PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

Regulamento n.º 183/2022

Sumário: Regulamento que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança.

Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes

A Lei n.º 46/2018, de 13 de agosto, estabeleceu o 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 dos sistemas de informação em toda a União.

O regime jurídico da segurança do ciberespaço aplica-se às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente, no âmbito da notificação voluntária de incidentes.

O regime jurídico da segurança do ciberespaço estabeleceu a Estrutura de Segurança do Ciberespaço, consagrando o Centro Nacional de Cibersegurança como Autoridade Nacional de Cibersegurança e o «CERT.PT» como Equipa de Resposta a Incidentes de Segurança Informática Nacional.

Foram ainda estabelecidas as obrigações de notificação de incidentes à Autoridade Nacional de Cibersegurança e as obrigações de implementação de requisitos de segurança para a Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais.

O regime jurídico da segurança do ciberespaço foi objeto de regulamentação através do Decreto-Lei n.º 65/2021, de 30 de julho, que procede ainda à 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.

Em consequência, foi necessário a aprovação de Instrução Técnica complementar ao Decreto-Lei n.º 65/2021, de 30 de julho, tendo como base legal a previsão do n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, para definir os termos de aplicação quanto às seguintes disposições do Decreto-Lei n.º 65/2021, de 30 de julho:

a) N.os 3, 4 e 5 do artigo 4.º, referente à indicação de ponto de contacto permanente;

b) N.os 2, 3 e 4 do artigo 5.º referente à indicação do responsável de segurança;

c) N.os 1, 2 e 3 do artigo 6.º referentes à informação que, para cada ativo, deve constar do inventário de ativos e à comunicação da lista de ativos;

d) N.os 1, 2, 3 e 4 do artigo 8.º relativo à informação que deve constar do relatório anual e à comunicação do relatório anual;

e) N.º 1 do artigo 12.º, n.º 1 do artigo 13.º, n.º 1 do artigo 14.º, n.º 1 do artigo 15.º e n.º 2 do artigo 17.º referentes ao envio das notificações de incidentes e de informação adicional.

Nos termos das competências que lhe são cometidas e de acordo com os poderes e funções do Centro Nacional de Cibersegurança, como Autoridade Nacional de Cibersegurança, o subdiretor-geral do Gabinete Nacional de Segurança responsável pela coordenação do Centro Nacional de Cibersegurança, aprovou por despacho de 3 de novembro de 2021 projeto de regulamento que configura uma Instrução Técnica relativa à comunicação e informação referentes a pontos de con-

tacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes, o qual foi submetido a consulta pública através do Aviso n.º 21606, de 17 de novembro, publicado no *Diário da República,* 2.ª série, n.º 223.

Findo o prazo de consulta pública, foram recebidas 13 pronúncias. Atento os contributos recebidos e de acordo com a fundamentação estabelecida no relatório da consulta pública, o projeto de regulamento em consulta pública foi objeto das alterações que se entenderam como oportunas e pertinentes de acordo com as sugestões realizadas.

A fundamentação da análise realizada pelo CNCS e das decisões tomadas consta do relatório da consulta pública, que se encontra publicado no sítio institucional do CNCS na Internet, em conjunto com as pronúncias integrais recebidas. Este relatório contém referência a todos os contributos recebidos, bem como o resultado da apreciação que reflete o entendimento sobre os mesmos e os fundamentos das opções tomadas pelo CNCS.

Assim, nos termos e em cumprimento do disposto na alínea *c*) do n.º 1 do artigo 2.º-A, no artigo 3.º e no n.º 4 do artigo 4.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, na redação atual, que aprova a orgânica do Gabinete Nacional de Segurança, nos termos do n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço e ao abrigo das competências que me foram delegadas através da alínea *a*) do n.º 1 do Despacho n.º 8689/2021, de 23 de agosto, do diretor-geral do Gabinete Nacional de Segurança, publicado no *Diário da República,* 2.ª série, de 2 de setembro de 2021, aprovo, nos termos referidos e fundamentados no relatório da consulta pública do projeto de regulamento, o seguinte Regulamento que configura Instrução Técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes:

28 de janeiro de 2022. — O Coordenador do Centro Nacional de Cibersegurança, *José Lino Alves dos Santos.*

Instrução técnica relativa à comunicação e informação referentes a pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes

No âmbito da competência de emitir instruções de cibersegurança atribuída ao Centro Nacional de Cibersegurança (CNCS) de acordo com o n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, e com o previsto no n.º 1 do artigo 19.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, que 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, serve a presente Instrução para definir os termos de aplicação deste normativo quanto às seguintes disposições: n.os 3, 4 e 5 do artigo 4.º, referente à indicação de ponto de contacto permanente; n.os 2, 3 e 4 do artigo 5.º referente à indicação do responsável de segurança; n.os 1, 2 e 3 do artigo 6.º referentes à informação que, para cada ativo, deve constar do inventário de ativos e à comunicação da lista de ativos; n.os 1, 2, 3 e 4 do artigo 8.º relativo à informação que deve constar do relatório anual e à comunicação do relatório anual; n.º 1 do artigo 12.º, n.º 1 do artigo 13.º, n.º 1 do artigo 14.º, n.º 1 do artigo 15.º e n.º 2 do artigo 17.º referentes ao envio das notificações de incidentes e de informação adicional.

