Desafio: MBA Digital

Edital: CPSI

1. O Desafio (Solução Inovadora)

Uma aplicação móvel padronizada centralizará a coleta de evidências digitais, registrando achados com metadados em tempo real e automatizando a documentação. Esta plataforma integrará anotações, fotografias e gravações, garantindo a integridade da cadeia de custódia e a rastreabilidade dos elementos coletados.

2. Objetivo

Disponibilizar solução digital integrada, com foco em mobilidade, destinada a padronizar e acelerar o cumprimento de mandados de busca e apreensão.

A ferramenta deve permitir o registro estruturado de ambientes, objetos e materiais com captura de fotos, vídeos e metadados georreferenciados, assegurando a imutabilidade dos dados e a preservação da cadeia de custódia.

A solução deverá gerar automaticamente documentos formais — como autos circunstanciados e termos de apreensão — a partir dos dados coletados em campo, reduzindo o tempo de resposta e viabilizando futura integração com sistemas internos e judiciais.

3. Oportunidades de Mercado

Segurança Pública e Ministérios Públicos: Aplicabilidade em todos os MPs estaduais, MPU e polícias judiciárias que executam ordens de busca.

Órgãos de Fiscalização: Uso por agências reguladoras e órgãos de controle que exerçam atividade de polícia administrativa em inspeções de campo que exijam fé pública e registro imutável.

Setor Privado (Compliance): Auditorias corporativas e vistorias de seguros que demandam registros periciais com integridade de dados.

4. Requisitos Funcionais

ID	Descrição	PoC	Homologação
01	Interface Responsiva: Otimizada para smartphones e tablets (iOS/Android).	Sim	Sim
02	Assinatura no Dispositivo: Coleta de assinaturas (membro, testemunhas, investigado).	15	Sim

ID	Descrição	PoC	Homologação
03	Georreferenciamento Nativo: Inclusão automática de coordenadas GPS em cada foto e vídeo.	Sim	Sim
04	Timestamp Inviolável: Carimbo de tempo sincronizado com fontes oficiais (NTP) em cada artefato, contendo mecanismo de proteção contra alteração de hora do dispositivo em caso de operação offline.	10	Sim
05	Captura Multimídia: Fotos e vídeos com metadados de integridade (EXIF/Hash).	Sim	Sim
06	Revisão de Rascunho em Tela: Funcionalidade de consolidação, visualização e edição em tela dos dados coletados para revisão e ajustes pelo usuário antes da geração do documento final.	10	Sim
07	Cadeia de Custódia Digital: Registro imutável de cada ato de apreensão por meio de hashing criptográfico e assinatura digital dos artefatos, garantindo a rastreabilidade sem dependência de infraestrutura de blockchain.	-	50
08	Cadastramento via QR Code: Geração e vinculação de códigos únicos para cada artefato.	20	40
09	Leitura e Classificação: Captura de QR Codes de lacres físicos para inventário rápido.	15	30

ID	Descrição	PoC	Homologação
10	Modo Offline-First: Operação total em locais sem conectividade.	15	Sim
11	OCR de Documentos: Extração de texto de documentos físicos apreendidos.	-	30
12	Transcrição de Áudio e Vídeo: Narração de achados convertida em texto para o auto.	15	25
13	Integração via API: Exportação de dados estruturados e documentos para os sistemas de gestão do MPRS via REST/JSON.	-	Sim
14	Reconhecimento de Objetos (IA): Sugestão de classificação de armas e drogas.	-	35
15	Checklist Procedimental: Validação de etapas para evitar nulidades.	Sim	Sim
16	Impressão Bluetooth: Emissão de etiquetas de QR Code em impressoras térmicas.	-	30
17	Dashboard Tático: Visão em tempo real das apreensões para a chefia.	10	20
18	Geração Automatizada de Documentos Formais: Geração imediata de arquivos PDF formatados conforme padrões do MPRS, incluindo o Auto Circunstanciado (com descrição detalhada, fotos e metadados) e o Termo de Apreensão (com a listagem simplificada dos itens para entrega ao	Sim	Sim

ID	Descrição	PoC	Homologação
	investigado).		

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
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	-	Sim

ID	Item	Descrição	PoC	Homologação
		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		
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 execução portável, permitindo serviços gerenciados/serverless e rollback.	-	Sim
10	6.2.9	Escalabilidade Horizontal: Quando aplicável à arquitetura da solução, balanceamento	-	Sim

ID	Item	Descrição	PoC	Homologação
		dinâmico para garantir escalabilidade.		
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.	Sim	Sim
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 manipulação (jailbreak) e vazamento de system prompts.	-	Sim
17	6.4.2	Mitigação de Alucinações (Grounded Generation): Condicionar respostas	Sim	Sim

ID	Item	Descrição	PoC	Homologação
		às fontes e evitar invenção de fatos/normativas.		
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.	Sim	Sim
22	6.4.6	Vedações Operacionais Mínimas: 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.	-	Sim
23	6.4.6	Agnosticismo de Modelo de IA: Possibilidade de troca	-	Sim

ID	Item	Descrição	PoC	Homologação
		do LLM		
24	6.4.7	Gestão de Prompts e Capacitação: Repositório versionado com controle de acesso e fornecimento de manuais/playbooks	-	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.	-	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	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 principal por chamadas externas ou tarefas de longa duração.	-	Sim
28	6.4.10	Métricas de OCR: Aferição pela métrica CER (Character Error Rate), com CER máximo de 5% em conjunto de testes.	Sim	Sim