anual que, em relação ao ano civil a que se reporta, contenha os seguintes elementos:

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 de segurança com impacto relevante ou substancial, com informação sobre:

i) Número de utilizadores afetados pela perturbação do serviço;
ii) Duração dos incidentes;
iii) Distribuição geográfica, no que se refere à zona afetada pelo incidente, 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 relevante.

2 — As entidades devem remeter o relatório anual ao CNCS, devidamente assinado pelo responsável de segurança, nos seguintes termos:

a) Relativamente ao primeiro relatório anual:

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;
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) Relativamente aos relatórios subsequentes anuais, 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 todo o período entre a data de início de atividade e o final do ano civil anterior.
4 — Para efeitos do disposto no presente artigo, o CNCS pode definir o formato em que a informação deve ser apresentada.
5 — As entidades reguladoras e as entidades com poderes de supervisão sobre os setores e subsetores identificados no anexo ao Regime Jurídico da Segurança do Ciberespaço, remetem ao CNCS os relatórios considerados equivalentes nos termos do artigo 18.º, quando tal resulte de instrução complementar emitida pelo CNCS, em articulação com as entidades reguladoras e de supervisão acima referidas.

CAPÍTULO III

Segurança das redes e dos sistemas de informação

Artigo 9.º

Medidas para cumprimento dos requisitos de segurança

1 — As entidades referidas na alínea *a*) do n.º 2 do artigo 1.º devem cumprir as medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas

de informação que utilizam, devendo, para o efeito, realizar uma análise dos riscos de acordo com o disposto no artigo seguinte.

2 — As medidas referidas no número anterior devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes, através da utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.

Artigo 10.º

Análise dos riscos e implementação dos requisitos de segurança

1 — As entidades da Administração Pública e os operadores de infraestruturas críticas, bem como os operadores de serviços essenciais, devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, no caso dos operadores de serviços essenciais, também em relação aos ativos que garantam a prestação dos serviços essenciais, nos seguintes termos:

a) Análise dos riscos de âmbito global, com a seguinte periodicidade:

i) Pelo menos uma vez por ano;
ii) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que implique uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS;

b) Análise dos riscos de âmbito parcial, com a seguinte periodicidade:

i) Durante o planeamento e preparação da introdução de uma alteração ao ativo ou ativos, em relação ao ativo ou ativos envolvidos;
ii) Após a ocorrência de um incidente com impacto relevante ou outra situação extraordinária, em relação aos ativos afetados;
iii) Após a notificação, por parte do CNCS, de um risco, de uma ameaça ou de uma vulnerabilidade emergentes que impliquem uma elevada probabilidade de ocorrência de um incidente com impacto relevante, dentro do prazo fixado pelo CNCS.

2 — As entidades devem documentar a preparação, a execução e a apresentação dos resultados da análise dos riscos.

3 — A análise do risco deve abranger para cada ativo:

a) A identificação das ameaças, internas ou externas, intencionais ou não intencionais, incluindo, nomeadamente:

i) Falha de sistema;
ii) Fenómeno natural;
iii) Erro humano;
iv) Ataque malicioso;
v) Falha no fornecimento de bens ou serviços por terceiro;

b) A caracterização do impacto e da probabilidade da ocorrência das ameaças identificadas na alínea anterior.

4 — A análise dos riscos deve ter em consideração:

a) O histórico de situações extraordinárias ocorridas;
b) O histórico de incidentes e, em especial, de incidentes com impacto relevante;
c) O número de utilizadores afetados pelos incidentes;

d) A duração dos incidentes;
e) A distribuição geográfica, no que se refere à zona afetada pelos incidentes;
f) As dependências intersetoriais para efeitos da prestação dos serviços, incluindo os constantes do anexo ao Regime Jurídico da Segurança do Ciberespaço e o setor das comunicações eletrónicas.

