WHITE PAPER

Arquitectura Nacional Resiliente para o Estado Digital

Dois data centers centrais, nós distritais Linux/x86, PostgreSQL, segurança Zero Trust e governação soberana de dados

Francisco Gonçalves

Fragmentos do Caos | Junho de 2026 | Versão 1.0

Nota editorial

Este white paper apresenta uma proposta técnica e conceptual para uma arquitectura nacional resiliente dos sistemas digitais do Estado português. A sua finalidade é estimular debate técnico, político e institucional sobre continuidade de serviço, soberania tecnológica, governação de dados e segurança operacional.

A proposta não pretende substituir estudos de engenharia detalhados, dimensionamento físico, análise de custos, avaliação de risco, normas de contratação pública ou projectos executivos. Pretende, isso sim, demonstrar que é possível pensar o Estado digital a partir de princípios de arquitectura, e não apenas a partir de aquisições dispersas de tecnologia.

Índice

1. Sumário executivo

O Estado português depende hoje de sistemas digitais para funções essenciais: saúde, finanças, segurança social, justiça, identificação civil, administração interna, protecção civil, educação, registos e serviços locais. No entanto, a evolução tecnológica do sector público tem sido, em demasiados casos, acumulativa e fragmentada, mais próxima de uma manta de retalhos informática do que de uma verdadeira arquitectura nacional.

Este white paper propõe uma arquitectura nacional resiliente, baseada em dois data centers centrais, localizados em Lisboa e no Porto, com plataformas IBM mainframe/LinuxONE a correr Linux e virtualização empresarial. Estes centros funcionariam como núcleo soberano dos sistemas críticos do Estado, com replicação, continuidade, segurança e capacidade de takeover em caso de falha regional ou catástrofe.

A arquitectura é complementada por nós distritais x86/Linux, com PostgreSQL local, caches autorizadas, filas persistentes, API gateways e capacidade de operação em modo degradado. Estes nós permitem continuidade de serviços de proximidade mesmo quando há falha temporária de comunicação com os centros nacionais.

O objectivo não é criar uma plataforma espectacular. É criar uma plataforma séria. A tecnologia existe quando tudo corre bem; a arquitectura revela-se quando algo falha.

Tese central

> *Um Estado moderno precisa de uma coluna vertebral digital soberana, redundante, auditável e operável em crise, em vez de ilhas tecnológicas compradas ao ritmo de cada organismo, fornecedor ou ciclo político.*

2. Contexto e problema

A digitalização do Estado tem avançado através de múltiplas iniciativas, portais, aplicações, bases de dados e contratos de prestação de serviços. Muitas destas iniciativas trouxeram valor. Porém, a ausência de uma arquitectura nacional vinculativa criou problemas estruturais: duplicação de sistemas, heterogeneidade excessiva, integrações frágeis, segurança desigual, dependência de fornecedores e dificuldade de assegurar continuidade de serviços críticos.

O problema não é apenas tecnológico. É organizacional. Sistemas de informação públicos não são aplicações isoladas. São infra-estruturas de soberania. Quando falham, bloqueiam direitos, serviços, pagamentos, consultas, actos administrativos, justiça e confiança pública.

Um Estado que não consegue garantir continuidade digital nos seus serviços essenciais fica exposto a falhas técnicas, ataques informáticos, catástrofes físicas, erros humanos e dependências contratuais perigosas. E depois descobre, geralmente tarde demais, que tinha tecnologia, mas não tinha arquitectura.

Problemas típicos a combater

- Bases de dados isoladas e sem governação nacional de dados.
- Integrações ponto-a-ponto frágeis, difíceis de auditar e de manter.
- Dependência excessiva de fornecedores e tecnologias proprietárias.
- Ausência de continuidade testada para serviços críticos.
- Backups sem imutabilidade ou sem testes regulares de reposição.
- Segurança tratada como camada final e não como princípio de desenho.
- Falta de observabilidade transversal dos serviços públicos.
- Feudos tecnológicos por ministério, instituto ou aplicação.

