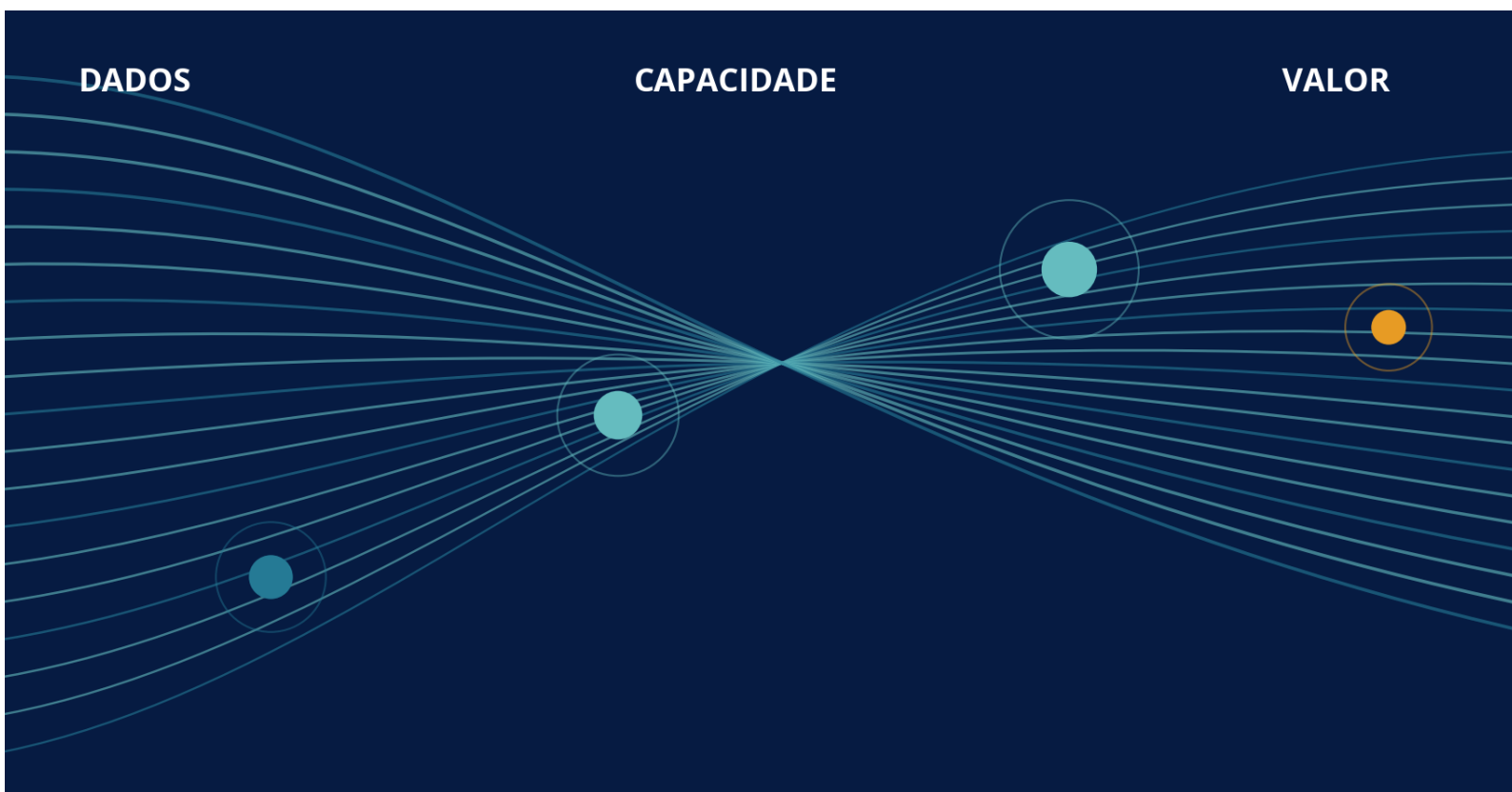


Soberania digital em Angola

Prioridades para a capacidade nacional e a transformação digital inclusiva

Angola pode reforçar o controlo sobre os seus ativos digitais e transformar esse controlo em melhores serviços, talento e atividade económica. O caminho passa por combinar proteção proporcional ao risco, cooperação internacional e capacidade de execução local.

DADOS**CAPACIDADE****VALOR**

ÍNDICE

Contexto global	4	
Contexto angolano	6	
Dados e infraestrutura	8	
Resiliência e contratação	10	
Talento e IA	12	
Serviços públicos e inclusão	14	
Economia digital	16	
Execução e indicadores	18	
Decisões prioritárias	20	
UM ROTEIRO PARA ANGOLA	21	
Referências	24	

Soberania digital é garantir que Angola tem capacidade para decidir, proteger, operar, regular e criar valor no mundo digital.