5 — A análise dos riscos deve ainda ter em consideração a avaliação integrada dos riscos para a segurança das redes e dos sistemas de informação a nível nacional, europeu e internacional, publicada anualmente ou notificada às entidades pelo CNCS.
6 — Na sequência de cada análise dos riscos, as entidades devem adotar as medidas técnicas e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, e que resultem, nomeadamente:

a) De normativo complementar setorial aprovado pelo CNCS, sem prejuízo da aplicação de outro normativo nacional e da União Europeia em matéria da segurança das redes e dos sistemas de informação;
b) Do Quadro Nacional de Referência de Cibersegurança, e respetivas disposições complementares, elaborado pelo CNCS, na ausência ou em complemento do normativo setorial previsto na alínea anterior.

7 — Os riscos para a segurança das redes e dos sistemas de informação caracterizados como residuais devem ser tratados pelas entidades nos termos do número anterior.
8 — As entidades devem rever e, se necessário, atualizar o seu plano de segurança, nos termos previstos no artigo 7.º, em função da evolução do contexto de atuação e da ocorrência de incidentes.
9 — As medidas a adotar ao abrigo do disposto no n.º 6 devem permitir:

a) A prevenção, a gestão e a redução dos riscos;
b) O reforço da robustez e da resiliência dos ativos, incluindo a respetiva proteção contra as ameaças identificadas e a respetiva recuperação ou redundância, de forma a assegurar um rápido restabelecimento do funcionamento das redes e dos sistemas de informação;
c) Uma resposta eficaz a incidentes, a ameaças ou a vulnerabilidades.

10 — Para efeitos do disposto no presente artigo, o CNCS pode emitir instruções técnicas com vista a uma harmonização da matriz de risco a adotar pelas entidades.

CAPÍTULO IV

Notificações de incidentes

Artigo 11.º

Obrigações de notificação

1 — A Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais notificam o CNCS da ocorrência de incidentes com impacto relevante ou substancial nos termos, respetivamente, dos artigos 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço.
2 — As entidades devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial.
3 — A Administração Pública e os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais devem, perante qualquer incidente detetado ou a estes comunicado pelos seus clientes, utilizadores ou outras entidades, atender aos parâmetros previstos, respetivamente, no n.º 4 do artigo 15.º, no n.º 4 do artigo 17.º e no n.º 4 do artigo 19.º do Regime Jurídico da Segurança do Ciberespaço, bem como aos constantes dos nor-

mativos complementares setoriais aplicáveis, para classificar os incidentes como tendo impacto relevante ou substancial.

Artigo 12.º

Tipos de notificações

1 — Por cada incidente que deva ser objeto de notificação ao abrigo do disposto no artigo anterior, as entidades devem submeter ao CNCS:

a) Uma notificação inicial, nos termos do artigo seguinte;
b) Uma notificação de fim de impacto relevante ou substancial, nos termos do artigo 14.º;
c) Uma notificação final, nos termos do artigo 15.º

2 — Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final com todos os campos de informação devidamente preenchidos, ficando dispensadas do envio das restantes notificações.

Artigo 13.º

Notificação inicial

1 — A notificação inicial deve ser enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação, devendo a entidade, sem prejuízo do cumprimento deste prazo, dar prioridade à mitigação e à resolução do incidente.
2 — A notificação inicial deve incluir 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 4.º, para efeito de um eventual contacto por parte do CNCS;
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 raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo 16.º e, 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 de impacto transfronteiriço;

e) Outra informação que a entidade considere relevante.

Artigo 14.º

Notificação de fim de impacto relevante ou substancial

1 — A notificação de fim de impacto relevante ou substancial do incidente deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial.
2 — A notificação de fim de impacto relevante ou substancial 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 do impacto existente no momento da perda de impacto relevante ou substancial, 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 15.º

Notificação final

1 — A notificação final deve ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar.
2 — A notificação final deve incluir a seguinte informação:

a) Data e hora em que o incidente assumiu o impacto relevante ou substancial;
b) Data e hora em que o incidente perdeu o impacto relevante ou substancial;
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 indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo seguinte, e o respetivo detalhe;

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;

f) Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente ao Ministério Público, à ANEPC, à ANACOM, à CNPD e a outras autoridades setoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis;
g) Outra informação que a entidade considere relevante.

3 — Nos casos em que exista uma situação residual do impacto à data da notificação final, descrita ao abrigo do disposto na alínea *e*) do número anterior, as entidades devem comunicar ao CNCS, logo que possível, a recuperação total dessa situação residual.