3. Princípios de desenho

A arquitectura proposta assenta numa combinação de princípios clássicos de engenharia de sistemas, segurança operacional e governação institucional. Não parte da moda tecnológica do momento. Parte do risco, da continuidade, dos dados e dos serviços críticos ao cidadão.

Princípio	Descrição
Centralização estratégica	Os dados e serviços críticos nacionais devem residir em plataformas centrais robustas, replicadas e auditáveis.
Descentralização operacional	Os nós distritais devem permitir atendimento e operação local, com autonomia controlada e modo degradado.
Soberania tecnológica	Linux, PostgreSQL, normas abertas, APIs documentadas, contratos reversíveis e equipas internas competentes.
Replicação por criticidade	Nem tudo deve ser síncrono; nem tudo deve ser assíncrono. O modelo depende do valor e risco dos dados.
Segurança por desenho	Zero Trust, MFA, mTLS, gestão de chaves, logs imutáveis, segmentação e menor privilégio.
Operação observável	Métricas, logs, traces, auditoria, alertas e dashboards nacionais e distritais.
Continuidade testada	Planos de falha, recuperação, ransomware e operação distrital isolada devem ser regularmente ensaiados.

4. Arquitectura física

A arquitectura física propõe dois data centers nacionais principais, localizados em Lisboa e no Porto, separados geograficamente e desenhados para operar cargas críticas. Cada centro deve ter capacidade de assumir serviços essenciais em caso de falha do outro. A distribuição geográfica reduz risco de catástrofe regional e permite continuidade de serviço em cenários adversos.

Figura 1 - Desenho físico da arquitectura nacional resiliente.

4.1 Data centers centrais

Os data centers de Lisboa e Porto funcionam como núcleo soberano. Cada um deve possuir plataforma IBM mainframe/LinuxONE, Linux empresarial, virtualização, storage empresarial, PostgreSQL central, API Gateway nacional, IAM, SIEM, gestão de chaves, monitorização e backups locais imutáveis.

A IBM posiciona o LinuxONE como uma família de servidores Linux empresariais para sistemas críticos e cargas de missão crítica [1]. Esta plataforma permite conjugar robustez mainframe com ecossistema Linux, evitando a falsa oposição entre tradição operacional e abertura tecnológica.

4.2 Cofre digital soberano

Para além dos dois centros activos, recomenda-se uma terceira localização com função de cofre digital soberano. Este local pode situar-se no interior ou em território insular, e tem como função conservar backups imutáveis, snapshots cifrados, arquivos críticos e cópias air-gapped.

Alta disponibilidade protege contra falhas previsíveis. Backups imutáveis e isolados protegem contra corrupção lógica, ransomware, erro humano e ataques destrutivos. Confundir uma coisa com a outra é uma excelente maneira de descobrir a diferença durante uma tragédia, que é o método pedagógico preferido da imprevidência humana.

5. Arquitectura lógica

A arquitectura lógica separa claramente três camadas: camada nacional crítica, camada de integração nacional e camada operacional distrital.

```
CAMADA NACIONAL CRÍTICA
Identidade civil | Finanças | Segurança Social | Saúde | Justiça | Protecção Civil
                 |
                 v
CAMADA DE INTEGRAÇÃO NACIONAL
API Gateway | Event Bus | IAM | Catálogo de APIs | Auditoria | Contratos de dados
                 |
                 v
CAMADA OPERACIONAL DISTRITAL
Atendimento local | PostgreSQL local | Cache | Filas persistentes | Modo degradado
```

Esta separação impede que a operação local se transforme em feudo tecnológico e impede que a centralização nacional se torne uma rigidez operacional. O Estado precisa de uma arquitectura capaz de distinguir dados soberanos, serviços críticos, operação local e análise estatística.