A soberania digital do país deve ser aberta, pragmática e inteligente: proteger o que é crítico, cooperar onde há escala, desenvolver capacidade nacional onde há valor, e garantir que ninguém fica fora da sociedade digital.

Este insight dirige-se a decisores públicos, dirigentes empresariais e parceiros de desenvolvimento. Apresenta um contributo para a reflexão sobre os temas centrais da transformação digital da sociedade da informação e uma agenda de execução para Angola.

O CEO da LBC, Carlos Valleré Oliveira, foi orador convidado no ANGOTIC 2026, realizado em Luanda de 11 a 13 de junho, no painel sobre “Soberania Digital e Transformação Digital da Sociedade da Informação”. Este artigo, bem como outro sobre a transformação digital da sociedade da informação em Angola, substanciaram a sua participação. E são contributos para discussão.

SÍNTESE EXECUTIVA

Soberania digital exige capacidade de decisão e execução

Angola deve tratar a soberania digital como uma agenda de desenvolvimento. O objetivo é garantir capacidade nacional para decidir sobre os dados, proteger serviços essenciais, gerir fornecedores e criar valor com a tecnologia. Esta capacidade permite beneficiar de soluções globais com maior segurança e poder de escolha.

A localização física de um centro de dados, por si só, não assegura controlo. Importam também os direitos de acesso, a gestão das chaves de encriptação, a capacidade de operação, a possibilidade de auditoria e a viabilidade de mudar de fornecedor. A política digital deve avaliar estas condições em conjunto.

EXHIBIT 1 Três dimensões para orientar as decisões**01****CONTROLO**

Dados estratégicos
Sistemas críticos
Regras e contratos

02**CAPACIDADE**

Talento nacional
Operação e auditoria
IA contextualizada

03**VALOR**

Serviços inclusivos
Empresas e emprego
Cooperação africana

Modelo de análise proposto pela LBC.

A primeira prioridade é identificar os ativos digitais estratégicos e definir requisitos proporcionais à sua criticidade. A segunda é criar equipas e instituições capazes de aplicar esses requisitos, operar os sistemas e desenvolver soluções adequadas ao contexto angolano. A terceira é assegurar que os investimentos produzem benefícios acessíveis à população e oportunidades para empresas angolanas.

A transformação digital deve ser avaliada pela utilização, pela qualidade do serviço e pela capacidade de o manter. A inclusão e a resiliência precisam de acompanhar o investimento desde o início.

A medida da soberania digital é a capacidade de escolher, operar e evoluir os sistemas de que o país depende.

01 CONTEXTO GLOBAL

Temas mais prementes da soberania digital

1. Dados: quem recolhe, onde ficam, quem acede e quem captura valor.

Os dados são hoje uma infraestrutura económica e política. A questão já não é apenas “proteger dados pessoais”, mas saber se o país tem regras, instituições e capacidade técnica para gerir dados públicos, empresariais, pessoais, estratégicos e setoriais. A União Africana coloca a governação de dados no centro da economia digital africana, defendendo quadros harmonizados, espaços partilhados de dados e padrões comuns para aumentar confiança, inovação e comércio digital interafricano.

2. Cloud, centros de dados e dependência tecnológica.

A soberania digital depende de saber que dados e sistemas devem estar na cloud pública global, na cloud governamental, em centros de dados nacionais ou infraestruturas regionais africanas. A resposta não deve ser “tudo local” nem “tudo fora”: deve ser uma classificação por criticidade. Dados de segurança, identidade, finanças públicas, saúde, infraestruturas críticas e justiça exigem controlo reforçado. Dados menos críticos podem beneficiar de escala global, desde que com contratos, encriptação, reversibilidade e auditoria.

3. Cibersegurança como segurança nacional.

A soberania digital falha quando infraestruturas críticas podem ser paralisadas por ataques, ransomware, sabotagem, espionagem ou dependência operacional externa. Angola já reconhece este cenário no seu quadro recente: o Decreto Presidencial n.º 258/25 cria o Conselho Nacional de Cibersegurança e enquadra a cibersegurança como essencial para proteger dados, redes, sistemas de informação e infraestruturas críticas, incluindo saúde, energia e telecomunicações.

4. Inteligência artificial, algoritmos e soberania cognitiva.

A inteligência artificial (IA) levanta uma nova camada de soberania: que modelos usamos, com que dados foram treinados, que línguas e culturas representam, que decisões automatizam e que enviesamentos reproduzem. Para África, a pergunta é: seremos apenas consumidores de modelos globais ou produtores de soluções adaptadas às nossas realidades, línguas, serviços públicos e economias?

