**Plano Operacional de Migração — Domínio Piloto  
Agendamento do Cidadão**

PUE — Plataforma Unificada do Estado

Versão 1.0 • Data: 06/11/2025

# 1. Escopo e Objectivos

Implantar um serviço transversal de marcação de atendimentos para cidadãos e empresas, abarcando múltiplos organismos (p.ex., Registos, Finanças, Segurança Social), com experiência única via PUE, autenticação Keycloak (eIDAS/Cartão de Cidadão), notificações multi‑canal e calendários por serviço e localização.

Objectivos: reduzir tempos de espera; consolidar sistemas de marcação dispersos; garantir acessibilidade WCAG 2.2 AA; obter métricas em tempo real e assegurar continuidade de serviço com replicação inter‑DC.

# 2. MVP e Fora de Escopo

## 2.1 MVP (Primeira Entrega)

• Marcação, remarcação e cancelamento de agendamentos por canal web (PUE).

• Gestão de slots por serviço e posto (capacidade, duração, janelas).

• Notificações por e‑mail/SMS; ficheiro .ics para calendário pessoal.

• Painel operacional (no‑show, taxa de ocupação, SLA de atendimento).

## 2.2 Fora de Escopo (nesta fase)

• Pagamentos associados ao agendamento (a incluir em fase posterior, se necessário).

• Integrações com sistemas legados que não disponibilizem dados minimamente consistentes.

# 3. Actores e Jornadas

• Cidadão/Empresa: pesquisa por serviço/local, selecciona slot, confirma e recebe comprovativo.

• Atendedor/Operador: abre calendário, ajusta capacidade, faz \*overbooking\* controlado.

• Administrador de Serviço: configura regras, horários, feriados e tipologias.

• Plataforma (automação): envia lembretes, aplica políticas de \*no‑show\*, gera relatórios.

# 4. Requisitos Não‑Funcionais e SLO

• Disponibilidade alvo (SLO): 99,95%/30 dias; Identidade: 99,99%.

• Latência p95: ≤ 300 ms para operações de leitura; ≤ 800 ms para criação de agendamento.

• Erro ≤ 0,1% das requisições; \*throttling\* e \*backoff\* no gateway.

• Acessibilidade: WCAG 2.2 AA; testes de leitor de ecrã e contraste.

# 5. Modelo de Dados (alto nível)

|  |  |  |
| --- | --- | --- |
| Entidade | Atributos‑chave | Notas |
| Serviço | service\_id, nome, tipologia, requisitos | Catálogo de serviços por organismo. |
| Local/Posto | site\_id, morada, geografia, capacidade | Mapeamento para filas físicas. |
| Calendário | calendar\_id, janelas, feriados, \*blackout\* | Regras por serviço/posto. |
| Slot | slot\_id, inicio, fim, capacidade, estado | Disponibilidade calculada + reservas. |
| Agendamento | appt\_id, citizen\_id, service\_id, slot\_id, estado | Estados: activo, remarcado, cancelado, no‑show. |
| Cidadão | uuid, NIF/ID, contacto, consentimento | Dados mínimos; encriptação em repouso. |

# 6. API (contratos principais)

|  |  |  |  |
| --- | --- | --- | --- |
| Método | Endpoint | Descrição | Auth |
| GET | /v1/services | Listar serviços e requisitos. | Público |
| GET | /v1/slots?service\_id&site\_id&date | Consultar slots disponíveis. | Público |
| POST | /v1/appointments | Criar agendamento. | OIDC (Cidadão) |
| PATCH | /v1/appointments/{id} | Remarcar/alterar dados. | OIDC (Cidadão) |
| DELETE | /v1/appointments/{id} | Cancelar. | OIDC (Cidadão) |
| POST | /v1/appointments/{id}/notify | Reenviar comprovativo/ICS. | Operador |

# 7. Integrações

• Identidade: Keycloak (OIDC), MFA/WebAuthn; atributos mínimos (uuid, nome, e‑mail, NIF opcional).

• Notificações: serviço de e‑mail e SMS governamental; \*templates\* por idioma.

