NOTA
INFORMATIVA

PLMJ
ADVOGADOS, SP, RL

50 ANOS
Consigo.

TELECOMUNICAÇÕES, MEDIA E TECNOLOGIAS DE INFORMAÇÃO

REGIME JURÍDICO DA SEGURANÇA DO CIBERESPAÇO

O Regime Jurídico da Segurança do Ciberespaço estabelece a Estrutura de segurança do ciberespaço, e vem exigir o cumprimento de requisitos de segurança e obrigações de notificação de incidentes e aplica-se a entidades públicas e privadas.

Foi publicada a Lei n.º 46/2018 de 13 de agosto, que aprova o **Regime Jurídico da Segurança do Ciberespaço** ("RJSC"), 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 informação em toda a União.

O Regime Jurídico da Segurança do Ciberespaço estabelece a Estrutura de segurança do ciberespaço, e vem exigir o cumprimento de **requisitos de segurança e obrigações de notificação de incidentes**, ao Centro Nacional de Cibersegurança, sempre que se esteja perante um incidente com impacto relevante ou substancial nas redes e sistemas de informação.

O RJSC aplica-se:

- Administração Pública;
- Operadores de infraestruturas críticas;
- Operadores de serviços essenciais;
- Prestadores de serviços digitais, cuja sede se situe em território nacional, e que prestem (i) serviços de mercado em linha, (ii) serviços de motor de pesquisa em linha e (iii) serviços de computação em nuvem;
- Quaisquer outras entidades que utilizem redes e sistemas de informação.

Este diploma vem exigir a estas entidades a observância de **requisitos de segurança** que implicam o cumprimento de 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.

Relativamente aos Prestadores de serviços digitais, para que assegurem um nível de segurança adequado ao risco que se coloca à segurança das redes e dos sistemas de informação que utilizam, no contexto da oferta dos serviços digitais, a nova Lei impõe que sejam considerados os seguintes fatores: (i) segurança dos sistemas e das instalações, (ii) tratamento dos incidentes, (iii) gestão da continuidade das atividades, (iv) acompanhamento, a auditoria e os testes realizados e, (v) conformidade com as normas internacionais.

O diploma implica o cumprimento de medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação.

FUNDAÇÃO PLMJ

ANDRÉ PRÍNCIPE
S/ Título da série Tunnels, 2005
Prova de branqueamento de corante
66 x 100 cm
Obra da Colecção da Fundação PLMJ

Já quanto à obrigação de **notificação de incidentes** ao Centro Nacional de Cibersegurança, os Prestadores de serviços digitais apenas serão obrigados a notificar um incidente quando estiverem perante um incidente com "impacto substancial" e na medida em que tiverem acesso a informação necessária para avaliar o impacto do acidente em função dos fatores acima indicados. Relativamente às restantes entidades abrangidas pelo diploma, a fim de se determinar a relevância do impacto do incidente, são tidos em conta nomeadamente, o número de utilizadores afetados, a duração do incidente e a distribuição geográfica. Exige-se também aos Prestadores de serviços digitais para além dos parâmetros atrás referidos, a avaliação do nível de gravidade da perturbação do funcionamento do serviço, e a extensão do impacto nas atividades económicas e societais.

Prevê-se ainda a possibilidade de quaisquer entidades poderem notificar voluntariamente um incidente, sempre que estejam em causa incidentes com impacto importante na continuidade dos serviços prestados.

Para efeitos de cumprimento do RJSC, **os Prestadores de serviços digitais e as entidades do setor das infraestruturas digitais (Pontos de troca de tráfego, Prestadores de serviços de Sistemas de nomes de domínio (DNS) e Registos de nomes de domínio de grupo) deverão comunicar de imediato ao Centro Nacional de Cibersegurança o exercício da respetiva atividade**, obrigação que não se aplica aos Operadores de serviços essenciais, na medida em que a iniciativa de identificação destas entidades ficou reservada ao Centro Nacional de Cibersegurança (processo que deverá ser concluído até ao próximo dia 9 de novembro de 2018). O incumprimento da obrigação de comunicação, constitui infração grave punível com coima até €9.000 no caso de se tratar de pessoas coletivas.

Os requisitos de segurança aplicáveis à Administração Pública e operadores de infraestruturas críticas, e operadores de serviços essenciais, bem como os requisitos de notificação serão objeto de desenvolvimento em sede legislação complementar, a aprovar no prazo de 150 dias seguintes à data de entrada em vigor do RJSC.

Apesar de as obrigações de implementação de medidas de segurança técnicas e organizativas e de notificação de incidentes, apenas se tornarem obrigatórias 6 (seis) meses após a publicação do RJSC, ou seja, a partir de 13 de fevereiro de 2019, as empresas devem começar desde já a planear e a criar os mecanismos internos necessários que permitam cumprir as novas exigências legais.

Prevê-se um quadro contraordenacional cuja fiscalização cabe ao Centro Nacional de Cibersegurança, podendo o valor máximo das coimas atingir os €50.000, no caso de se tratar de pessoas coletivas.

Por fim, estão excluídos do âmbito de aplicação do diploma (i) as micro e pequenas empresas, (ii) as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, (iii) Prestadores de serviços de confiança, (iv) as redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior das Forças Armadas, e (v) as redes e sistemas de informação que processem informação classificada.

Apesar de estas medidas se tornarem obrigatórias 6 meses após a publicação do RJSC, ou seja, a partir de 13 de fevereiro de 2019, as empresas devem começar desde já a planear e a criar os mecanismos internos necessários que permitam cumprir as novas exigências legais.