5. Identidade digital, pagamentos e interoperabilidade pública.

Quem controla os sistemas de identidade, autenticação, assinatura digital, pagamentos e troca segura de dados controla a espinha dorsal da sociedade digital. O Banco Mundial destaca a infraestrutura pública digital – identidade digital, pagamentos e partilha segura de dados – como a base para serviços públicos digitais, inclusão e inovação.

6. Dependência de fornecedores e procurement público.

Soberania digital também é evitar dependência excessiva de um único fornecedor, tecnologia ou país. Isto implica interoperabilidade, standards abertos, portabilidade de dados, cláusulas de saída, transferência de conhecimento e desenvolvimento de capacidade local.

7. Talento e capacidade produtiva.

Um país não é digitalmente soberano apenas porque compra tecnologia. É soberano quando tem engenheiros, juristas digitais, gestores de dados, especialistas de cibersegurança, arquitetos cloud, reguladores competentes, start-ups e empresas angolanas capazes de criar, manter e auditar soluções.

02 CONTEXTO ANGOLANO

Inclusão define a escala do desafio angolano

O acesso efetivo à internet deve orientar as escolhas de transformação digital. As estimativas do relatório "Digital 2026: Angola", referidas a outubro de 2025, indicam que mais de metade da população ainda não utiliza a internet. A existência de ligações móveis não elimina esta distância: uma ligação pode servir apenas voz ou mensagens, e uma pessoa pode ter várias ligações. [1]

EXHIBIT 2 A maioria da população ainda não utilizava internet em 2025

44,8%

utiliza a internet

55,2%

não utiliza a internet

17,6 milhões de pessoas

21,7 milhões de pessoas

30,6 milhões de ligações móveis

Ligações móveis não correspondem a utilizadores únicos de internet.

Fonte: DataReportal, "Digital 2026: Angola". Dados de outubro de 2025. Percentagens sobre a população total; valores arredondados.

A resposta deve combinar cobertura, dispositivos acessíveis, custo dos dados, energia, competências digitais e serviços úteis. Para o cidadão, estas condições funcionam em conjunto. Uma rede disponível não resolve a falta de equipamento; um equipamento não resolve a dificuldade em compreender ou concluir um serviço.

Base estratégica já definida

O "Livro Branco das Tecnologias de Informação e Comunicação 2023-2027" enquadra a transformação digital nos instrumentos angolanos de desenvolvimento, incluindo o Plano de Desenvolvimento Nacional 2023-2027 e Angola 2050. Organiza a intervenção em seis eixos: banda larga, conectividade e inclusão digital; capacitação; modernização

tecnológica da Administração Pública; inovação tecnológica; regulação; e cibersegurança. [2]

A soberania deve dar coerência à execução desta agenda. Cada investimento precisa de explicitar o serviço que melhora, a dependência que reduz, a capacidade que desenvolve e os recursos necessários para funcionar ao longo do tempo.

Escala africana reforça a capacidade nacional

A Estratégia de Transformação Digital para África (2020-2030) defende uma economia digital inclusiva e a construção de um mercado único digital. A harmonização de regras e a interoperabilidade podem ampliar a escala disponível para empresas e instituições africanas. Para Angola, cooperar em dados, pagamentos, cibersegurança e competências pode aumentar a capacidade de negociação e o acesso a mercados. [3, 4]

03 DADOS E INFRAESTRUTURA

Controlo dos dados deve acompanhar a sua criticidade

A primeira decisão é identificar os ativos digitais de que dependem o Estado e a economia. O inventário deve abranger identidade civil, finanças públicas, saúde, justiça, segurança, energia, telecomunicações, banca, transportes, recursos naturais e informação geoespacial. Para cada ativo, importa identificar o responsável, os utilizadores autorizados, as dependências e as consequências de perda, alteração ou indisponibilidade.

Uma política de dados deve traduzir este inventário em regras de recolha, utilização, conservação, partilha e transferência. O quadro de política de dados da União Africana oferece uma referência para harmonizar a governação, promover confiança e desenvolver espaços de dados que apoiem inovação e comércio digital. [4]

EXHIBIT 3 Critérios para decidir o alojamento e o controlo de dados

Tipo de ativo	Opção a avaliar	Condições de controlo
Estratégico ou crítico	Infraestrutura nacional, governamental ou solução com controlo reforçado	Autoridade sobre acessos e chaves; continuidade testada; auditoria; capacidade de operação
Sensível ou regulado	Arquitetura nacional, regional ou híbrida, conforme risco e regime aplicável	Acesso limitado; encriptação; registo de operações; regras de transferência e conservação
Não sensível ou público	Infraestrutura que ofereça a melhor combinação de escala, custo e serviço	Integridade; disponibilidade; formatos abertos; portabilidade e recuperação dos dados

Matriz de decisão proposta pela LBC. As opções dependem da classificação concreta do ativo e do regime aplicável; não constituem uma regra geral de localização.