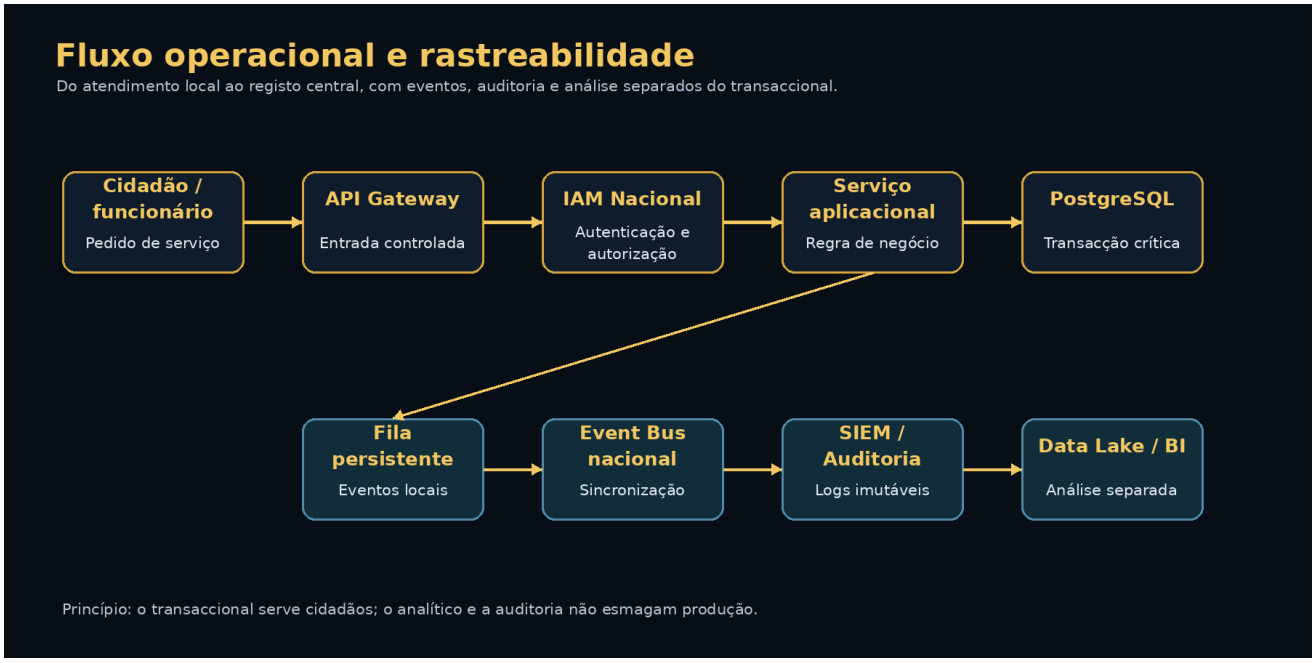

Figura 2 - Fluxo operacional, eventos, auditoria e separação entre transaccional e analítico.

6. Modelo de dados e replicação

A base de dados estratégica proposta é PostgreSQL, não por moda, mas por robustez, maturidade, abertura, capacidade transaccional e ecossistema de alta disponibilidade. A documentação oficial do PostgreSQL descreve soluções para alta disponibilidade, balanceamento e replicação, incluindo cenários em que servidores podem assumir rapidamente a função de primário em caso de falha [2]. O PostgreSQL suporta também replicação lógica com controlo fino sobre objectos e alterações [3], e recuperação point-in-time através de arquivamento contínuo de WAL [4].

6.1 Classificação de dados

Classe	Exemplos	Modelo recomendado
Dados críticos nacionais	Identidade, fiscalidade, segurança social, justiça, saúde essencial, registos fundamentais.	PostgreSQL central, replicação síncrona Lisboa-Porto, RPO próximo de zero.
Dados operacionais distritais	Atendimento local, processos em curso, cache autorizada, documentos pendentes.	PostgreSQL local, sincronização assíncrona, filas persistentes, reconciliação posterior.
Logs e auditoria	Acessos, alterações, eventos de segurança, transacções relevantes.	Streaming contínuo para SIEM, arquivo imutável, retenção definida por lei e risco.
Dados analíticos	BI, estatística, planeamento, IA pública, análise de políticas.	Data lake e data warehouse separados; alimentação por CDC/eventos.

