SEGURANÇA DIGITAL

DEZ REGRAS DE OURO PARA A SEGURANÇA DA INFORMAÇÃO

O grupo IT4Legal detalhou dez regras de segurança de informação que os advogados devem respeitar. Aqui ficam.

1 Mantenha a informação sujeita a segredo profissional em local seguro, de acesso reservado (nunca deixe documentos em papel ou equipamentos informáticos com informação sujeita a segredo profissional em local onde um terceiro possa aceder livremente).

2 Utilize conta de correio electrónico autónoma para as mensagens profissionais e uma outra conta distinta para fins privados (não misture mensagens profissionais com privadas nas contas de correio). Seleccione cuidadosamente os fornecedores de serviços de correio electrónico, alojamento de dados e outros, analisando cuidadosamente as condições contratuais aplicáveis (tenha especial atenção à jurisdição onde serão alojados os dados sujeitos a segredo profissional, bem como às regras de confidencialidade da caixa de correio).

3 Evite alojar dados sujeitos a segredo profissional em dispositivos móveis (utilize-os só quando estritamente necessário). Se porventura tiver dados sujeitos a segrego profissional em dispositivos móveis, evite deixá-los em locais propensos a furtos (por exemplo, automóvel). Procure utilizar sempre mecanismos de bloqueio/encriptação dos dados guardados em dispositivos móveis (ou amovíveis).

4 Sempre que alojar dados sujeitos a segredo profissional em serviços de Cloud deve assegurar que a entidade prestadora do serviço respeita as regras de confidencialidade, privacidade e propriedade da informação bem como respeite os artigos 70º e 71º do estatuto da Ordem dos Advogados.

5 O acesso a computadores que contenham informação sujeita a segredo profissional deve estar protegida por passwords com um nível de segurança mínimo (pelo menos, 9 caracteres, idealmente dois níveis de autenticação), devendo activar o bloqueio de password sempre que se ausentar do posto de trabalho.

6 Não divulgue na Internet informação sujeita a segredo profissional (em especial, tenha em consideração a natureza pública das redes sociais).

7 Evite aceder a sítios da Internet desconhecidos ou fazer downloads de ficheiros desconhecidos através do dispositivo onde aloje dados sujeitos a segredo profissional, nem utilize redes sem fios desconhecidas ou públicas e não deixe a sua rede sem fios desprotegida (o acesso deve ser restrito).

8 Utilize sempre mecanismos de anti-vírus, anti-spyware, anti-malware e firewall actualizados.

9 Não divulgue a terceiros a sua password, nem dissemine por terceiros o certificado digital emitido pela Ordem dos Advogados para uso profissional. Nunca revele dados pessoais e privados por e-mail (senhas, códigos de cartões de crédito e outros).

10 Assegure-se que as empresas que prestam serviços informáticos possuem seguro de responsabilidade civil e que os funcionários estão sujeitos a cláusulas de confidencialidade.