Decidir além da localização física

A cloud pública global pode proporcionar escala e acesso a tecnologia. Infraestruturas nacionais ou regionais podem responder a necessidades específicas de controlo e continuidade. A seleção deve considerar o risco, a jurisdição, a capacidade técnica, o custo total e a operação efetiva. Manter tudo local sem capacidade de manutenção também pode criar fragilidade.

A gestão de chaves, os acessos privilegiados, as cópias de segurança e os mecanismos de auditoria devem ser desenhados antes da contratação. O mesmo se aplica à reversibilidade: é necessário saber como recuperar dados, configurações e documentação, quanto custa a migração e quem consegue executá-la.

A escolha da infraestrutura deve resultar de uma avaliação de risco e de capacidade operacional, com revisão quando os sistemas, os serviços ou as condições de fornecimento mudam.

04 RESILIÊNCIA E CONTRATAÇÃO

Proteger sistemas críticos implica testar a continuidade

Uma interrupção num sistema de saúde, na energia, nas telecomunicações, finanças, nos portos, aeroportos ou na administração fiscal pode afetar serviços essenciais e a confiança económica. A soberania digital exige capacidade para prevenir incidentes, detetar anomalias, responder e recuperar a operação. A proteção deve incluir sistemas de informação e, quando aplicável, tecnologia operacional.

O Decreto Presidencial n.º 258/25, de 3 de dezembro, criou o Conselho Nacional de Cibersegurança e aprovou o seu regimento. Este enquadramento reforça a dimensão institucional da cibersegurança. A execução requer responsabilidades claras entre coordenação nacional, entidades setoriais e operadores dos serviços. [5]

Da conformidade à capacidade de resposta

As organizações responsáveis por ativos críticos devem conhecer as dependências entre sistemas, definir tempos de recuperação e testar cenários de falha. Cópias de segurança só dão proteção efetiva quando é possível restaurá-las. Um plano de continuidade só é credível quando os responsáveis sabem quem decide, quem comunica e como se mantém o serviço durante uma interrupção.

Exercícios conjuntos permitem avaliar falhas que atravessam várias entidades. Também ajudam a distinguir indisponibilidade técnica, perda de dados e compromisso de credenciais, situações que exigem respostas diferentes. As conclusões dos testes devem originar ações corretivas com responsáveis e prazos.

Contratação pública deve preservar opções

A dependência excessiva de um fornecedor, tecnologia ou país reduz a capacidade de escolha. Os contratos devem prever padrões abertos, interfaces documentadas, portabilidade, níveis de serviço, direitos de auditoria e condições de saída. A avaliação económica deve incluir operação, atualização, formação e transição para outro prestador.

A reversibilidade contratual só tem valor quando existe capacidade técnica para a executar.

A transferência de conhecimento deve produzir evidência verificável: equipas treinadas em tarefas reais, documentação atualizada, acesso às configurações relevantes e exercícios de operação autónoma. Quando adequado, devem existir condições para auditar o código. Estes requisitos tornam a parceria internacional mais sustentável e reforçam a responsabilidade pelo serviço.

A diversidade de fornecedores deve ser proporcional ao risco. Multiplicar soluções sem uma arquitetura comum aumenta a complexidade. O objetivo é manter alternativas viáveis e competência interna para as avaliar, integrar e gerir.

05 TALENTO E INTELIGÊNCIA ARTIFICIAL

A capacidade nacional deve crescer com cada projeto

A aquisição de tecnologia deve ser acompanhada por capacidade para a utilizar, manter e melhorar. Angola precisa de profissionais de dados, desenvolvimento de software, arquitetura cloud, cibersegurança, gestão de produto e regulação digital. Precisa também de líderes públicos capazes de relacionar decisões tecnológicas com resultados de serviço.

A formação ganha valor quando está ligada ao trabalho. Equipas mistas, manutenção acompanhada, revisão de arquiteturas e resolução conjunta de incidentes permitem transferir conhecimento que um curso isolado dificilmente assegura. Universidades, centros de formação, empresas e instituições públicas podem organizar percursos ligados a necessidades concretas de operação.

Aplicar IA a problemas delimitados

A IA acrescenta uma dimensão de soberania ligada aos dados, às línguas e às decisões que os modelos influenciam. Angola pode utilizar modelos globais e desenvolver capacidade local para os adaptar, integrar e avaliar. Isto inclui testar o português usado no país, as línguas nacionais e a adequação das respostas aos contextos institucionais e culturais.