6.2 Replicação por criticidade

Tipo de informação	Modelo de replicação	Objectivo
Dados vitais nacionais	Síncrona Lisboa-Porto	Perda zero ou quase zero, à custa de maior latência.
Dados administrativos	Assíncrona controlada	Escalabilidade e menor impacto operacional.
Dados distritais	Local + sincronização posterior	Continuidade de atendimento em modo degradado.
Logs de auditoria	Streaming contínuo	Rastreabilidade, investigação e responsabilização.
Backups	Imutáveis, cifrados, testados	Recuperação limpa em caso de corrupção ou

		ransomware.

7. Segurança e Zero Trust

A segurança deve ser princípio de desenho, não verniz final para tranquilizar auditorias. O modelo recomendado segue princípios de Zero Trust. O NIST SP 800-207 descreve a arquitectura Zero Trust como uma abordagem que deixa de confiar em perímetros estáticos e passa a focar utilizadores, activos e recursos, aplicando verificação contínua e controlo contextual [5].

- Autenticação forte e MFA para utilizadores e administradores.
- IAM nacional federado, com autorização por função, contexto e risco.
- mTLS entre serviços e API gateways.
- PKI interna e gestão de certificados.
- HSM ou KMS soberano para chaves críticas.
- Gestão central de segredos.
- Segmentação de rede e contenção de movimento lateral.
- SIEM nacional com logs imutáveis.
- Bastion hosts para administração.
- Políticas de menor privilégio.
- Backups cifrados, imutáveis e testados.

8. Observabilidade e operação

Um sistema crítico do Estado deve ser observado em tempo real. A indisponibilidade não deve ser descoberta através de chamadas de cidadãos, rodapés televisivos ou pânico em grupos de WhatsApp. A observabilidade tem de incluir métricas, logs, traces, auditoria, alertas, capacidade disponível e estado de replicação.

Domínio	Indicadores
Serviços	Disponibilidade, tempos de resposta, erros, degradação.
Bases de dados	Lag de replicação, locks, crescimento, I/O, WAL, backups.
Filas e eventos	Mensagens pendentes, atrasos, retries, dead-letter queues.
Segurança	Falhas de autenticação, anomalias, acessos privilegiados, alertas SIEM.
Infra-estrutura	CPU, RAM, rede, storage, energia, temperatura, capacidade.
SLA público	Indicadores por serviço essencial e por região.

9. Continuidade, desastre e recuperação

A arquitectura deve prever falhas, não fingir surpresa perante elas. Falha de data center, falha de comunicação distrital, ataque ransomware, corrupção lógica de dados ou indisponibilidade regional são cenários que devem ser ensaiados. Um plano que nunca foi testado é apenas literatura optimista, e literatura optimista raramente restaura bases de dados.

Figura 3 - Modelo de continuidade, failover e recuperação soberana.

Cenário	Resposta prevista
Falha de Lisboa	Porto assume serviços críticos; tráfego redireccionado; integridade validada; operação monitorizada.
Falha do Porto	Lisboa mantém serviços críticos; componentes dependentes entram em degradação controlada.
Falha de ligação distrital	Nó distrital opera em modo degradado; eventos ficam em fila local; sincronização posterior.
Ransomware	Isolamento, rotação de credenciais, validação de snapshots, recuperação a partir de cofre soberano.
Corrupção lógica	PITR, validação de integridade, auditoria de transacções, restauração selectiva quando possível.

10. Governação técnica

A solução exige uma entidade técnica nacional com autoridade real. Não uma comissão decorativa, nem um observatório de observação, nem uma unidade orgânica que produz relatórios enquanto os sistemas ardem com elegância administrativa. É necessária uma Autoridade Nacional de Arquitectura Digital do Estado.

