Uma Arquitetura avançada para todos os Sistemas de Informação do Estado Português

Publicado em 2025-11-06 15:25:42

Plataforma Unificada do Estado (PUE): Sumário Executivo

Uma plataforma única, browser-enabled, para todos os serviços públicos — assente em **Linux Ubuntu**, soluções **open-source por omissão**, **segurança máxima por desenho** e **dados soberanos**. Dois **data-centers governamentais**

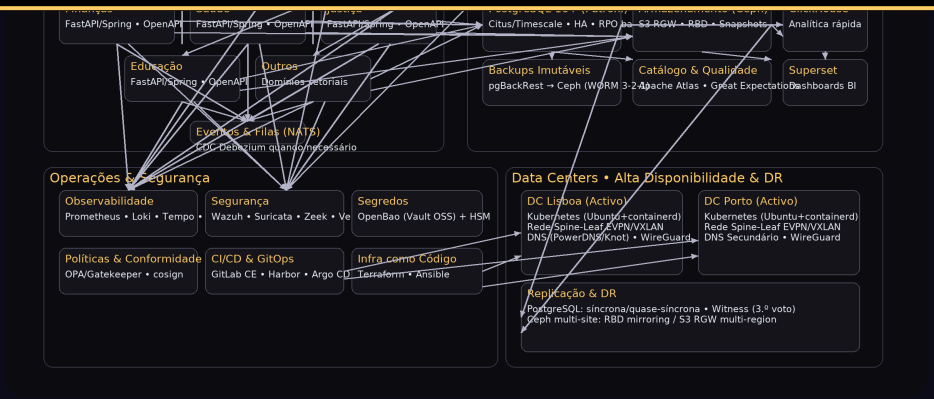
Box de Factos

- **Núcleo**: Kubernetes multi-cluster active-active (Lisboa/Porto), CI/CD declarativo, Infra-as-Code.
- **Identidade**: Keycloak (OIDC/SAML, eIDAS/Cartão de Cidadão), MFA/WebAuthn, RBAC/ABAC.
- **Dados**: PostgreSQL 16+ com Patroni (HA, PITR), Debezium CDC, object-storage Ceph/S3 (WORM para auditoria).
- **Integração**: APIs REST padronizadas (OpenAPI) + eventos NATS; um gateway leve.
- **Observabilidade**: OpenTelemetry → Prometheus/Grafana; logs e traces unificados.
- **Segurança**: hardening CIS, SAST/DAST, Wazuh/SIEM, cifragem total; RGPD por defeito.
- **Metas**: SLO 99,95% por domínio (Identidade 99,99%); p95 leitura ≤ 300 ms, escrita ≤ 800 ms.

Open-Source | Active-Active | Zero-Trust | WCAG 2.2 AA | RPO≈0 / RTO baixo

Terraform/Ansible.

2. **Identidade & Acesso**: Keycloak, MFA/WebAuthn, integração eIDAS/Cartão de Cidadão; RBAC/ABAC, least-privilege.
3. **Dados transaccionais e ficheiros**: PostgreSQL 16+ (Patroni, PITR), Debezium CDC para análise, Ceph/S3 com object-lock (WORM).
4. **Integração simplificada**: contratos OpenAPI e eventos NATS; um gateway governamental leve (rate-limit, auth, observability).
5. **Observabilidade & Segurança**: OpenTelemetry (métricas/traces), Prometheus/Grafana; Wazuh/SIEM, SAST/DAST, secret scanning, hardening CIS.
6. **Experiência digital**: front-ends responsivos, sem plug-ins, **WCAG 2.2 AA**, .ics, notificações e linguagem clara; design-system comum.
7. **IA aplicada**: previsão de procura (slots, picos), detecção de anomalias/fraude, recomendação de capacidade, assistentes de apoio.



PUE - Diagrama Lógico

Demonstração Piloto

Agendamento do Cidadão: mock React (tema escuro, acessível), APIs em OpenAPI, checklist operacional, modelo de dados, cutover e critérios Go/No-Go. Exportação **.ics** e autenticação OIDC simulada.

Vantagens Técnicas

- **Resiliência real**: Active-active Lisboa/Porto, **RPO≈0**, **RTO** reduzido, failover orquestrado.
- **Desempenho previsível**: p95 leitura ≤ 300 ms; escrita ≤ 800 ms; autoscaling guiado por SLO.
- **Segurança por omissão**: cifragem total, least-privilege, WORM para auditoria, RGPD operacionalizado.
- **Interoperabilidade sem cola**: OpenAPI e eventos padronizados; menos gateways, menos atrito.

traces num só plano; problemas visíveis antes de doer.

