Desafio: E-VEILING

Edital: CPSI

1. O Desafio (Solução Inovadora)

Uma plataforma inteligente para o Velamento de Fundações integra uma interface de gestão centralizada com um aplicativo móvel de fiscalização in loco. Esta solução consolida dados financeiros, processuais e administrativos de múltiplas fontes, permitindo inspeções técnicas offline com garantia de integridade e padronização de relatórios.

2. Objetivo

Desenvolvimento de solução multimodal (Mobile/Web) com arquitetura Offline-First para suporte a inspeções de campo.

A solução deve consolidar dados de patrimônio, processos e regularidade fiscal; implementar geolocalização e registro fotográfico imutável; gerar painéis de saúde financeira com alertas de insolvência; automatizar relatórios de inspeção integrados; e permitir a interoperabilidade de dados com outros Ministérios Públicos e órgãos de controle.

3. Oportunidades de Mercado

Mercado potencial composto pelas 26 outras unidades do Ministério Público Estadual (MPE) e pelo Ministério Público do Distrito Federal e Territórios (MPDFT), que possuem atribuições idênticas de fiscalização de fundações.

Solução com alta aderência também para o setor privado, incluindo empresas de auditoria, escritórios de compliance e conselhos municipais de assistência social e educação.

4. Requisitos Funcionais

ID	Descrição	PoC	Homologação
01	Disponibilização de aplicativo (Mobile/PWA) operando em arquitetura Offline-First com persistência local de dados criptografada.	Sim	Sim
02	Preenchimento de formulários estruturados (checklists incluindo campos para dados cadastrais, governança, saúde	Sim	Sim

ID	Descrição	PoC	Homologação
	financeira, CEBAS, processos cíveis/trabalhistas e regularidade fiscal) parametrizáveis e de texto livre, com suporte a validação de campos em tempo real.		
03	Interface de coleta de dados multimodal (texto, imagem e áudio), com recurso de transcrição de voz para texto executado de forma estritamente local no dispositivo móvel (on-device) durante o modo offline, sem qualquer dependência de conectividade ou serviços de nuvem para o processamento básico.	10	15
04	Captura de evidências fotográficas diretamente pela interface do aplicativo.	15	15
05	Funcionalidade de ingestão prévia de relatórios da inspeção anterior realizada.	10	10
06	Módulo de Geração Automatizada de Relatórios de Inspeção, em formato editável, com base nos dados coletados.	Sim	Sim
07	Parametrização dinâmica: campo para o usuário inserir prompts definindo o tamanho, o estilo e o escopo do texto gerado pela IA para o relatório.	20	25
08	Ferramenta para conversão do	15	15

ID	Descrição	PoC	Homologação
	documento já editado em formato PDF.		
09	Suporte à assinatura eletrônica/digital no relatório gerado.	15	15
10	Possibilidade de fluxo de encaminhamento automático do relatório via e-mail.	15	15
11	Funcionalidade de georreferenciamento das fundações com visualização em mapa.	15	15
12	Disponibilização de filtros no mapa por status de regularidade (fiscal, processual, CEBAS) e por intervalo de data da última inspeção.	10	10
13	Injeção obrigatória e irreversível de metadados de estampa de tempo (Timestamp auditável) em todas as mídias coletadas.	15	15
14	Sincronização automática ou sob demanda dos dados coletados offline com a base de dados centralizada da aplicação assim que a conectividade for restabelecida.	15	15
15	Resolução inteligente de conflitos de sincronização (ex: múltiplos usuários editando dados da mesma unidade em horários distintos).	10	20
16	Motor de validação em tempo real: emissão de alerta visual na interface ao detectar discrepância numérica (ex: >20%) entre a coleta atual e a base histórica extraída.	25	40

ID	Descrição	PoC	Homologação
17	Capacidade de exportação de todas as tabelas de dados coletados em formatos tabulares e estruturados (JSON e CSV) para integração com sistemas de Business Intelligence do MPRS.	15	15

5. Requisitos Técnicos

ID	Item	Descrição	PoC	Homologação
01	-	Arquitetura Simplificada (MVP): Solução funcional demonstrando fluxos essenciais.	Sim	-
02	6.2.1	Segregação lógica: Isolamento absoluto de dados e interações.	Sim	Sim
03	6.2.2	Segurança da informação: Vedação de credenciais no código, comunicação via HTTPS com TLS 1.2 ou superior, quando aplicável. Autenticação integrada à Microsoft Entra ID, por meio de protocolos padronizados de autenticação e autorização (ex.: OAuth 2.0 ou equivalentes).	-	Sim
04	6.2.3	Autenticação Avançada: Configurável por perfil e obrigatória para administradores, quando houver interface administrativa, console de gestão ou operações privilegiadas. Deverá ser compatível com provedores de identidade institucionais.	-	Sim