Artigo 16.º

Taxonomia de incidentes e de efeitos

1 — Para efeitos do disposto nos artigos 13.º a 15.º, os incidentes podem ter as seguintes categorias de causas raiz:

a) Falha de sistema;
b) Fenómeno natural;

c) Erro humano;
d) Ataque malicioso;
e) Falha no fornecimento de bens ou serviços por terceiro.

2 — Para os efeitos do disposto nos artigos 13.º a 15.º, os incidentes podem ter os seguintes efeitos produzidos:

a) Infeção por *malware*;
b) Disponibilidade;
c) Recolha de informação;
d) Intrusão;
e) Tentativa de intrusão;
f) Segurança da informação;
g) Fraude;
h) Conteúdo abusivo;
i) Outro.

3 — As entidades podem enviar ao CNCS, de forma voluntária, qualquer informação adicional relevante que sirva de suporte ao reporte de incidentes e que facilite o respetivo acompanhamento.

Artigo 17.º

Disposições complementares

1 — O CNCS presta à entidade notificante as informações relevantes relativas ao processamento do incidente notificado, nomeadamente informações que possam contribuir para o tratamento eficaz do incidente.

2 — As entidades devem dar resposta a qualquer pedido de informação adicional por parte do CNCS sobre os incidentes reportados.

3 — As entidades podem optar por enviar ao CNCS qualquer campo de informação antes do final dos prazos fixados para o efeito, desde que disponham de informação fiável para o fazer.

4 — Sem prejuízo do disposto no presente capítulo, as entidades devem seguir o formato e o procedimento de notificação de incidentes definido nos normativos complementares setoriais aplicáveis.

CAPÍTULO V

Disposições complementares e finais

Artigo 18.º

Regulamentação complementar

1 — O CNCS pode, no âmbito das suas competências, emitir instruções técnicas complementares em matéria de requisitos de segurança e de notificação de incidentes, designadamente normativos complementares setoriais.

2 — Sempre que um ato jurídico setorial da União Europeia exigir que as entidades abrangidas pelo presente decreto-lei garantam a segurança das respetivas redes e dos respetivos sistemas de informação ou a notificação de incidentes, são aplicáveis as disposições desse ato jurídico setorial desde que os seus requisitos tenham pelo menos efeitos equivalentes às obrigações constantes do presente decreto-lei, devendo, sempre que necessário, ser especificada a respetiva implementação pelo CNCS em articulação com as entidades reguladoras e com as entidades com poderes de su-

pervisão sobre os setores e subsetores identificados no anexo ao Regime Jurídico da Segurança do Ciberespaço, seguindo-se o seguinte procedimento:

a) O CNCS, em articulação com as entidades reguladoras e as entidades com poderes de supervisão sobre os setores e subsetores identificados no anexo ao Regime Jurídico da Segurança do Ciberespaço avaliam o grau de equivalência das regras relativas ao inventário de ativos e ao relatório anual bem como dos requisitos de segurança e notificação de incidentes estabelecidos para cada setor;

b) Na avaliação do grau de equivalência deve ser ponderado em que medida os requisitos setoriais definidos pela lei, pelas disposições europeias e pelos normativos setoriais cumprem os requisitos previstos no presente decreto-lei, procurando, sempre que possível, evitar a sobreposição de requisitos e reportes;

c) O CNCS emite, por instrução técnica, o resultado da avaliação do grau de equivalência prevista no presente decreto-lei.

Artigo 19.º

Comunicações

1 — As comunicações entre as entidades e o CNCS, incluindo as notificações de incidentes, devem seguir o formato e o procedimento definido em regulamentação complementar.

2 — Na ausência de regulamentação complementar, todas as comunicações dirigidas ao CNCS no âmbito do presente decreto-lei, bem como o envio de informação, devem ser realizadas por meios eletrónicos.

3 — O CNCS mantém e gere a informação em matéria de segurança e integridade num sistema de informação seguro, em conformidade com as disposições respeitantes à segurança de matérias classificadas no âmbito nacional e no âmbito das organizações internacionais de que Portugal é parte.

4 — 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 de 2014, relativo à identificação eletrónica e aos serviços de confiança, designadamente através do Cartão de Cidadão e da Chave Móvel Digital.