Domínio	Aplicação inicial possível	Condição para avançar
Administração pública	Apoio ao atendimento, à pesquisa e à análise documental	Fontes verificadas; proteção de dados; revisão humana e encaminhamento de exceções
Educação e saúde	Apoio a docentes e profissionais; conteúdos e informação	Validação por especialistas; limites claros; avaliação de erros e acessibilidade
Agricultura, pequenas e médias empresas (PME)	Informação técnica, apoio à gestão e ao acesso a serviços	Adaptação local; canais acessíveis; teste com os utilizadores
Alfândegas e fiscalização	Triagem documental e identificação de anomalias	Rastreabilidade; teste de enviesamentos; decisão e responsabilização humanas

Exemplos de aplicações propostos para análise. A adequação depende dos dados disponíveis, do risco e da capacidade de supervisão.

O primeiro investimento deve privilegiar casos com utilidade demonstrável e possibilidade de medir a qualidade. Antes de alargar uma solução, importa verificar precisão, custo por tarefa, tempo poupado, incidentes e efeitos sobre o acesso ao serviço. Decisões com impacto em direitos ou prestações exigem supervisão reforçada e mecanismos de contestação.

Desenvolver capacidade própria em IA não obriga a começar pela construção de grandes modelos de base. Pode começar pela qualidade dos dados, por avaliações independentes e por aplicações setoriais que as equipas nacionais consigam operar e evoluir.

06 SERVIÇOS PÚBLICOS E INCLUSÃO

Infraestrutura comum pode simplificar a relação com o Estado

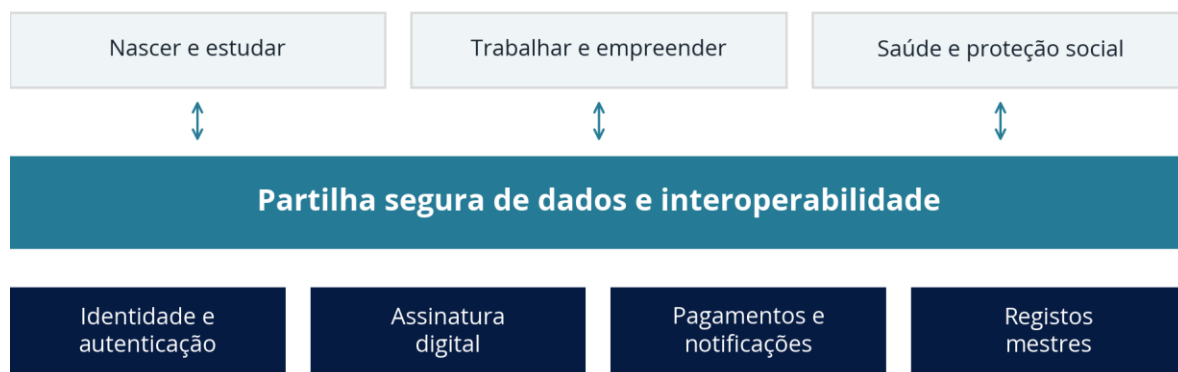
Digitalizar a Administração Pública exige redesenhar serviços em torno de necessidades concretas: registar um nascimento, estudar, abrir uma empresa, pagar impostos, receber apoios ou aceder a cuidados de saúde. Publicar formulários sem rever processos mantém muitas das dificuldades que o cidadão já enfrenta.

Uma infraestrutura pública digital comum permite reutilizar identidade, autenticação, assinatura, pagamentos e partilha de dados. O Banco Mundial identifica a infraestrutura pública digital como uma base para melhorar a prestação de serviços entre setores. [6]

Para Angola, a arquitetura deve definir componentes comuns, responsabilidades pelos registos e condições seguras de acesso.

EXHIBIT 4 Componentes partilhados para serviços públicos integrados

SERVIÇOS ORGANIZADOS EM TORNO DA VIDA DO CIDADÃO



Base transversal Segurança • Proteção de dados • Acessibilidade • Supervisão

Arquitetura conceitual proposta pela LBC, informada pela abordagem de infraestrutura pública digital do Banco Mundial. [6]

O princípio de fornecer informação uma única vez deve orientar a simplificação. A sua aplicação requer registos fiáveis, uma base legal adequada e controlo de acessos. O consentimento deve ser utilizado quando for a base aplicável; não substitui os restantes requisitos de legitimidade, segurança e transparência.

Desenhar para quem enfrenta mais barreiras

Os serviços devem funcionar em dispositivos acessíveis, com baixo consumo de dados e instruções compreensíveis. Canais de apoio e atendimento assistido são necessários para pessoas com menor literacia digital, limitações de acesso ou deficiência. A expansão territorial deve considerar escolas, funcionários públicos, PME, agricultores e jovens, incluindo fora de Luanda.

A confiança depende de um serviço previsível: saber que dados são pedidos, porquê, quem os utiliza e como corrigir um erro. A avaliação deve acompanhar a conclusão dos pedidos, o tempo de resolução e a satisfação, com análise das diferenças territoriais e entre grupos de utilizadores.