ID	Item	Descrição	PoC	Homologação
05	6.2.4	Controle de Acesso (RBAC): Implementação de RBAC para segmentação granular e rastreabilidade.	-	Sim
06	6.2.5	Gestão de Segredos: Cofres (Vaults) com política de rotação de chaves. Aplicável quando a solução realizar armazenamento, processamento ou integração com credenciais, chaves, tokens de acesso ou segredos operacionais sensíveis. Em ambientes on-premise, admite-se o uso de mecanismos institucionais equivalentes do MPRS	-	Sim
07	6.2.6	Proteção de Rede: Defesa contra OWASP Top 10, quando aplicável à arquitetura proposta. Soluções com APIs, acesso externo ou serviços em nuvem deverão implementar rate limiting e mitigação contra DoS/DDoS. Soluções SaaS, cloud ou híbridas, a proteção de infraestrutura será responsabilidade da proponente.	-	Sim
08	6.2.7	Arquitetura API First: Disponibilizando interfaces padronizadas e interoperáveis (ex.: REST, GraphQL, gRPC ou equivalentes), com autenticação segura, documentação técnica e versionamento controlado.	Sim	Sim
09	6.2.8	Conteinerização e Serverless: Imagens Docker/OCI com	-	Sim

ID	Item	Descrição	PoC	Homologação
		execução portável, permitindo serviços gerenciados/serverless e rollback.		
10	6.2.9	Escalabilidade Horizontal: Quando aplicável à arquitetura da solução, balanceamento dinâmico para garantir escalabilidade.	-	Sim
11	6.2.10	Observabilidade: Quando aplicável à arquitetura da solução, emissão de métricas, logs e traços (OpenTelemetry ou equivalente).	-	Sim
12	6.2.11	FinOps (Gestão de Consumo) : Para itens com tarifação variável ou consumo elástico de recursos, limites/quotas parametrizáveis, alertas de consumo, rateio/atribuição e relatórios de auditoria financeira.	-	Sim
13	6.3.1	Trilhas de Auditoria Básicas: Garantia de integridade e rastreabilidade das operações.	-	Sim
14	6.3.2	Computação Forense (WORM): Armazenamento de logs em padrão WORM, integridade garantida por hash/criptografia e rastreabilidade da cadeia de custódia.	-	-
15	6.3.3	Inventário SBOM: Documentação SBOM (SPDX ou CycloneDX).	Sim	Sim
16	6.4.1	Prevenção a Injeção e Vazamento: Quando aplicável a soluções que utilizem modelos de Inteligência Artificial generativa ou LLMs, proteção contra	-	Sim

ID	Item	Descrição	PoC	Homologação
		manipulação (jailbreak) e vazamento de system prompts.		
17	6.4.2	Mitigação de Alucinações (Grounded Generation): Condicionar respostas às fontes e evitar invenção de fatos/normativas, quando aplicável à arquitetura da solução.	Sim	Sim
18	6.4.2.1	Metodologia de Aferição Objetiva: durante a avaliação, a solução será submetida a um Dataset de Validação fornecido pelo MPRS.	Sim	Sim
19	6.4.2.2	Critério de Aceite: Quando aplicável a soluções que utilizem modelos de Inteligência Artificial generativa ou LLMs, o desempenho será aferido pela métrica HAM (Hallucination Rate), com HAM máximo de 10% sobre o conjunto de testes.	-	Sim
20	6.4.3	Avaliação Contínua e Fine-Tuning: Quando aplicável a soluções baseadas em IA generativa ou RAG, uso de frameworks de qualidade técnica (como RAGAS) medindo fidelidade e consistência.	-	Sim
21	6.4.4	Trilha de Justificativa de IA: Rastreabilidade de ID, fontes/referências, parâmetros da execução e motivos de bloqueio, quando aplicável à arquitetura da solução.	Sim	Sim
22	6.4.6	Vedações Operacionais Mínimas:	-	Sim

ID	Item	Descrição	PoC	Homologação
		Bloqueio de respostas com "aparência de certeza" sem verificação, vedação de uso de dados reais não autorizados e bloqueio contra desativação de segurança por comandos, quando aplicável à arquitetura da solução.		
23	6.4.6	Agnosticismo de Modelo de IA: Possibilidade de troca do LLM, quando aplicável à arquitetura da solução.	-	Sim
24	6.4.7	Gestão de Prompts e Capacitação: Repositório versionado com controle de acesso e fornecimento de manuais/playbooks, quando aplicável à arquitetura da solução.	-	Sim
25	6.4.8	Agentes Autônomos em Sandbox: Atuação de agentes autônomos em sandbox com limites configuráveis de autonomia e recursos, e bloqueio auditável de operações sensíveis ou escalonamento indevido de privilégios, quando aplicável à arquitetura da solução.	-	Sim
26	6.4.9	Métricas de Mídia: Aferição pela métrica WER (Word Error Rate), com WER máximo de 10% em conjunto de testes.	-	Sim
27	6.2.12	Processamento Paralelo e Execução Assíncrona: Quando aplicável à solução, suportar processamento paralelo e execução assíncrona, evitando bloqueios sequenciais e degradação do fluxo	-	Sim

ID	Item	Descrição	PoC	Homologação
		principal por chamadas externas ou tarefas de longa duração.		
28	6.4.10	Métricas de OCR: Aferição pela métrica CER (Character Error Rate), com CER máximo de 5% em conjunto de testes.	-	Sim