PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

Centro Nacional de Cibersegurança

Aviso n.º 1517/2024

Sumário: Projeto de regulamento relativo à implementação do regime jurídico da segurança do ciberespaço nas entidades da Administração Pública.

Projeto de regulamento relativo à implementação do Regime Jurídico da Segurança do Ciberespaço nas entidades da Administração Pública

Nos termos e em cumprimento das disposições conjugadas do artigo 101.º do Código do Procedimento Administrativo 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 4 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 14083/2022, de 7 de dezembro, do diretor-geral do Gabinete Nacional de Segurança, publicado no *Diário da República,* 2.ª série, de 7 de dezembro de 2022, aprovo o projeto de regulamento relativo à implementação do Regime Jurídico da Segurança do Ciberespaço nas entidades da Administração Pública, aqui submetido a consulta pública juntamente com a sua nota justificativa, para recolha de sugestões, procedendo-se, para o efeito, à publicação de aviso na 2.ª série do *Diário da República* e à difusão na página do Centro Nacional de Cibersegurança na internet.

Para a versão que se apresenta agora a consulta pública foi solicitado parecer prévio às entidades representadas no Conselho para as Tecnologias de Informação e Comunicação na Administração Pública e foi promovida a audição, nos termos do n.º 100 do Código do Procedimento Administrativo. da Associação Nacional de Municípios Portugueses e da Associação Nacional de Freguesias.

Assim, para os efeitos previstos no artigo 101.º do Código do Procedimento Administrativo, se submete o presente projeto de regulamento a consulta pública, a decorrer pelo período de 30 dias, mediante publicação no sítio institucional do Centro Nacional de Cibersegurança na Internet e na 2.ª série do *Diário da República.*

Neste contexto, solicita-se aos interessados que enviem os respetivos contributos, por escrito e em língua portuguesa, preferencialmente por correio eletrónico para o endereço: drsc@cncs.gov.pt.

Encerrada a consulta pública, o Centro Nacional de Cibersegurança procederá à apreciação dos contributos apresentados pelos interessados e disponibilizará um relatório contendo referência a todos os contributos recebidos, bem como uma apreciação global que reflita o entendimento sobre os mesmos e os fundamentos das opções tomadas.

14 de dezembro de 2023. — O Coordenador do Centro Nacional de Cibersegurança, *José Lino Alves dos Santos.*

Nota justificativa

A segurança das redes e sistemas de informação tem um papel fundamental para o regular funcionamento do Estado, bem como para a confiança dos cidadãos no processo de transformação digital da Administração Pública. Perante um cenário de ameaças crescentes e cada vez mais diversificadas, e a tendência para o crescente aumento da dependência das tecnologias da informação e de comunicação nas entidades públicas, torna-se essencial que estas integrem a cibersegurança na sua cultura organizacional como uma componente intrínseca à sua atividade.

A importância da segurança das redes e sistemas de informação na Administração Pública foi novamente reconhecida, e reforçada, pela Diretiva (UE) 2022/2555 do Parlamento Europeu e do

Conselho, de 14 de dezembro de 2022, relativa a medidas a garantir um elevado nível comum de cibersegurança na União (Diretiva SRI 2), com a inclusão das entidades da Administração Pública no seu âmbito de aplicação. No entanto, a Lei n.º 46/2018, de 13 de agosto, que 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 da informação em toda a União, já incluiu no seu âmbito de aplicação, além dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais, as entidades que integram a Administração Pública, nomeadamente o Estado, as regiões autónomas, as autarquias locais, as entidades administrativas independentes, os institutos públicos, as empresas públicas e as associações públicas.

