Recomendação do Conselho de Prevenção da Corrupção

SOBRE

Boas Práticas de Cibersegurança

Considerando a relevância de garantir um elevado nível comum de segurança das redes e dos sistemas de informação para o regular funcionamento das entidades e órgãos da Administração Pública, protegendo-as contra os ataques que coloquem em causa a confidencialidade, integridade e disponibilidade da informação e respetivos serviços, o Conselho de Prevenção da Corrupção sublinha a importância da implementação das melhores práticas de cibersegurança, bem como a sua manutenção e atualização. De facto, o ciberespaço é uma realidade dinâmica e fluida, em permanente mutação, colocando desafios de alcance transnacional e que atravessa vários setores de atividade.

Pese embora a consagração de um Regime Jurídico da Segurança do Ciberespaço, os requisitos previstos no Decreto-Lei n.º 65/2021, de 30 de julho, constituem um mínimo obrigatório a assegurar pelas entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, não obstante as referências e as ferramentas disponibilizadas pelo Centro Nacional de Cibersegurança, enquanto Autoridade Nacional de Cibersegurança, como o Quadro Nacional de Referência para a Cibersegurança, o Quadro de Avaliação de Capacidades de Cibersegurança, o CiberCheckUp e o Roteiro para Capacidades Mínimas de Cibersegurança.

Deste modo, torna-se necessário e oportuno, que os órgãos e as entidades adotem medidas de reforço e adequação, mantendo uma comunicação estreita entre elas, e promovendo a sensibilização para o papel fundamental que os recursos humanos têm no processo.

Nestes termos, ao abrigo do artigo 2.º da Lei n.º 54/2008, de 4 de setembro, o Conselho de Prevenção da Corrupção delibera recomendar a todos os órgãos e entidades públicas e a todas as demais entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, que:

1. Promovam ações de formação e sensibilização em programas de Cibersegurança já disponíveis ou criando programas próprios, para os recursos humanos em geral, e para os seus dirigentes.

2. Reúnam os meios técnicos adequados para garantir um elevado nível de Cibersegurança, dando cumprimento ao estabelecido no Decreto-Lei n.º 65/2021, de 30 de julho, e no Regulamento n.º 183/2022, de 21 de fevereiro, nomeadamente:
    a) Implementação de mecanismos adequados de governação, risco e *compliance*;
    b) Elaboração de um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, mantendo-o permanentemente atualizado;
    c) Elaboração de um Relatório anual, assinado pelo Responsável de segurança;
    d) Elaboração de um inventário de todos os ativos essenciais para a prestação dos respetivos serviços, mantendo-o permanentemente atualizado;
    e) Cumprimento das medidas técnicas e organizativas destinadas a gerir os riscos que se colocam à segurança das redes, e dos sistemas de informação que utilizam;
    f) Realização de 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, ainda, aos ativos que garantam a prestação dos serviços;
    g) Implementação dos necessários controlos de prevenção, deteção e investigação;
    h) Notificação ao CNCS da ocorrência de incidentes com impacto relevante ou substancial.
3. Reforcem a articulação das medidas de Cibersegurança aplicadas, tendo em vista a partilha das melhores práticas, bem como os casos de sucesso e as fragilidades na implementação das mesmas, privilegiando as Recomendações de Cibersegurança já existentes para as entidades públicas, designadamente:

a) Desenvolver e planificar um plano de resposta a incidentes;

b) Verificar o acesso que os colaboradores têm na organização e as permissões que podem representar um risco para a entidade, o que inclui ativar a autenticação por dois fatores;

c) Manter o *software* atualizado com as últimas atualizações de segurança consideradas, dando prioridade às novas vulnerabilidades identificadas;

d) Verificar se os mecanismos de cópias de segurança e recuperação estão a funcionar corretamente;

e) Assegurar a formação dos colaboradores dedicados à proteção dos ativos de informação, na identificação de eventuais ameaças ou comportamentos anormais na rede;

f) Caso sejam prestados serviços de informação a outras entidades, recomenda-se a monitorização e inspeção do tráfego da rede dessas organizações e dos controlos de acesso às mesmas;

g) É recomendável, ainda, o conhecimento permanente das recentes ameaças que estão a ser levadas a cabo.

4. Assegurem o conhecimento especializado necessário, através de ações de formação especializadas dos seus trabalhadores afetos a esta área, nomeadamente do Responsável de Segurança e do Ponto de Contacto Permanente, competindo ao Responsável de Segurança:

   a) Assegurar a definição, implementação e manutenção da estratégia de Segurança da Informação e Cibersegurança de forma holística e estruturada;

   b) Garantir a conformidade com a legislação e regulamentação aplicável, como o Regime Jurídico de Segurança do Ciberespaço e Regulamento Geral de Proteção de Dados;

   c) Conhecer e garantir a implementação de boas práticas de Segurança da Informação e Cibersegurança, como o "Quadro Nacional de Referência para a Cibersegurança" e "ISO/IEC 27001";

d) Definir e identificar requisitos e medidas de Segurança da Informação e Cibersegurança;
e) Assegurar o desenvolvimento e implementação de políticas, processos e procedimentos de Segurança da Informação e Cibersegurança;
f) Definir e implementar estratégias de avaliação e de resposta aos riscos;
g) Acompanhar e avaliar a execução nomeadamente dos processos de Gestão de Alterações e de Gestão de Incidentes;
h) Acompanhar auditorias de Segurança da Informação e Cibersegurança e garantir a implementação de ações de melhoria para mitigação do risco;
i) Alinhar as opções estratégicas gerais da instituição com a estratégia e atividades de suporte de TI, nomeadamente no que se refere à definição, aquisição e implementação de soluções de TI e sua integração nos processos de negócios, incluindo necessariamente a segurança, a monitorização de desempenho e conformidade;
j) Garantir que os utilizadores das informações mais relevantes têm a formação específica e o conhecimento necessário para proteger as entidades das tentativas de ataque.

Publique-se na 2.ª Série do *Diário da República*

Lisboa, 1 de abril de 2022

José F.F. Tavares
(Presidente do TdC e do CPC)

Fernando Oliveira Silva

(Diretor-Geral do TdC e Secretário-Geral do CPC)

António Ferreira dos Santos

(Inspetor-Geral de Finanças)

João Rolo

(Secretário-Geral do Ministério da Economia e do Mar)

Orlando Soares Romano

(Procurador-Geral Adjunto)

Pedro Tenreiro Biscaia

(Advogado)

João Amaral Tomaz

(Economista)