07 ECONOMIA DIGITAL

A procura pública pode desenvolver capacidade produtiva nacional

A soberania digital tem uma dimensão económica. Projetos públicos e grandes investimentos empresariais podem criar procura para fornecedores angolanos de software, dados, cibersegurança, formação e serviços de operação. Para que tal aconteça, os contratos precisam de transformar participação local em competências e capacidade de entrega duradouras.

Criar oportunidades com exigência de qualidade

A contratação pode facilitar a participação de empresas angolanas através de requisitos proporcionais, interfaces abertas, consórcios e condições claras de transferência de conhecimento. A seleção deve continuar a exigir qualidade, segurança e sustentabilidade económica. A participação local acrescenta valor quando as empresas conseguem manter soluções, assumir responsabilidades técnicas e conquistar novos clientes.

A agenda empresarial deve abranger comércio eletrónico, pagamentos, serviços financeiros digitais, tecnologia para a agricultura, educação e saúde, bem como digitalização das PME. Serviços digitais exportáveis podem contribuir para a diversificação económica quando existem competências, qualidade e acesso a mercados.

Construir uma posição regional com condições concretas

Angola pode ambicionar uma posição de plataforma digital regional. Esta possibilidade deve ser avaliada em função da conectividade, da disponibilidade e do custo da energia, da qualidade das infraestruturas, da previsibilidade regulatória, do talento e da procura. A ambição deve traduzir-se numa proposta competitiva para empresas e utilizadores.

A cooperação africana pode ampliar o mercado e reduzir fragmentação. Regras compatíveis para dados, interoperabilidade e pagamentos transfronteiriços facilitam o desenvolvimento de serviços regionais. A participação angolana na agenda digital

africana deve procurar benefícios operacionais e comerciais concretos, ao preservar o controlo sobre ativos estratégicos. [3, 4]

Integrar a sustentabilidade no investimento

O crescimento digital aumenta a utilização de energia, água, equipamentos e materiais. A UNCTAD (sigla em inglês para Conferência das Nações Unidas sobre Comércio e Desenvolvimento) chama a atenção para a pegada ambiental ao longo do ciclo de vida da digitalização e para a distribuição desigual dos seus custos. [7] Centros de dados, redes e dispositivos devem ser avaliados considerando eficiência, manutenção, durabilidade, reutilização e tratamento de resíduos eletrónicos.

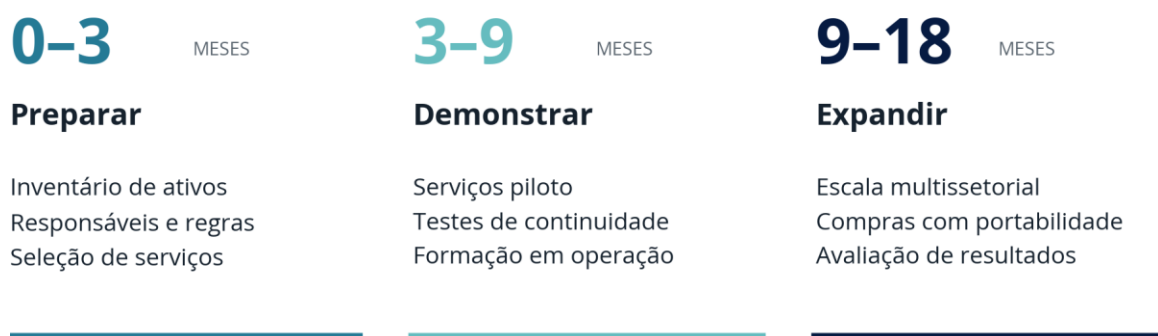
A capacidade produtiva local deve ser avaliada pelo conhecimento e pela operação que permanecem no país.

08 EXECUÇÃO E INDICADORES

Sequenciar as prioridades torna a agenda executável

Propõe-se uma sequência indicativa de 18 meses, a partir do arranque de um programa, centrada em ativos críticos e serviços de elevado valor público. A proposta deve ser ajustada aos recursos e às decisões institucionais; não corresponde a um compromisso governamental.

EXHIBIT 5 Sequência indicativa para criar capacidade e demonstrar resultados



Proposta LBC. Os horizontes referem-se a meses após o início do programa; as frentes podem sobrepor-se.

A preparação deve definir ativos, dependências e responsáveis. Os pilotos devem testar a experiência do utilizador, o controlo, a continuidade e a operação local. A expansão deve depender dos resultados demonstrados, com avaliação de custos e capacidade de suporte.

A coordenação deve integrar serviços, dados, tecnologia, cibersegurança, contratação e capacitação. Cada iniciativa precisa de um responsável por resultados, orçamento de operação, critérios de aceitação e acompanhamento dos riscos e das decisões entre entidades.

