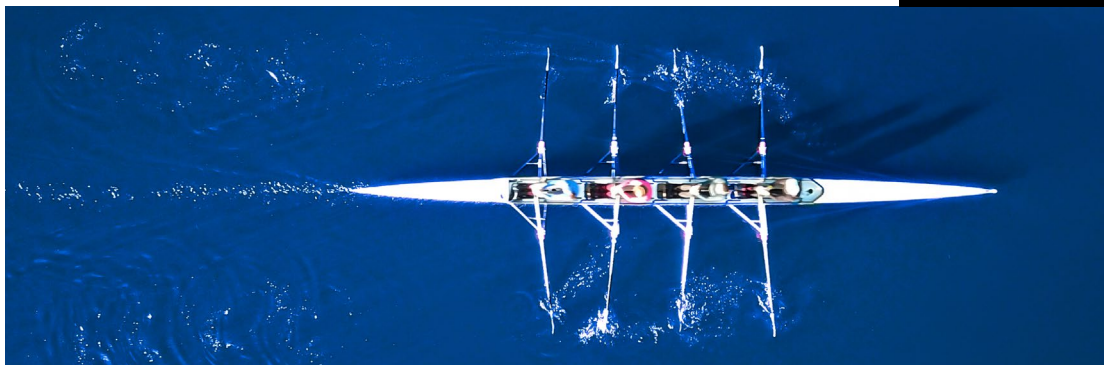




OUT. 26

ANGOLA

NEWS

TECNOLOGIA, MEDIA E COMUNICAÇÕES

Lei da Cibersegurança

Foi recentemente publicada no Diário da República a Lei n.º 9/26, de 28 de Setembro (“Lei da Cibersegurança”) que revoga integralmente a Lei n.º 7/17, de 16 de Fevereiro (Lei de Protecção das Redes e Sistemas Informáticos). A Lei estabelece o quadro jurídico aplicável à protecção dos cidadãos e das entidades públicas e privadas contra ciberameaças e ciberataques, bem como à segurança das redes, dos sistemas de informação, das infra-estruturas críticas e dos serviços essenciais do País.

Comparativamente ao regime anterior, a Lei estabelece um âmbito de aplicação significativamente mais amplo, abrangendo todas as pessoas singulares e colectivas, públicas e privadas, que utilizem ou operem no ciberespaço angolano. A sua aplicação estende-se igualmente aos actos praticados no território nacional e fora dele, sempre que estes se destinem ou produzam efeitos no ciberespaço angolano.

A aplicação da Lei estende-se igualmente aos actos praticados no território nacional e fora dele, sempre que estes se destinem ou produzam efeitos no ciberespaço angolano.

Principais Novidades

Entre as principais alterações introduzidas, destacam-se:

- i) A criação do Sistema Nacional de Cibersegurança, que é composto pelo Conselho Nacional de Cibersegurança, pelo Centro Nacional de Cibersegurança (CNC) e pela Rede Nacional de CSIRT;
- ii) A definição de categorias específicas de entidades sujeitas a obrigações de cibersegurança, incluindo operadores de infra-estruturas críticas e de serviços essenciais, prestadores de serviços digitais, comunicações electrónicas, centros de dados, *cloud* e serviços de cibersegurança;
- iii) Introdução de obrigações de gestão e avaliação de riscos cibernéticos;
- iv) Obrigação de notificação de incidentes de cibersegurança às entidades competentes;
- v) Reforço da fiscalização, auditoria e poderes de supervisão.

Renata Valenti
José Luquinda
PLMJ Colab Angola
– RVA Advogados

Pedro Lomba
Mafalda de Brito
Fernandes
PLMJ Advogados

ANGOLA

Os prestadores abrangidos devem comunicar os incidentes de impacto significativo às entidades competentes, incluindo o CERT.ao e o respectivo CSIRT sectorial.

Principais deveres para os prestadores abrangidos

Entre os principais deveres dos prestadores abrangidos destacam-se:

1. Registo e governação:

Registo junto do Centro Nacional de Cibersegurança e, em função da dimensão, risco e criticidade da actividade, criação de CSIRT institucional, designação de ponto focal de cibersegurança ou adesão a CSIRT sectorial;

2. Gestão de segurança e risco:

Adopção de medidas técnicas e organizativas adequadas e proporcionais para a prevenção, detecção, resposta e recuperação de incidentes, incluindo mecanismos de gestão de riscos, continuidade dos serviços e controlo de acessos;

3. Notificação e resposta a incidentes:

Comunicação dos incidentes de impacto significativo às entidades competentes, incluindo o CERT.ao e o respectivo CSIRT sectorial, bem como, quando aplicável, apresentação de relatório final sobre a resposta e resolução do incidente;

4. Requisitos específicos para centros de dados e serviços de computação em nuvem:

Adopção de políticas e medidas destinadas a garantir a continuidade de negócio, recuperação de desastres e gestão de riscos, contratação de seguro adequado e comunicação aos clientes ou assinantes sobre incidentes relevantes e respectiva cobertura;

5. Conformidade regulamentar:

Observância dos requisitos técnicos, procedimentos, prazos e canais de notificação que venham a ser definidos na regulamentação aplicável.

Os deveres concretamente aplicáveis dependerão da natureza, dimensão, risco e criticidade da actividade desenvolvida, devendo cada entidade avaliar o seu enquadramento regulatório à luz dos serviços prestados, das redes e sistemas utilizados e das relações estabelecidas com clientes, assinantes e prestadores terceiros.

ANGOLA

Regime Sancionatório

O incumprimento das obrigações previstas na Lei pode constituir contra-ordenação leve, grave ou muito grave, sendo aplicáveis coimas e, em determinados casos, sanções acessórias de suspensão temporária de actividades e de proibição de participação em procedimentos de contratação pública por período não superior a 3 anos. Para pessoas colectivas, as coimas podem atingir 2.000 a 4.000 salários mínimos nacionais no caso de infracções muito graves, sem prejuízo das demais consequências previstas na Lei. A fiscalização e a aplicação das sanções cabem ao Centro Nacional de Cibersegurança.

Em determinados casos, podem ser aplicadas sanções acessórias de suspensão temporária de actividades e de proibição de participação em procedimentos de contratação pública por período não superior a 3 anos.

Entrada em vigor e recomendações

A Lei entrou em vigor na data da sua publicação, 28 de Setembro de 2026. As entidades sujeitas a registo dispõem de 180 dias, contados da entrada em vigor, para proceder ao respectivo registo.

Recomenda-se que as entidades potencialmente abrangidas:

- i) confirmem a sua classificação e as obrigações aplicáveis;
- ii) concluam o registo e designem responsáveis, pontos focais e equipas de resposta;
- iii) documentem a gestão de riscos, os controlos técnicos e organizativos, os planos de continuidade e recuperação; e
- iv) testem os procedimentos de detecção, contenção, notificação e elaboração do relatório final. ■