Artigo 1.º

Envio e tratamento de informação

1 — O envio de informação ao CNCS no âmbito dos artigos 4.º, 5.º, 6.º e 8.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, deve ser realizada por meios eletrónicos para o endereço de correio eletrónico sri@cncs.gov.pt, ou via API (application programming interface) disponibilizada pelo CNCS para o efeito.

2 — Caso as entidades pretendam enviar a informação protegida por método criptográfico, podem proteger a informação utilizando a chave pública de PGP, associada ao endereço de correio eletrónico referido no número anterior, publicada no sítio na Internet do CNCS.

3 — O CNCS mantém e gere a informação recebida nos números anteriores, num sistema de informação seguro em conformidade com as disposições respeitantes à segurança de matérias classificadas com o grau de segurança Reservado na marca Nacional, salvo quando necessário grau de segurança superior.

Artigo 2.º

Ponto de contacto permanente

1 — O ponto de contacto permanente deve ser comunicado ao CNCS nos termos dos n.os 3, 4 e 5, do artigo 4.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021.

2 — A informação a constar da comunicação a realizar ao CNCS deve conter o nome da pessoa ou pessoas responsáveis, ou serviço disponível ou equipa operacional, por assegurar as funções de ponto de contacto permanente, e indicação dos meios de contacto principais e alternativos, nomeadamente contendo, no mínimo, a seguinte informação:

a) Nome da entidade;
b) Endereço de correio eletrónico principal;
c) Endereço de correio eletrónico alternativo;
d) Número de telefone fixo principal, se aplicável;
e) Número de telefone móvel principal;
f) Número de telefone fixo alternativo, se aplicável;
g) Número de telefone móvel alternativo;
h) Outros contactos alternativos.

3 — Esta comunicação deve ser realizada para o endereço de correio eletrónico indicado no n.º 1 do artigo 1.º da presente Instrução, preenchendo e juntando o formulário, constante do anexo I à presente Instrução, e disponível no sítio na Internet do Centro Nacional de Cibersegurança, que deve ser descarregado após a publicação da presente Instrução.

Artigo 3.º

Responsável de segurança

1 — A indicação da pessoa designada para as funções de responsável de segurança deve ser comunicada ao CNCS nos termos dos n.os 2, 3 e 4 do artigo 5.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021.

2 — A informação a constar da comunicação a realizar ao CNCS deve conter o nome da pessoa designada para assegurar as funções de responsável de segurança nomeadamente contendo, no mínimo, a seguinte informação:

a) Nome da entidade;
b) Nome do responsável de segurança;
c) Cargo do responsável de segurança;
d) Endereço de correio eletrónico;
e) Número de telefone fixo, se aplicável;
f) Número de telefone móvel.

3 — Esta comunicação deve ser realizada para o endereço de correio eletrónico indicado no n.º 1 do artigo 1.º da presente Instrução, preenchendo e juntando o formulário, constante do anexo II à presente Instrução, e disponível no sítio na Internet do Centro Nacional de Cibersegurança, que deve ser descarregado após a publicação da presente Instrução.

Artigo 4.º

Inventário de ativos

1 — Para os efeitos do disposto na presente instrução, entende -se por «Ativo» todo o sistema de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços.

2 — Para cada ativo identificado de acordo com o n.º 1 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021 aplica-se o seguinte:

2.1 — A entidade deve efetuar o inventário dos seus equipamentos de acordo com as seguintes regras:

a) Os dispositivos físicos e sistemas devem ser inventariados com a seguinte informação:

i) Número de inventário;
ii) Nome e modelo do equipamento;
iii) Número de série;
iv) Localização.

b) Os dispositivos ligados à rede devem ter a seguinte informação complementar:

i) Endereço IP;
ii) Endereço de hardware.

c) Os responsáveis dos dispositivos e sistemas devem ser identificados com, pelo menos, os seguintes elementos:

i) Nome;
ii) Contacto;
iii) Departamento.

d) Os dispositivos físicos e sistemas devem ser classificados de acordo com a sua criticidade para a entidade.

2.2 — A entidade deve elaborar o inventário de todas as suas aplicações, identificando:

a) Informação necessária ao inventário de uma aplicação, nomeadamente:

i) Nome do software;
ii) Versão;
iii) Fabricante.

b) Os responsáveis pelas aplicações com, pelo menos, os seguintes elementos:

i) Nome;
ii) Contacto;
iii) Departamento.

c) A classificação em função da criticidade da aplicação para a entidade;
d) Quando aplicável, o tipo de contrato de suporte em vigor com o fornecedor da aplicação ou plataforma de software.