• Calendários: exportação ICS; \*webhooks\* para sincronização interna (NATS eventos).

• Dados: PostgreSQL 16+ (Patroni); \*CDC\* Debezium para replicação analítica; Ceph S3 para anexos.

# 8. Migração de Dados (do legado)

• Inventariar sistemas actuais de marcação; avaliar qualidade e \*mapping\* para o novo modelo.

• Planear migração incremental: apenas agendamentos futuros + últimas 8 semanas de histórico (RGPD).

• Regras de limpeza: normalizar contactos, remover duplicados por hash (NIF+data+serviço).

• \*Dry run\* em \*staging\* com relatórios de discrepâncias e correções.

|  |  |  |  |
| --- | --- | --- | --- |
| Fonte | Tabelas | Registos (estim.) | Estado |
| Sist. A (Min. X) | appointments, slots, users | 120 000 | A mapear |
| Sist. B (Min. Y) | bookings, locations | 45 000 | Extract pronto |

# 9. Segurança e RGPD

• Dados pessoais mínimos; encriptação AES‑GCM em repouso e TLS 1.3 em trânsito.

• Retenção: 24 meses para \*audit trail\*; anonimização dos registos aos 12 meses salvo obrigação legal.

• \*Consent logs\* por canal; \*DPIA/LIA\* concluídas; \*least privilege\* e \*NetworkPolicies\* por namespace.

• Auditoria: logs imutáveis (WORM), correlação no SIEM (Wazuh).

# 10. Testes e Aceitação

• Funcionais: CRUD completo de agendamento; regras de conflito de slots; políticas de \*no‑show\*.

• Carga: 1 000 RPS leitura, 150 RPS criação; \*spikes\* em T‑24h de campanhas públicas.

• Acessibilidade: teclado, ARIA, contraste e suporte a leitores de ecrã verificados.

• Segurança: DAST/ZAP \*baseline\*, \*secrets scanning\* (Gitleaks), SAST no pipeline.

# 11. Operação e Suporte

• Alertas primários: p95 latência, taxa de erros, saturação DB, filas de \*jobs\* de notificações.

• \*Runbooks\*: falha de gateway, \*drain\* de nós K8s, \*failover\* Patroni, reenvio massivo de SMS.

• Helpdesk: \*scripts\* de 1.º nível e \*FAQ\* PUE; \*status page\* pública com incidentes.

# 12. Cutover — Checklist Específica

T−7 dias: congelar alterações nos sistemas legados; gerar \*snapshot\* de slots/agenda.

T−1 dia: \*dry run\* final; enviar comunicação a utentes com agendamentos T+7.

T±0: executar migração; \*smoke tests\* (pesquisa, reservar, cancelar); monitorização apertada 2 h.

T+1/T+7: relatórios de adesão, \*no‑show\*, queima de orçamento de erros; \*post‑mortem\* se necessário.

# 13. RACI (Domínio Piloto)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tarefa | Responsável (R) | Aprovador (A) | Consultado (C) | Informado (I) |
| Modelação de dados | DBA Domínio | Arq. Dados | Negócio, Segurança | Equipa Plataforma |
| Desenho de APIs | Equipa Domínio | Arq. Aplicacional | Plataforma, Segurança | Negócio |
| Migração de dados | Equipa Domínio | Gestor Programa | DBA, Segurança | Negócio |
| Testes WCAG | UX/QA | Gestor Domínio | Negócio | Plataforma |

# 14. Go/No‑Go — Condições para Produção

• SLOs cumpridos em \*staging\* durante 7 dias; sem \*P1\* abertas; DR test (PITR) validado.

• Aprovação de acessibilidade (WCAG AA) e de segurança (DAST/SAST sem críticos).

• Helpdesk preparado; comunicação ao público pronta; \*rollback\* ensaiado.

# 15. Indicadores de Sucesso (KPIs)

• Tempo médio de marcação < 2 minutos; \*drop‑off\* no funil < 10%.

• \*No‑show\* < 8% (com lembretes automáticos); taxa de ocupação de slots > 85%.

• Satisfação do utente ≥ 4/5; taxa de erro < 0,1%.