5 — Nos casos em que a entidade não tenha temporariamente capacidade operacional para assegurar a comunicação prevista nos n.os 2 e 3, ou nos casos em que o sítio na Internet do CNCS 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, de acordo com instruções técnicas a emitir pelo CNCS.

Artigo 20.º

Autoridade Nacional de Certificação da Cibersegurança

1 — O CNCS é a Autoridade Nacional de Certificação da Cibersegurança (ANCC) designadamente para efeitos do disposto no artigo 58.º do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, gozando para este efeito de independência técnica.

2 — A ANCC pode, para além das respetivas atribuições no âmbito dos esquemas europeus de certificação da cibersegurança, desenvolver e implementar esquemas específicos de certificação da cibersegurança relativos a 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.

3 — A ANCC implementa um quadro nacional de certificação da cibersegurança, estabelecendo as disposições necessárias à elaboração, implementação e execução dos esquemas de certificação previstos no número anterior, 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 de 2019.

4 — Constituem competências da ANCC:

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 respetivas atribuições;

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 lei em matéria de certificação da cibersegurança;

c) Executar as demais competências 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 de 2019.

5 — A avaliação dos esquemas de certificação específicos, designadamente sobre a respetiva adequação, é efetuada pela ANCC em articulação com o Instituto Português de Acreditação, I. P., enquanto organismo nacional de acreditação e com o Instituto Português da Qualidade, I. P., enquanto organismo nacional de normalização e com as demais entidades públicas com competências no âmbito da matéria abrangida pela certificação.

Artigo 21.º

Regime sancionatório

1 — Às infrações ao disposto no presente decreto-lei é aplicável o regime sancionatório previsto no Regime Jurídico da Segurança do Ciberespaço aprovado pela Lei n.º 46/2018, de 13 de agosto.

2 — Constitui contraordenação punível com coima de € 1000,00 a € 3740,98, no caso de pessoa singular, ou de € 5000,00 a € 44 891,81, no caso de pessoa coletiva, a prática das seguintes infrações:

a) A utilização 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.

3 — Sem prejuízo das competências atribuídas a outras entidades em razão da matéria, às contraordenações previstas no número anterior aplica-se o disposto nos artigos 21.º e 25.º a 28.º do Regime Jurídico da Segurança do Ciberespaço.

Artigo 22.º

Disposição transitória

1 — O primeiro relatório anual a que se refere a alínea *a*) do n.º 2 do artigo 8.º deve ser entregue até 31 de janeiro de 2022, sem prejuízo do disposto na subalínea *ii*) da alínea *a*) do n.º 2 do mesmo artigo.

2 — A versão inicial do inventário de ativos a que se refere o artigo 6.º deve ser entregue em conjunto com o relatório anual referido no número anterior.

Artigo 23.º

Entrada em vigor e produção de efeitos

1 — Sem prejuízo dos números seguintes, o presente decreto-lei entra em vigor no décimo dia seguinte ao da sua publicação.

2 — O disposto nos artigos 4.º, 5.º, 7.º e 11.º a 17.º produz efeitos 90 dias após a entrada em vigor do presente decreto-lei.

3 — O disposto nos artigos 9.º e 10.º produz efeitos no prazo de um ano após a entrada em vigor do presente decreto-lei.

Visto e aprovado em Conselho de Ministros de 17 de junho de 2021. — *António Luís Santos da Costa — Pedro Gramaxo de Carvalho Siza Vieira — Augusto Ernesto Santos Silva — Mariana Guimarães Vieira da Silva — João Rodrigo Reis Carvalho Leão — Eduardo Arménio do Nascimento Cabrita — Francisca Eugénia da Silva Dias Van Dunem — Alexandra Ludomila Ribeiro Fernandes Leitão — Marta Alexandra Fartura Braga Temido de Almeida Simões — João Pedro Soeiro de Matos Fernandes — Hugo Santos Mendes — Ricardo da Piedade Abreu Serrão Santos.*

Promulgado em 22 de julho de 2021.

Publique-se.

O Presidente da República, Marcelo Rebelo de Sousa.

Referendado em 23 de julho de 2021.

O Primeiro-Ministro, *António Luís Santos da Costa.*

114443494