- **Escalabilidade e eficiência**: contentores densificados, right-sizing automático, custos sob controlo.
- **Qualidade contínua**: SAST/DAST, policy-as-code, canary e progressive delivery.

Vantagens Operacionais

- **Um balcão digital** para múltiplos serviços: queda drástica da fragmentação e “portalite”.
- **Time-to-market** menor: templates de domínio, pipelines e playbooks já testados.
- **Custos directos mais baixos**: licenciamento reduzido, consolidação de infra, suporte simplificado.
- **Disponibilidade elevada**: SLO 99,95% (Identidade 99,99%); comunicação transparente de incidentes.
- **Governança de dados**: catálogos, trilhos de auditoria, retention e anonimização por política.
- **Acessibilidade e inclusão**: WCAG 2.2 AA por defeito, content design e linguagem simples.
- **Operação previsível**: SLO/SLA claros, runbooks e post-mortems com melhoria contínua.

- Do "zoo de portais" para **uma plataforma coerente**.
- Do "cada ministério por si" para **domínios ágeis sobre um núcleo comum**.
- Do "apagar fogos" para **prever e prevenir** com telemetria e IA.

Conclusão. Menos entropia, mais Estado: mais simples para o cidadão, mais sólido para a operação, mais livre para evoluir. É arquitectura para décadas — não para a próxima urgência.

Anexos e Documentação

Pacotes consolidados (ZIP)

PUE_Pacote_TOTAL_v2.zip /span>

PUE_Agendamento_Pacote_Comple

Especificações

openapi-pue-agendamento.yaml em Zip File OpenAPI 3.0

Custos de Implantação, Operação e Licenciamento — Exercício

Notas: valores sem IVA, em euros, com variação ±20% conforme contratação, câmbios, energia e escala. Assumimos plataforma **active-active Lisboa↔Porto**, Linux Ubuntu, **stack aberto** (PostgreSQL, Ceph, Keycloak, Wazuh), **gateway leve** e observabilidade nativa.

Suposições de base

Parâmetro	Hipótese	Observaçõe
Aplicações do Estado	700 (exercício)	Cenários de sensibilidade: 5
Carga IT por data-center	0,6–1,0 MW	PUE alvo ≈ 1,35–1,45 (eficiência).
Energia (€/kWh)	0,14	Tarifa média empresaria contratos rea
Vida útil/refresh HW	4–5 anos	Reserva anual para refres técnica).
Equipa plataforma + segurança + operação	110–140 FTE	Custo médio total/FTE ≈

		etalhe
— 2 DC	M	s, Ceph, re HSM, firewalls.
Obras/MEP DC & rede (adaptações)	5–9 M	Salas, UPS, cooling, cross protecções física
Engenharia de plataforma (setup)	8–12 M	Automação, CI/CD, observabilid runbooks.
Total CAPEX (faixa)	**23–39 M**	

2) OPEX anual — operação dos 2 data-centers

Rubrica	Faixa €/ano	Observações
Energia eléctrica (2 DC)	2,1–3,4 M	0,6–1,0 MW IT por DC; PUE≈1,4 facility por DC.
Equipas (plataforma, SRE, segurança, redes)	7,8–10,0 M	110–140 FTE × 65–75k
Conectividade & DDoS	0,5–1,0 M	Trânsito multi-operador, peeri volumétrica.
Segurança física	0,6–1,0 M	Vigilância, controlo de acessos, sistemas.
Segurança lógica (amenities & threat intel)	0,4–0,8 M	Feeds, testes intrusivos, *b controlado.
Manutenção HW (peças/SLAs)	1,0–1,5 M	≈ 6–10% do CAPEX har

3) Custos de desenvolvimento/migração das aplicações

Modelo por classe de esforço (refactor/rewrite, integração, testes, segurança). Distribuição típica — afinar com inventário real.

