Desafio: Custódia de Prova Digital

Edital: CPSI

1. O Desafio (Solução Inovadora)

A solução consiste em uma plataforma digital que integra mecanismos avançados de prova de integridade, utilizando estruturas de dados imutáveis ou descentralizadas, e gestão de acesso auditável. Esta plataforma assegura a custódia de aquisições forenses e relatórios processados, com backup criptografado, indexação e funcionalidades para compartilhamento seguro e visualização controlada de provas.

2. Objetivo

Disponibilizar solução tecnológica para custódia segura de vestígios digitais (mídia bruta e relatórios), assegurando integridade e governança em conformidade com o CPP.

A solução deverá permitir:

(i) armazenamento criptografado (on-premises ou nuvem) com gestão de chaves;
(ii) diferenciação entre aquisição forense original e cópia processada;
(iii) validação automática de hashes em todas as etapas;
(iv) registro de cadeia de custódia em logs imutáveis (padrão WORM) por no mínimo 5 anos;
(v) controle de acesso via Microsoft Entra ID com MFA.

Adicionalmente, a ferramenta deve oferecer:

(vi) backup automatizado e criptografado;
(vii) disponibilização rastreável ao Judiciário e Defesa via link seguro ou integração com sistemas de processo eletrônico;
(viii) geração de relatórios técnicos de custódia com metadados completos; e
(ix) arquitetura 'API First' (OpenAPI 3.0) para integração com o ecossistema do MPRS, garantindo agnosticismo de infraestrutura e escalabilidade.

3. Oportunidades de Mercado

Validade da prova digital é o pilar central do processo penal moderno.

Com a positivação da cadeia de custódia no CPP, a demanda por soluções que evitem a “quebra da confiança’ da prova tornou-se universal no setor público.

Soluções genéricas de storage são inadequadas para o rigor forense, criando um mercado interessante para ferramentas especializadas em custódia digital.

A solução possui alto potencial de replicabilidade para os 26 Ministérios Públicos Estaduais, o MPF, Polícias Civis e Federal, todos submetidos à mesma legislação federal.

4. Requisitos Funcionais

ID	Descrição	PoC	Homologação
1	Gestão de Casos com vinculação de Membro responsável, autorização de perfis visualizadores e geração de links de acesso auditáveis para terceiros (Judiciário/Defesa).	10	15
2	Interface web para execução dos fluxos de ingestão, verificação de integridade e exportação, com sinalização de status das operações em tempo real.	5	10
3	Ingestão segura e auditável de vestígios e evidências digitais, com suporte a formatos forenses padrão (UFDR, IPED, dumps estruturados), registro automático de metadados e hash na entrada, com diferenciação entre aquisição forense original e cópias processadas.	15	25
4	Geração e armazenamento imutável de hash criptográfico (SHA-256 ou superior) para cada vestígio digital no momento da ingestão.	10	10
5	Criptografia de arquivos antes do tráfego para o provedor de nuvem, utilizando chaves locais ou simuladas na fase de PoC, e integração com HSM ou cofre de chaves institucional na fase de Homologação.	5	15
6	Verificação automática de	10	15

ID	Descrição	PoC	Homologação
	integridade (hash) nas operações de exportação e disponibilização, com alerta em caso de discrepância.		
7	Controle de integridade contínuo com verificação periódica automática dos arquivos armazenados.	-	10
8	Controle de acesso baseado em perfis funcionais (RBAC), garantindo a segregação de funções entre Administrador, Técnico Forense, Visualizador e Auditor.	-	10
9	Registro de trilhas de auditoria completas e imutáveis para todas as operações críticas sobre os vestígios, contendo identificação do usuário, endereço IP, porta lógica e timestamp.	-	10
10	Disponibilização de aquisição forense original e cópia processada ao Poder Judiciário e à defesa: disponibilização separada e rastreável, mediante requisição formal, com registro do ato, identificação do destinatário, endereço IP, porta lógica, data/hora e recibo com hash verificável.	10	20
11	Integração ou simulação de integração com sistemas do Poder Judiciário para upload de cópias processadas e	-	15