O regime jurídico da segurança do ciberespaço foi objeto, de acordo com o artigo 31.º da Lei n.º 46/2018, de 13 de agosto, de legislação complementar, através do Decreto-Lei n.º 65/2021, de 30 de julho, que definiu os requisitos de segurança das redes e sistemas de informação e as regras de notificação de incidentes que devem ser cumpridos pelas entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, e 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. Este decreto-lei foi objeto de regulamentação complementar, de acordo com o seu artigo 19.º e nos termos do n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, através do Regulamento n.º 183/2022, de 21 de fevereiro, que configura instrução técnica relativa a comunicações entre as entidades e o Centro Nacional de Cibersegurança, nomeadamente no que diz respeito à informação referente a pontos de contacto permanente, responsáveis de segurança, inventário de ativos, relatório anual e notificação de incidentes.

Atendendo à diversidade dos vários órgãos e serviços que integram a estrutura da Administração Pública, que variam relativamente à sua dimensão e complexidade organizacional e interesses públicos distintos que prosseguem, seja a nível nacional, regional ou local, não se considera razoável, proporcional e eficaz para aumentar a maturidade e resiliência digital, exigir os mesmos requisitos de segurança das redes e sistemas de informação a todas as entidades da Administração Pública, independentemente das suas características ou do impacto potencial de um incidente de cibersegurança nos seus serviços. Atendendo às especificidades das diferentes entidades públicas, o presente projeto de regulamento estabelece, assim, nos termos do n.º 7 do artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho, as condições específicas para o cumprimento de requisitos de segurança das redes e sistemas de informação por parte das entidades da Administração Pública, em termos proporcionais e adequados à sua dimensão ou complexidade organizacional. Este regulamento tem ainda em linha de conta o disposto na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, em relação à Administração Pública, com vista à transposição desta diretiva na ordem jurídica nacional.

O presente projeto de regulamento define os critérios que delimitam o universo das entidades da Administração Pública que devem cumprir com os requisitos de segurança das redes e sistemas de informação previstas no Artigo 14.º, n.º 1 da Lei n.º 46/2018, de 13 de agosto, nomeadamente referentes às medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, e reguladas no DecretoLei n.º 65/2021, de 30 de julho, nomeadamente referentes ao pontos de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e análise de risco.

Os critérios aqui definidos têm em conta a dimensão e a complexidade organizacional, e a caracterização das entidades tendo como base o tipo organizacional a que pertencem os diferentes órgãos e serviços que integram a Administração Pública, tendo por base a classificação do Sistema de Informação da Organização do Estado (SIOE), da Direção-Geral da Administração e do Emprego Público, na ótica de pesquisa da AP Jurídica. Foi ainda tido em conta as particularidades daqueles que têm como missão prestar um conjunto de serviços nas áreas do desenvolvimento, manutenção e gestão de infraestruturas de tecnologias de informação e comunicação e daqueles que, apesar de não prestarem serviços nestas áreas, apresentam um grau particularmente elevado de integração digital na prestação dos seus serviços, incluindo o armazenamento e gestão de informações sensíveis e dados pessoais.

Atendendo ao elevado grau de exigência das obrigações previstas no Decreto-Lei n.º 65/2021 de 30 de julho e medidas técnicas e organizativas que devem ser tidos em conta na gestão dos riscos que se colocam a tais redes e sistemas e que resultem, nomeadamente, do Quadro Nacional de Referência para a Cibersegurança (QNRCS) considerou-se necessário definir requisitos de segurança das redes e sistemas em termos mais adequados e proporcionais à dimensão e complexidade organizacional das entidades da Administração Pública. Nesse sentido, o presente projeto de regulamento vem definir requisitos de segurança em linha com as medidas de segurança constantes no referencial do esquema de certificação Maturidade Digital — Selo Digital, na dimensão de cibersegurança. Por este último se destinar à promoção da consciencialização e proteção perante os riscos mais comuns e prejudiciais à cibersegurança de entidades públicas e privadas, de diferentes tipologias e dimensões, considerou-se adequado e proporcional incluir requisitos equivalentes aos exigidos para a certificação nos níveis Prata e Bronze para guiarem a maioria das entidades da Administração Pública na prevenção e mitigação dos riscos de cibersegurança.

