

A Cyber Crucible atende ao requisito de localização de dados da Zâmbia?

Resposta curta: Sim. A Lei de Proteção de Dados da Zâmbia exige que os controladores processem e armazenem dados pessoais e dados pessoais sensíveis em um centro de dados ou servidor **dentro da Zâmbia**. A implantação on-premises da Cyber Crucible satisfaz isso diretamente — o backend é executado dentro da sua própria infraestrutura, no país.

O que a lei exige

A Parte X da Lei de Proteção de Dados da Zâmbia regula a transferência transfronteiriça, e a Seção 70 obriga um controlador de dados a processar e armazenar dados pessoais e dados pessoais sensíveis em um centro de dados ou servidor localizado dentro da Zâmbia.

Trata-se de um **mandato de localização de armazenamento**, não de um teste de salvaguardas. Proteções contratuais não satisfazem esse requisito.

Por que isso elimina a maioria das ferramentas de segurança baseadas em nuvem

Um fornecedor cujo produto exija o envio de telemetria de endpoint para uma região de nuvem fora da Zâmbia não pode atender à Seção 70 melhorando seus contratos ou sua criptografia. O requisito diz respeito a *onde os dados estão fisicamente localizados*.

Por que esta arquitetura a satisfaz

- **Backend on-premises** — todo o software de gerenciamento é executado em servidores que você controla, dentro da Zâmbia.
- **Análise local** — a avaliação de ameaças e a interdição ocorrem no próprio endpoint, de modo que a proteção nunca depende de um serviço fora do país.

- **Zero telemetria de saída** na configuração isolada (air-gapped).
- **Escopo mínimo** — chaves, credenciais, tokens e conteúdo nunca são coletados, de modo que o volume de dados pessoais sujeitos à Seção 70 já é pequeno desde o início.

“ Situação no momento da redação — confirme com assessoria jurídica local, incluindo quaisquer regras específicas do setor.

Revision #1

Created 2026-07-24 05:59:28 UTC by Dennis Underwood

Updated 2026-07-24 05:59:28 UTC by Dennis Underwood