ID	Descrição	PoC	Homologação
	protocolos de disponibilização da aquisição forense original.		
12	Link seguro e temporário da aquisição forense original e cópia processada ao Poder Judiciário e à defesa para download.	5	10
13	Disponibilização por mídia física criptografada: geração de pacote criptografado (AES-256) para entrega em casos em que o volume inviabilize a transferência em rede, com hash do conteúdo, documento de entrega e registro auditável no histórico do Caso.	-	10
14	Cadastro de operações investigativas com vinculação estruturada dos vestígios digitais a cada Caso.	5	10
15	Geração de relatórios técnicos de custódia com identificação do caso, descrição do material, metadados, hashes e histórico de movimentações.	5	10
16	Backup automatizado e criptografado (AES-256), com periodicidade configurável.	-	15
17	Suporte a Resumable Uploads (Protocolo TUS ou similar) para arquivos de grande volume (Gigas/Terabytes), garantindo a continuidade em caso de falha de rede.	5	15

ID	Descrição	PoC	Homologação
18	Geração automática de Relatório de Cadeia de Custódia em formato PDF/A, contendo o histórico cronológico de todas as interações, hashes de entrada/saída e identificação de responsáveis, com assinatura digital da aplicação.	-	15
19	Criptografia no lado do cliente (Zero-Knowledge) para armazenamento em nuvem, garantindo que o provedor não possua acesso às chaves de decriptografia dos vestígios.	-	15
20	Imutabilidade Lógica da Mídia Bruta: Implementação de travas de software que impeçam qualquer operação de edição ou exclusão (WORM lógico) sobre os arquivos classificados como 'aquisição forense original', permitindo apenas a leitura e a cópia para processamento.	10	15

5. Requisitos Técnicos

ID	Item	Descrição	PoC	Homologação
01	-	Arquitetura Simplificada (MVP): Solução funcional demonstrando fluxos essenciais.	Sim	-
02	-	Segregação lógica: Isolamento absoluto de dados e interações.	Sim	Sim
03	-	Segurança da	-	Sim

ID	Item	Descrição	PoC	Homologação
		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).		
04	-	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	Sim
05	-	Controle de Acesso (RBAC): Implementação de RBAC para segmentação granular e rastreabilidade.	-	Sim
06	-	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-premises, admite-se o uso de mecanismos institucionais equivalentes do MPRS	-	Sim
07	-	Proteção de Rede: Defesa contra OWASP	-	Sim

ID	Item	Descrição	PoC	Homologação
		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.		
08	-	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	-	Conteinerização e Serverless: Imagens Docker/OCI com execução portável, permitindo serviços gerenciados/serverless e rollback.	-	Sim
10	-	Escalabilidade Horizontal: Quando aplicável à arquitetura da solução, balanceamento dinâmico para garantir escalabilidade.	-	Sim
11	-	Observabilidade: Quando aplicável à arquitetura da solução, emissão de métricas, logs e traços (OpenTelemetry ou equivalente).	-	Sim
12	-	FinOps (Gestão de Consumo): Para itens com tarifação variável ou consumo elástico de recursos, limites/quotas parametrizáveis, alertas de consumo,	-	Sim

ID	Item	Descrição	PoC	Homologação
		rateio/atribuição e relatórios de auditoria financeira.		
13	-	Trilhas de Auditoria Básicas: Garantia de integridade e rastreabilidade das operações.	-	Sim
14	-	Computação Forense (WORM): Armazenamento de logs em padrão WORM, integridade garantida por hash/criptografia e rastreabilidade da cadeia de custódia.	Sim	Sim
15	-	Inventário SBOM: Documentação SBOM (SPDX ou CycloneDX).	Sim	Sim
16	-	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	-	Mitigação de Alucinações (Grounded Generation): Condicionar respostas às fontes e evitar invenção de fatos/normativas.	Sim	Sim
18	-	Metodologia de Aferição Objetiva: durante a avaliação, a solução será submetida a um Dataset de Validação fornecido pelo MPRS.	Sim	Sim
19	-	Critério de Aceite:	Sim	Sim

ID	Item	Descrição	PoC	Homologação
		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.		
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
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 do LLM	-	Sim
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	-	Sim

ID	Item	Descrição	PoC	Homologação
		limites configuráveis de autonomia e recursos, e bloqueio auditável de operações sensíveis ou escalonamento indevido de privilégios.		
26	6.4.9	Métricas de Mídia: Aferição pela métrica WER (Word Error Rate), com WER máximo de 10% em conjunto de testes.	-	-
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.	-	-