Funções essenciais

- Definir normas técnicas vinculativas para sistemas críticos.
- Aprovar arquitecturas de organismos públicos antes da contratação.
- Manter catálogo nacional de APIs e contratos de dados.
- Definir padrões de segurança, continuidade e observabilidade.
- Auditar backups, recuperação e exercícios de crise.
- Reduzir dependência de fornecedores e promover reversibilidade contratual.
- Manter equipas internas de arquitectura, segurança, bases de dados, redes e operação.
- Impedir a criação de novos feudos tecnológicos.

11. Plano de implementação

Fase	Nome	Objectivo
Fase 1	Inventário e classificação	Sistemas, dados, dependências, criticidade, fornecedores, riscos e continuidade.
Fase 2	Núcleo nacional	Construção dos data centers Lisboa/Porto, IAM, SIEM, PostgreSQL central, backups imutáveis.
Fase 3	Pilotos distritais	2 a 3 nós distritais, testes de operação local, falha de rede, sincronização e reconciliação.
Fase 4	Migração progressiva	Por domínio funcional; APIs; eventos; desactivação gradual de sistemas redundantes.
Fase 5	Exercícios de crise	Falha de Lisboa, falha do Porto, ransomware, corrupção lógica, operação distrital isolada.

12. Benefícios esperados

- Maior resiliência dos serviços públicos essenciais.
- Continuidade operacional em caso de falha regional ou nacional parcial.
- Menor fragmentação tecnológica.
- Melhor governação de dados.
- Maior soberania tecnológica.
- Redução de dependência de fornecedores proprietários.
- Interoperabilidade por APIs e eventos.
- Segurança transversal e auditável.
- Melhor capacidade de recuperação pós-ransomware.
- Base sólida para estatística, planeamento e IA pública.
- Melhor confiança dos cidadãos nos serviços digitais do Estado.

13. Riscos e mitigação

Risco	Mitigação
Centralização excessiva	Nós distritais resilientes, modo degradado e autonomia operacional controlada.
Latência Lisboa-Porto	Replicação síncrona apenas para dados críticos; assíncrona nos restantes domínios.
Dependência de fornecedor	Linux, PostgreSQL, standards abertos, equipas internas e contratos reversíveis.
Resistência institucional	Autoridade técnica vinculativa e migração gradual por domínio.
Ransomware	Backups imutáveis, cofre soberano, segmentação, Zero Trust e testes regulares.
Caos de integrações	API Gateway, catálogo nacional de APIs, event bus e contratos de dados.

14. Síntese conceptual

A proposta pode ser resumida numa fórmula: dois centros nacionais soberanos, nós distritais resilientes, Linux em toda a infra-estrutura, PostgreSQL como base de dados estratégica, replicação por criticidade, integração por APIs e eventos, segurança transversal e governação nacional de dados.

Ou, de forma ainda mais directa: um Estado com coluna vertebral digital, em vez de uma manta de retalhos informática.

Esta arquitectura não procura brilhar em conferências. Procura funcionar. Não procura parecer moderna. Procura ser resiliente. Não procura substituir pensamento por fornecedor. Procura devolver ao Estado capacidade interna de arquitectura, operação, segurança e continuidade.

A diferença entre ter tecnologia e ter arquitectura é simples: a tecnologia existe quando tudo corre bem; a arquitectura revela-se quando algo falha.

15. Referências técnicas

[1] IBM LinuxONE: https://www.ibm.com/products/linuxone

[2] PostgreSQL - High Availability, Load Balancing, and Replication: https://www.postgresql.org/docs/current/high-availability.html

[3] PostgreSQL - Logical Replication: https://www.postgresql.org/docs/current/logical-replication.html

[4] PostgreSQL - Continuous Archiving and Point-in-Time Recovery: https://www.postgresql.org/docs/current/continuous-archiving.html

[5] NIST SP 800-207 - Zero Trust Architecture: https://csrc.nist.gov/pubs/sp/800/207/final

Assinatura editorial

White paper de Francisco Gonçalves, com coautoria editorial assistida por inteligência artificial. Documento preparado para publicação e discussão no projecto Fragmentos do Caos.

A tese é simples: o Estado português não precisa de mais decoração digital. Precisa de arquitectura, continuidade, soberania, segurança e responsabilidade técnica.