RECOMENDAÇÃO DO CPC SOBRE BOAS PRÁTICAS DE CIBERSEGURANÇA

O Conselho de Prevenção da Corrupção ("CPC") emite recomendação sobre boas práticas de cibersegurança dirigida à Administração Pública por forma a reforçar a proteção das redes contra ataques informáticos.

O Conselho de Prevenção da Corrupção ("**CPC**"), entidade que funciona junto do Tribunal de Contas, aprovou recentemente uma Recomendação sobre Boas Práticas de Cibersegurança, dirigida às entidades e órgãos da Administração Pública, alertando para a necessidade de proteção das redes contra ataques informáticos que ponham em causa a confidencialidade, integridade e a disponibilidade da informação e respetivos serviços.

Reconhecendo a importância da implementação das melhores e mais atualizadas práticas de cibersegurança, bem como o papel fundamental dos recursos humanos na sua adoção, todos os órgãos e entidades públicas e demais entidades abrangidas pelo Regime Jurídico da Segurança do Ciberespaço devem adotar, entre outras, as seguintes recomendações:

(i) Promoção de ações de formação e sensibilização em programas de Cibersegurança;

(ii) Realização de uma análise dos riscos envolvidos no funcionamento das redes e dos sistemas de informação utilizados e adoção de mecanismos adequados de governação e "compliance";

(iii) Elaboração de um plano de segurança e de um relatório anual, assinados pelo Responsável de Segurança, bem como de um inventário de todos os ativos essenciais para a prestação dos respetivos serviços; e

(iv) Notificação ao Centro Nacional de Cibersegurança ("**CNCS**") de incidentes com impacto relevante ou substancial.

Quanto às medidas de cibersegurança em curso, o CPC sublinha a necessidade de:

(i) Assegurar a formação e verificar o acesso dos colaboradores na organização, de modo a determinar em que medida estas permissões podem representar um risco para a entidade;

(ii) Manter o "software" atualizado com as últimas atualizações de segurança e garantir o correto funcionamento dos mecanismos de cópias de segurança e recuperação; e

(iii) No caso de prestação de informação a outras entidades, monitorizar a inspeção do tráfego da rede dessas organizações e dos respetivos controlos de acesso.

O CPC entendeu ainda ser conveniente reforçar as funções do Responsável de Segurança no âmbito da gestão das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes. O Responsável de Segurança deverá, designadamente, (i) garantir a conformidade com a legislação e regulamentação aplicável (incluindo o RGPD), e (ii) acompanhar auditorias de Segurança da Informação e Cibersegurança.

CONTACTOS

CLÁUDIA FERNANDES MARTINS
CMARTINS@MACEDOVITORINO.COM

DÉBORA DUTRA
DDUTRA@MACEDOVITORINO.COM