CONSULTA PÚBLICA DO REGIME DE SEGURANÇA DO CIBERESPAÇO NA ADMINISTRAÇÃO PÚBLICA

Este Projeto, atualmente em consulta pública, visa estabelecer condições específicas para o cumprimento de requisitos de segurança das redes e sistemas de informação pela Administração Pública, cujas entidades, dependendo do grupo onde se inserem, ficarão sujeitas ao cumprimento de um conjunto de obrigações e requisitos específicos.

O Projeto relativo à implementação do Regime Jurídico da Segurança do Ciberespaço nas entidades da Administração Pública encontra-se em consulta pública até ao dia 5 de março.

Este Projeto visa estabelecer 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. Para tal, as entidades que integram a Administração Pública estão divididas em Grupos aos quais se aplicam diferentes requisitos. Destacamos os seguintes:

- O Grupo A é composto por entidades que prestem serviços nas áreas do desenvolvimento, manutenção e gestão de infraestruturas de tecnologias de informação e comunicação ou que apresentem um grau particularmente elevado de integração digital na prestação dos seus serviços (depende sempre de notificação à entidade e parecer prévio do Conselho Superior de Segurança no Ciberespaço) devem cumprir com as obrigações e requisitos previstos no Decreto-Lei n.º 65/2021, de 30 de julho.
- O Grupo B é composto por: Agrupamentos de Centros de Saúde, Áreas Metropolitanas, Associações de Freguesias, Comunidades Intermunicipais, Entidades Administrativas Independentes, Inspeções Regionais e Serviços Municipalizados. Estas entidades devem: elaborar e implementar uma política de acessos e permissões; definir uma política que acautele a mudança organizacional ao nível das TIC; definir um plano de reação de incidentes de cibersegurança; verificar a sua conformidade a nível de *Webcheck*; implementar uma solução para gestão de palavras-passe; aplicar mecanismos de controlo de instalação de aplicações; e cumprir com os requisitos aplicáveis ao Grupo C (*infra*).
- O Grupo C é composto por Agrupamentos Complementares de Empresas, Associações, Associações de Municípios de fins específicos, Centros de Formação Profissional, Direções Regionais, Direções-Gerais, Entidades Regionais de Turismo, Fundações, Inspeções-Gerais, Institutos Públicos e Secretarias-Gerais. Estas entidades devem: identificar as funções ou atividades críticas e a sua dependência das TIC; fazer um inventário dos ativos e documentação da arquitetura e comunicação de dados; implementar uma política de cópias de segurança; garantir a atualização automático dos sistemas operativos bem como a existência de proteção contra ciberameaças de todos os postos de trabalho; garantir a proteção perimetral da infraestrutura através de *firewall*; ativar a autenticação multifator em todas as aplicações; definir e executar um plano de formação e sensibilização aplicável a todos os colaboradores da organização e definir um plano de acompanhamento regular de

CONTACTOS

CLÁUDIA FERNANDES MARTINS
CMARTINS@MACEDOVITORINO.COM

MARIA HELENA CÔRTES
MCORTES@MACEDOVITORINO.COM

fontes de informação de modo a acompanhar a evolução das ameaças à segurança da informação.

As entidades que se enquadrem nos Grupos B e C devem ainda elaborar e manter atualizado um documento que evidencie a implementação dos requisitos de segurança referidos *supra*.

Os interessados devem enviar os seus contributos por escrito para o e-mail drsc@cncs.gov.pt até ao dia 5 de março de 2024.

Após a consulta pública, o Centro Nacional de Cibersegurança vai publicar um relatório fazendo referência a todos os contributos, bem como ao seu entendimento e fundamento relativamente às opções tomadas.