EXHIBIT 6 Indicadores para medir capacidade e valor público

Dimensão	Indicador sugerido	Evidência a recolher
Controlo e resiliência	Ativos críticos classificados; recuperação dentro do tempo definido	Inventário validado e resultados de testes
Autonomia operacional	Sistemas operáveis por equipas locais; saídas de fornecedor testadas	Exercícios de operação e de portabilidade
Serviço e inclusão	Pedidos concluídos; tempo de resolução; utilização por território	Registos de serviço e investigação com utilizadores
Talento e economia	Competências aplicadas; contratos com transferência demonstrada	Avaliação prática e entregáveis aceites
Sustentabilidade	Consumo de energia e destino dos equipamentos	Medição operacional e registo de reutilização ou reciclagem

Indicadores propostos. Estabelecer a linha de base e as metas por serviço antes de avaliar o desempenho; evitar usar a despesa ou o número de plataformas como medidas de sucesso.

09 DECISÕES PRIORITÁRIAS

Dez decisões para orientar a soberania digital de Angola

A agenda de soberania digital deve traduzir-se em decisões verificáveis. As prioridades seguintes articulam proteção, capacidade nacional e criação de valor, mantendo abertura a parceiros e mercados internacionais.

01 Identificar os ativos estratégicos. Inventariar dados e sistemas essenciais, atribuir responsáveis e classificar criticidade, sensibilidade e dependências.

02 Definir a política de dados. Clarificar condições de acesso, alojamento, utilização, conservação, partilha e transferência, com controlo proporcional ao risco.

03 Reforçar a cibersegurança nacional. Ligar a coordenação institucional à prevenção, deteção, resposta e recuperação, com exercícios nos setores críticos.

04 Reduzir dependências excessivas. Exigir interoperabilidade, portabilidade, documentação, direitos de auditoria e condições de saída que possam ser executadas.

05 Desenvolver talento nacional. Associar formação a projetos reais e verificar a capacidade das equipas para gerir, manter, auditar e melhorar os sistemas.

06 Construir capacidade em IA. Selecionar aplicações úteis, qualificar dados e avaliar modelos no contexto angolano, com supervisão proporcional ao impacto.

07 Consolidar a infraestrutura pública digital. Reutilizar identidade, autenticação, assinatura, pagamentos e partilha segura de dados para simplificar serviços.

08 Transformar a procura em atividade económica. Criar oportunidades para empresas nacionais, serviços exportáveis e emprego qualificado, com exigência de qualidade.

09 Manter abertura com regras claras. Mobilizar investimento e tecnologia internacionais com proteção dos ativos estratégicos e transferência de conhecimento.

10 Participar na agenda digital africana. Promover cooperação em dados, cloud, cibersegurança, IA e pagamentos, procurando escala e interoperabilidade regional.

10 UM ROTEIRO PARA ANGOLA

Proposta de um roteiro para Angola

1.º: Definir de forma clara quais são os ativos digitais estratégicos.

Nem todos os dados e sistemas têm o mesmo nível de sensibilidade. Angola deve identificar quais são os dados críticos do Estado e da economia: identidade civil, dados fiscais, saúde, segurança, justiça, energia, telecomunicações, banca, infraestruturas críticas, recursos naturais e dados geoespaciais. A soberania digital começa por saber **o que é estratégico e o que precisa de proteção reforçada.**

2.º: Definir uma política clara sobre dados nacionais.

O país deve decidir que dados podem estar em clouds internacionais, que dados devem estar em infraestruturas nacionais ou regionais, e que regras devem existir para acesso, armazenamento, tratamento e transferência internacional de dados. A questão central não é apenas “onde estão os dados?”, mas também: **quem tem acesso, com que autorização, com que segurança e para que finalidade?**

3.º: Reforçar a capacidade nacional de cibersegurança.

A soberania digital depende da capacidade de prevenir, detetar, responder e recuperar de ataques digitais. Isto é especialmente importante para setores como energia, telecomunicações, banca, administração pública, saúde, transportes, portos, aeroportos e petróleo e gás. A cibersegurança deve ser tratada como uma matéria de **segurança nacional, continuidade do Estado e confiança económica.**

4.º: Evitar dependências tecnológicas excessivas.

A dependência de um único fornecedor, de uma única plataforma, de uma única tecnologia ou de um único país pode criar vulnerabilidades estratégicas. Angola deve promover interoperabilidade, standards abertos, portabilidade de dados, cláusulas de saída nos contratos públicos e capacidade interna de gestão das soluções. Soberania digital não significa rejeitar parceiros internacionais; significa **negociar melhor, controlar melhor e manter capacidade de escolha.**

5.º: Desenvolver talento digital nacional.