3 — Para efeitos do n.º 3 do artigo 6.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, as entidades devem comunicar ao CNCS, com base no inventário de ativos a que se refere o n.º 1 do

artigo 6.º do referido normativo, para todos os ativos diretamente acessíveis publicamente através da Internet, uma lista com a seguinte informação:

a) Serviço suportado;
b) Nome do equipamento/Nome do software;
c) Modelo/Versão;
d) Endereço IP, se aplicável;
e) Fully Qualified Domain Names (FQDNs), se aplicável;
f) Fabricante.

4 — A lista a que se refere o número anterior deve ser remetida para o endereço de correio eletrónico indicado no n.º 1 do artigo 1.º da presente Instrução, preenchendo e juntando o formulário, constante do anexo III à presente Instrução, e disponível no sítio na Internet do Centro Nacional de Cibersegurança, que deve ser descarregado após a publicação da presente Instrução.

Artigo 5.º

Relatório anual

1 — O relatório anual deve ser comunicado ao CNCS nos termos dos n.os 2 e 3 do artigo 8.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, contendo a informação referida no n.º 1 do mesmo artigo.

2 — O relatório anual deve ser remetido para o endereço de correio eletrónico indicado no n.º 1 do artigo 1.º da presente Instrução, preenchendo e juntando um ficheiro PDF, o qual deverá respeitar a estrutura constante do anexo IV à presente Instrução, e disponível no sítio na Internet do Centro Nacional de Cibersegurança, que deve ser descarregado após a publicação da presente Instrução.

Artigo 6.º

Notificações de incidentes

1 — O envio das notificações de incidentes e de informação adicional, de acordo com os termos dos artigos 11.º a 16.º do Decreto-Lei n.º 65/2021, de 30 de julho de 2021, com produção de efeitos prevista no n.º 2 do artigo 23.º, deve ser realizado através do sítio na Internet do Centro Nacional de Cibersegurança (https://www.cncs.gov.pt) na funcionalidade «Notificação de Incidentes», mediante o preenchimento do modelo de reporte estabelecido para o efeito, ou via API (application programming interface) disponibilizada pelo CNCS para o efeito.

2 — Nos casos em que a entidade em resultado do incidente ou por outro motivo de natureza eminentemente técnica devidamente justificado, não tem temporariamente capacidade operacional para assegurar a notificação no sítio na Internet do Centro Nacional de Cibersegurança, ou nos casos em que o mesmo esteja indisponível, a notificação poderá ser efetuada, a título excecional, através:

a) De correio eletrónico remetido para o seguinte endereço: cert@cert.pt;
b) Por telefone através do número (+351) 210 497 399;
c) Por telefone através do número (+351) 910 599 284, em disponibilidade contínua (24 horas por dia e sete dias por semana).

3 — Caso as entidades pretendam enviar a notificação protegida por método criptográfico, podem proteger a informação utilizando a chave pública de PGP, associada ao endereço de correio eletrónico referido na alínea *a*) do número anterior, publicada no sítio na Internet do CNCS.

4 — O CNCS mantém e gere a informação recebida nos números anteriores, num sistema de informação seguro em conformidade com as disposições respeitantes à segurança de matérias classificadas com o grau de segurança Reservado na marca Nacional, salvo quando necessário grau de segurança superior.

ANEXO I

(a que se refere o artigo 2.º)

Ponto de contacto permanente

Nome da entidade	Nome do ponto ou pontos de contacto permanente/ serviço disponível ou equipa operacional	Endereço de correio eletrónico principal	Endereço de correio eletrónico alternativo	Número de telefone fixo principal (se aplicável)	Número de telefone móvel principal	Número de telefone fixo alternativo (se aplicável)	Número de telefone móvel alternativo	Outros contactos alternativos

ANEXO II

(a que se refere o artigo 3.º)

Responsável de segurança

Nome da entidade	Nome do responsável de segurança	Cargo do responsável de segurança	Endereço de correio eletrónico	Número de telefone fixo (se aplicável)	Número de telefone móvel

ANEXO III

(a que se refere o artigo 4.º)

Lista de ativos

Serviço Suportado	Nome do equipamento/ Nome do software	Modelo/Versão	Endereço IP (se aplicável)	FQDN (se aplicável)	Fabricante

ANEXO IV

(a que se refere o artigo 5.º)

Relatório anual

1 — Designação da entidade:

2 — Ano civil e período de tempo do relatório:

3 — Descrição sumária das principais atividades desenvolvidas em matéria de segurança das redes e dos serviços de informação:

4 — Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes:

5 — Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:

5.1 — Número de utilizadores afetados pela perturbação do serviço

5.2 — Duração dos incidentes

5.3 — Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço

6 — Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação:

7 — Problemas identificados e medidas implementadas na sequência dos incidentes:

8 — Qualquer outra informação relevante:

Data:

Responsável de segurança:

Assinatura do Responsável de segurança:

314959368