A Cyber Crucible cumpre a Lei de Proteção de Dados do Quénia?

Resposta curta: Sim. A Lei de Proteção de Dados do Quénia de 2019 restringe a transferência transfronteiriça para países com salvaguardas apropriadas e aplica uma regra mais rigorosa aos dados pessoais sensíveis. A Cyber Crucible não recolhe quaisquer dados pessoais sensíveis e pode ser implementada de forma a que nenhum dado saia do Quénia.

O que a lei exige

As secções 48 e 49 da Lei de Proteção de Dados de 2019 proíbem a transferência de dados pessoais para um país que não disponha de salvaguardas de segurança de dados apropriadas, com várias bases permitidas, incluindo a adequação.

A regra mais rigorosa que importa: a transferência de dados pessoais *sensíveis* só é permitida quando o titular dos dados tiver consentido **e** existirem salvaguardas apropriadas. Ambas as condições, não apenas uma.

Por que a regra sobre dados sensíveis é o ponto-chave

Esse requisito duplo é difícil de satisfazer operacionalmente — obter e comprovar o consentimento individual de cada titular de dados afetado, de forma contínua, para uma ferramenta de segurança.

A Cyber Crucible contorna essa questão: **não é recolhido qualquer dado pessoal sensível.** Nem dados biométricos, de saúde ou genéticos; nem dados que revelem origem racial ou étnica, crença religiosa ou opinião política. A telemetria descreve o comportamento do sistema e eventos de segurança, não atributos pessoais.

Quando a telemetria comportamental puder identificar indiretamente um indivíduo, os identificadores são pseudonimizados ou mascarados.

Transferência

O staging regional mantém o processamento dentro do Quénia. A implementação com air-gap não produz qualquer telemetria de saída, pelo que as secções 48–49 não são aplicáveis.

> Situação à data de redação — confirme com o consultor jurídico local.

Revision #1
Created 2026-07-24 05:58:36 UTC by Dennis Underwood
Updated 2026-07-24 05:58:36 UTC by Dennis Underwood