Não há soberania digital sem pessoas qualificadas. O país precisa de formar programadores, especialistas em dados, arquitetos cloud, profissionais de cibersegurança, gestores de produto digital, juristas digitais, reguladores tecnológicos e líderes públicos capazes de compreender tecnologia. Comprar tecnologia é relativamente fácil; **criar capacidade nacional para a gerir, auditar e evoluir é o verdadeiro desafio.**

6.º: Construir capacidade própria em IA.

A IA coloca uma nova dimensão na soberania: os modelos podem influenciar decisões, linguagem, cultura, políticas públicas, crédito, recrutamento, educação e acesso a serviços. Angola deve usar IA global quando fizer sentido, mas também desenvolver soluções adaptadas ao contexto angolano, à língua portuguesa, às línguas nacionais, aos serviços públicos e aos setores prioritários da economia. Caso contrário, corre o risco de ser apenas consumidor de algoritmos concebidos fora da sua realidade.

7.º: Criar uma infraestrutura pública digital robusta.

Identidade digital, assinatura digital, pagamentos digitais, autenticação segura, interoperabilidade entre bases de dados públicas e troca segura de informação são componentes fundamentais da soberania digital. Sem esta infraestrutura, a transformação digital fica fragmentada, cara e pouco confiável. Com ela, Angola pode acelerar serviços públicos, inclusão financeira, formalização da economia e eficiência do Estado.

8.º: Transformar soberania digital em oportunidade económica.

A soberania digital não deve ser vista apenas como defesa ou proteção. Deve também ser uma oportunidade para desenvolver empresas tecnológicas nacionais, start-ups, centros de dados, serviços digitais exportáveis, soluções de govtech, fintech, agritech, edtech e healthtech. Angola pode usar a procura pública e os grandes projetos digitais como alavanca para criar uma indústria digital nacional.

9.º: Equilibrar soberania com abertura internacional.

Um erro seria confundir soberania digital com isolamento. Angola precisa de parceiros globais, investimento estrangeiro, tecnologia internacional e cooperação regional. Mas deve fazê-lo com regras claras, proteção dos interesses nacionais e transferência de conhecimento. A melhor posição é uma **soberania aberta**: cooperar com o mundo, mas preservar controlo sobre o que é estratégico.

10.º: Participar de modo ativo na agenda digital africana.

Muitos desafios digitais exigem escala regional ou continental: cibersegurança, cloud, IA, pagamentos transfronteiriços, proteção de dados, comércio digital e regulação de plataformas. Angola deve posicionar-se não apenas como utilizador, mas como protagonista da construção do mercado digital africano. A soberania digital de Angola será mais forte se estiver articulada com a soberania digital africana.

Para Angola, soberania digital significa ter capacidade nacional para proteger dados, operar os sistemas críticos, formar talento, negociar com parceiros internacionais e transformar tecnologia em desenvolvimento económico e social.

O critério final deve ser o desenvolvimento económico e social: cidadãos com melhor acesso a serviços, instituições capazes de proteger e operar os seus sistemas e empresas aptas a criar valor.

A inclusão e a sustentabilidade devem acompanhar a execução de todas estas decisões.

REFERÊNCIAS

Fontes e enquadramento

As referências seguintes sustentam os dados e os enquadramentos citados no texto. As matrizes, as aplicações exemplificativas, a sequência de execução e os indicadores são propostas de análise da LBC.

1 DataReportal

"Digital 2026: Angola". Estimativas sobre utilização da internet e ligações móveis, com referência a outubro de 2025.

[Consultar o relatório](#)

2 República de Angola

Decreto Presidencial n.º 272/24, de 5 de dezembro. Aprova o "Livro Branco das Tecnologias de Informação e Comunicação 2023-2027".

[Consultar o diploma](#)

3 União Africana

The Digital Transformation Strategy for Africa 2020–2030. Estratégia continental para uma sociedade e uma economia digitais inclusivas.

[Consultar a estratégia](#)

4 União Africana

"AU Data Policy Framework". Quadro de política de dados adotado em 2022.

[Consultar o quadro de política](#)

5 República de Angola

Decreto Presidencial n.º 258/25, de 3 de dezembro. Cria o Conselho Nacional de Cibersegurança e aprova o respetivo regimento.

[Consultar o diploma](#)

6 Banco Mundial

"Digital Progress and Trends Report 2023". Capítulo 4, sobre infraestrutura pública digital e prestação de serviços entre setores.

[Consultar o relatório](#)

7 UNCTAD

"Digital Economy Report 2024. Shaping an Environmentally Sustainable and Inclusive Digital Future".

[Consultar a publicação](#)

LBC

Intelligent Transformation

Governança digital e transformação das organizações.