Projeto de regulamento relativo à implementação do Regime Jurídico da Segurança do Ciberespaço nas entidades da Administração Pública

Artigo 1.º

Objeto

O presente regulamento procede à implementação do Regime Jurídico da Segurança do Ciberespaço nas entidades da Administração Pública definindo, em termos proporcionais e adequados, de acordo com o n.º 7 do artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho, os requisitos específicos de segurança e de notificação de incidentes que devem ser cumpridos.

Artigo 2.º

Âmbito de aplicação

1 — O presente regulamento aplica-se às entidades que integram a Administração Pública, como exigido pelo n.º 2 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, sem prejuízo do disposto no n.º 5 do artigo 2.º da mesma lei, para efeitos do disposto no n.º 1 do mesmo artigo, e de acordo com os seguintes grupos:

a) Pertencem ao grupo A, as entidades da Administração Pública que tenham como missão prestar 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 e que, em ambos os casos, tenham sido notificadas pelo CNCS para este efeito, no seguimento do parecer prévio do Conselho Superior de Segurança do Ciberespaço.

b) Pertencem ao grupos B as entidades da Administração Pública que se enquadrem numa das tipologias organizacionais referidas nas listas constantes no anexo I assim como aquelas que preencham os seguintes critérios:

i) Entidades referidas na alínea *c*) do n.º 2 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, referente às autarquias locais, com 250 ou mais trabalhadores;

ii) Entidades referidas na alínea *f*) do n.º 2 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, referente às empresas públicas, que tenham 250 ou mais trabalhadores ou com volume de negócios anual superior a 50 milhões de euros, ou cujo balanço total anual excede 43 milhões de euros.

c) Pertencem ao grupo C as entidades da Administração Pública que se enquadrem numa das tipologias referidas nas listas constantes no anexo I e tenham pelos menos 50 trabalhadores, assim como aquelas que preencham os seguintes critérios:

i) Entidades referidas na alínea *c*) do n.º 2 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, referente às autarquias locais, com pelos menos 50 trabalhadores no seu quadro de pessoal;

ii) Entidades referidas na alínea *f*) do n.º 2 do artigo 2.º da Lei n.º 46/2018, de 13 de agosto, referente às empresas públicas, que tenham entre 50 e 249 trabalhadores no seu quadro de pessoal e volume de negócios anual igual ou inferior a 50 milhões de euros, ou balanço total anual igual ou inferior a 43 milhões de euros.

2 — De forma justificada e mediante notificação, pode o CNCS determinar, após parecer do Conselho Superior de Segurança do Ciberespaço, que qualquer entidade da Administração Pública tem de cumprir com requisitos de segurança diferentes daqueles previstos para o grupo onde se enquadram e independentemente da sua tipologia organizacional.

Artigo 3.º

Definição dos requisitos de segurança

1 — As entidades da Administração Pública que se enquadrem no grupo A devem cumprir com as obrigações e os requisitos de segurança das redes e sistemas de informação previstos no Decreto-Lei n.º 65/2021 de 30 de julho, tendo em conta as normas técnicas do Quadro Nacional de Referência para a Cibersegurança, comunicados nos termos do disposto no Regulamento n.º 183/2022, de 21 de fevereiro, quando aplicável.

2 — As entidades da Administração Pública que se enquadrem no grupo B devem cumprir com os requisitos de segurança das redes e sistemas de informação constantes no anexo II e III do presente regulamento, de forma cumulativa.

3 — As entidades da Administração Pública que se enquadrem no grupo C devem cumprir com os requisitos de segurança das redes e sistemas de informação constantes no anexo III do presente regulamento.

4 — As entidades da Administração Pública que não se enquadrem em qualquer dos grupos referidos devem adotar medidas técnicas e organizativas destinadas a promoverem um nível de cibersegurança que seja adequado e proporcional à sua dimensão.