Classe	%	Custo por app (€)	Apps (500)	Total (500)	Apps (700)	Total (700)	A (9
Pequena (S)	45 %	50.000	225	11,25 M	315	15,75 M	4
Média (M)	35 %	150.000	175	26,25 M	245	36,75 M	3
Grande (L)	15 %	450.000	75	33,75 M	105	47,25 M	1
Crítica (XL)	5%	1.200.000	25	30,00 M	35	42,00 M	4
Total por cenário				**101,25 M**		**141,75 M**	

Acrescentar 1–2% para formação, gestão da mudança e communication packs (ex.: +1,5% → +1,52 M€ no cenário 700 apps).

		bservaçõe
Ubuntu (suporte enterprise)	0,15–0,30 M	Por nó/ano; depende de
PostgreSQL (suporte/consultoria)	0,20–0,45 M	Por cluster/nível; *tunir
Ceph/S3 (suporte)	0,10–0,25 M	Capacidade e SLA d
Keycloak/ID (suporte)	0,08–0,20 M	Integrações, upgrade se response.
Wazuh/SIEM & *threat intel*	0,15–0,30 M	Feeds, regras, red teamin
Observabilidade (Prometheus/ Grafana, OTEL)	0,10–0,30 M	Se parcialmente SaaS, a c
Cripto/HSM & PKI (quando aplicável)	0,30–0,60 M	HSMs e tokens com m
Total anual (faixa)	**1,1–2,2 M**	**Stack aberto + suport selectivo.**

5) Leituras de síntese

Escopo	Estimativa	Comentário
CAPEX inicial (plataforma+infra)	23–39 M€	Uma vez, com rampa faseada por
		12–24 meses; waves por priorida

[illegible]	M€/ano	[illegible]s, refresh
Licenciamento + suporte **(open-source)**	1,1–2,2 M€/ano	Suporte comercial selectivo, sem fabricantes e marcas comer

Métrica cidadã (ordem de grandeza): se o investimento inicial global rondar ~180 M€, isso equivale a ~17–18 € por cidadão (uma vez), e um OPEX total anual de ~20–22 M€ equivale a ~2 € por cidadão/ano — valores ilustrativos, a validar com inventário e **benchmarks** reais.

Próximo passo: substituir hipóteses por medições — carga IT real, PUE por commissioning, nº exacto de apps por classe, inventário HW e contratos de energia/transporte. Depois, congelar baseline e SLO orçamentais por domínio.

Autoria e Base dos Estudos

Autoria deste Estudo de Viabilidade

Francisco Gonçalves & **Augustus Veritas Lumen**

Co-autoria

Data Publicação: **6 Nov 2025** Versão: **v1.0**

Contacto: https://www.softelabs.pt

active (Lisboa↔Porto); integração por APIs (OpenAPI) e eventos.

- **Stack**: Linux Ubuntu, PostgreSQL 16+ (Patroni/PITR), Ceph/S3 (WORM), Keycloak (OIDC/SAML), OpenTelemetry→Prometheus/Grafana, Wazuh/SIEM.
- **Segurança**: zero-trust, RBAC/ABAC, MFA/WebAuthn; hardening CIS; cifragem em trânsito/repouso; auditoria imutável.
- **Operação**: SLO 99,95% por domínio (Identidade 99,99%); p95 leitura ≤ 300 ms / escrita ≤ 800 ms (exercício).
- **Dados e DC**: dois data-centers governamentais com replicação em tempo real; PUE alvo ~1,35–1,45.
- **Custos**: estimativas por classes de esforço (S/M/L/XL) e faixas CAPEX/OPEX; valores indicativos a validar com inventário real.

Âmbito e limitações

- Exercício técnico-operacional baseado em tecnologias avançadas e robustas e benchmarks do sector; não substitui cotações formais.

semanas) para calibração com métricas reais e congelação de baseline.

Referências e materiais (a inserir)

- OpenAPI — Agendamento do Cidadão: openapi-pue-agendamento.yaml
- Front-end demo (ZIP): pue-agendamento-demo_v2.zip
- Pacote completo: PUE_Agendamento_Pacote_Completo_v1.zip
- Pacote total: PUE_Pacote_TOTAL_v2.zip
- DOCX: Checklist Operacional / Piloto / Anexos (Hardening, SLO/Orçamento de Erros, ADR, Playbooks): http://www.fragmentoscaos.eu/wp-content/uploads/2025/11/PUE_Checklist_Plano_Operacional.docx

Declaração. Este trabalho foi desenvolvido com foco na **total soberania digital de Portugal**, eficiência operacional e **redução de entropia sistémica no Estado.** As estimativas financeiras são de ordem de grandeza e devem ser validadas por medições e cotações oficiais. **Reutilização**