# ¿Cómo afectan las leyes africanas de protección de datos a la selección de proveedores de seguridad?

**Respuesta breve:** La mayoría de las jurisdicciones africanas restringen la transferencia transfronteriza, y varias van más allá con una localización de datos estricta: Nigeria y Zambia exigen que los datos personales se almacenen dentro del país. Esto elimina las herramientas de seguridad dependientes de la nube de forma estructural, no contractual.

## El panorama regional

| Jurisdicción | Marco normativo | Posición sobre la salida de datos del país |
|---|---|---|
| **Nigeria** | Ley de Protección de Datos de 2023 | **Localización** — los datos personales de los ciudadanos deben almacenarse en Nigeria |
| **Zambia** | Ley de Protección de Datos, Parte X | **Localización** — la Sección 70 exige el almacenamiento en un servidor dentro de Zambia |
| **Kenia** | Ley de Protección de Datos de 2019 | Transferencia restringida; los datos sensibles requieren consentimiento **y** salvaguardas |
| **Sudáfrica** | POPIA (2013) | Consentimiento, o destino con una protección sustancialmente similar |
| **Egipto** | Ley de protección de datos | Se requiere **aprobación previa** para la transferencia |
| **Ruanda** | Ley supervisada por la NCSA | Localización sectorial — los bancos deben conservar los datos primarios en Ruanda |
| **Ghana** | Marco de protección de datos | Excepción notable — sin condiciones adicionales para las transferencias transfronterizas |
| **Marruecos** | Ley 09-08 + Decreto 2-09-165 | Supervisado por la CNDP; régimen establecido |

| Jurisdicción | Marco normativo | Posición sobre la salida de datos del país |
|---|---|---|
| **Libia** | Aún sin marco integral | La soberanía es una decisión comercial más que legal |

Estado vigente al momento de redactar esto; confirmar con asesoría legal local.

# El patrón que vale la pena entender

Aparecen tres modelos distintos, y exigen cosas diferentes de un proveedor:

1. **Mandatos de ubicación de almacenamiento** (Nigeria, Zambia; Ruanda para el sector bancario). Los contratos y el cifrado no satisfacen estos requisitos — solo importa dónde se encuentran físicamente los datos.
2. **Transferencia condicional** (Kenia, Sudáfrica). Permitida con salvaguardas, consentimiento o adecuación — una evaluación que debe poder acreditarse.
3. **Transferencia basada en permisos** (Egipto). Aprobación previa, con riesgos asociados de tiempo y renovación.

Las normas sectoriales suelen añadir localización adicional, particularmente en los servicios financieros.

# Por qué esto favorece una arquitectura de procesamiento local

Un producto de seguridad diseñado para enviar telemetría de endpoints a la nube del proveedor está, por diseño, exportando datos personales como condición para funcionar. Bajo el modelo 1, esto es irresoluble.

Cyber Crucible analiza en el endpoint y puede funcionar completamente en las instalaciones locales, sin telemetría saliente — de modo que los datos nunca salen, y la cuestión de la transferencia nunca se plantea.

> El detalle por país está disponible en las **Guías de Cumplimiento por País**.

---

Revision #1
Created 2026-07-24 01:56:48 UTC by Dennis Underwood
Updated 2026-07-24 01:56:48 UTC by Dennis Underwood