5 — As entidades que se enquadrem nos Grupos B e C devem elaborar e manter atualizado um documento que evidencie a implementação dos requisitos de segurança estabelecidos nos anexos II e III do presente regulamento.

6 — A obtenção voluntária de certificados nos níveis Prata ou Bronze do Documento Normativo Português — Especificação Técnica (DNP TS) 4577-1:2021, Maturidade Digital — Selo Digital, por parte das entidades que se enquadrem no grupos B ou C, respetivamente, atesta o cumprimento dos requisitos de segurança.

7 — O disposto no presente regulamento não impede as entidades da Administração Pública de adotarem requisitos de segurança mais exigentes.

Artigo 4.º

Notificação de incidentes

1 — Aplicam-se às entidades enquadradas nos grupos A e B as obrigações de notificação de incidentes de segurança previstas nos termos dos artigos 11.º, 12.º, 13.º, 14.º, 15.º e 16.º do Decreto-Lei n.º 65/2021, de 30 de julho, e comunicadas ao Centro Nacional de Cibersegurança de acordo com o artigo 6.º do Regulamento n.º 183/2022, de 21 de fevereiro de 2022.

2 — A notificação de incidentes de segurança é voluntária para as demais entidades da Administração Pública.

Artigo 5.º

Entrada em vigor

O presente regulamento entra em vigor no dia seguinte à data da respetiva publicação no *Diário da República.*

ANEXO I

Distribuição das entidades da Administração Pública

(tipologia com base na caracterização das entidades da Administração Pública utilizada pelo Sistema de Informação da Organização do Estado, na ótica de pesquisa da AP Jurídica)

Grupo B

Agrupamento de Centros de Saúde
Área Metropolitana
Associação de Freguesias
Comunidade intermunicipal
Entidade Administrativa Independente
Inspeção Regional
Serviço Municipalizado

Grupo C

Agrupamento Complementar de Empresas
Associação
Associações de Municípios de fins específicos
Centros de Formação Profissional
Direção Regional
Direção-Geral
Entidade Regional de Turismo
Fundação
Inspeção-Geral
Instituto Público
Secretaria-Geral

ANEXO II

Requisitos de segurança aplicáveis às entidades no grupo B

Requisitos de segurança	Definição
Política de palavra-passe	Definir uma política de palavra-passe de acordo com as melhores práticas de segurança que contenha, pelos menos, os requisitos relativos à dimensão e complexidade, o prazo para alteração regular e os mecanismos técnicos a implementar de modo a garantir a sua execução.
Política de acessos e permissões	Elaborar e implementar um processo de gestão de acessos e permissões aos principais sistemas e aplicações da organização de forma segmentada, com base nos princípios *need-toknow* e *least privilege*.
Gestão da mudança organizacional	Definir uma política que acautele a mudança organizacional ao nível das TIC, com especial incidência nas ações que devem ser executadas após a saída de um trabalhador ou da mudança das funções que lhe estão associadas.
Plano de reação a incidentes de cibersegurança	Definir um plano de reação a incidentes de cibersegurança que defina, no mínimo, as funções e responsabilidades na gestão do incidente, a notificação do incidente, e acções de mitigação e contenção.
Conformidade *Webcheck*	Assegurar a conformidade do seu domínio principal com, pelo menos, as seguintes validações da plataforma *Webcheck* (https://webcheck.pt) — nível Intermédio: HSTS, Cabeçalhos de segurança, DKIM.
Gestão da palavra-passe	Assegurar a implementação da respetiva política e garantir que as palavras-passe associadas à gestão da infraestrutura são armazenadas através de uma solução para a gestão de palavras-passe.

Requisitos de segurança	Definição
Privilégios de acesso diferenciados	Garantir que qualquer tipo de acesso atribuído bem como as permissões de administração dos sistemas, aplicações e infraestrutura são concedidas numa base de *need-to-know* e *least privilege*, e de acordo com a política definida.
Securização de configurações	Aplicar as melhores práticas de segurança e privacidade ao nível do posto de trabalho (e.g. disponibilização de TPM 2.0; garantir secureBoot UEFI; assegurar a proteção da BIOS), das configurações do sistema operativo e principais aplicações utilizadas (soluções de produtividade, browsers, etc.).
Controlo aplicacional	Aplicar mecanismos que previnam a instalação de aplicações não autorizadas por parte dos utilizadores.
Recolha e armazenamento de registos	Implementar um repositório central para registos produzidos pelos sistemas operativos e pelas aplicações de suporte à atividade da organização com um período mínimo de armazenamento de um ano. Cada servidor deve ter a capacidade de armazenar os seus próprios registos por um período mínimo de um mês.
Plano de formação	Definir e executar um plano de formação aplicável aos colaboradores com perfis técnicos da organização, visando a obtenção de conhecimentos mais avançados sobre cibersegurança.

ANEXO III

Requisitos de segurança aplicáveis às entidades nos grupos B e C

Requisitos de segurança	Definição
Identificação de funções ou atividades críticas	Garantir uma identificação completa e atualizada de funções ou atividades críticas, e respetiva dependência das Tecnologias da Informação e Comunicação.
Inventariação dos ativos e documentação da arquitetura de comunicações de dados.	Inventariação completa dos ativos (*hardware* e *software*) e elaboração de um mapa com a arquitetura de rede e informação relevante associada. Garantir a atualização regular desta informação.
Política de Utilização Aceitável das Tecnologias de Informação e Comunicação.	Elaborar um documento que estabelece os princípios orientadores da utilização adequada das redes e sistemas de informação da organização destinado aos colaboradores com acesso aos mesmos.
Ponto de contacto para a cibersegurança	Designar um ponto de contacto do ponto de vista técnico/operacional que deve ser capaz de responder a solicitações externas, sendo esperada disponibilidade para contactos de emergência fora do horário de expediente.
Cópias de segurança	Implementar uma política de cópias de segurança e assegurar que os dados da organização são salvaguardados automática e regularmente através de uma plataforma de cópias de segurança.
Atualizações de segurança	Configurar e garantir a atualização automática dos sistemas operativos e aplicações em todos os postos de trabalho da organização.
Proteção dos postos de trabalho	Garantir a existência de proteção contra ciberameaças em todos os postos de trabalho e dispositivos móveis da organização.
Proteção perimetral e da infraestrutura	Garantir a proteção perimetral da infraestrutura, através de um dispositivo com mecanismos de *firewall*, e a aplicação de boas práticas na sua configuração (p. ex. segmentação de redes). Ativar, em todos os dispositivos, a proteção por palavra-passe e alterar a que se encontra definida por omissão em todos os equipamentos que se encontrem expostos na internet. A segurança física dos principais componentes da infraestrutura deve ser igualmente assegurada.
Conformidade *Webcheck*	Assegurar a conformidade do seu domínio principal com, pelo menos, as seguintes validações da plataforma *Webcheck* (https://webcheck.pt) — nível Inicial: Ligação HTTP/S, Certificado Digital, SPF.
Autenticação multifator	Ativar a autenticação multifator em todas as aplicações críticas para a organização, sempre que a opção esteja disponível.

Requisitos de segurança	Definição
Plano de sensibilização	Definir e executar um plano de formação e sensibilização aplicável a todos os colaboradores da organização, visando a obtenção de conhecimentos fundamentais de ciberhigiene, ciberameaças e respetivos canais de reporte das mesmas, assim como das políticas de segurança da organização.
Fontes de informação e canais de comunicação	Definir um plano de acompanhamento regular de fontes de informação de modo a acompanhar o aparecimento e evolução das ameaças à segurança de informação.

317227618