

Desafio: CAO-LM

Edital: CPSI

1. O Desafio (Solução Inovadora)

A solução é uma plataforma unificada de gestão de conhecimento institucional, dotada de inteligência artificial para indexação semântica e taxonomia multidimensional. Esta plataforma oferece pesquisa transversal avançada, síntese automatizada de documentos e captura estruturada de debates jurídicos colaborativos.

2. Objetivo

Desenvolver e implementar a solução inovadora denominada Atena.IA, plataforma web conversacional que funciona como um Hub Temático de Conhecimento e um ambiente de Comunidade de Prática para o MPRS. A solução deve utilizar Inteligência Artificial Generativa (RAG), Processamento de Linguagem Natural (NLP) e uma arquitetura de orquestração de múltiplos agentes especializados para transformar a gestão da informação, operando sobre o acervo de dados dos Centros de Apoio Operacional (CAOs). A arquitetura deve permitir o processamento encadeado de requisições através de trilhas de agentes especializados, garantindo a formulação de respostas com contraditório interno e verificação rigorosa de fontes, com foco na validação de teses e busca inteligente. A plataforma deve permitir a ingestão contínua de conteúdos multimodais, cruzar essas informações de entrada com o acervo institucional e analisar criticamente os documentos frente ao acervo dos CAOs, sendo capaz de gerar artefatos precisos e fundamentados, sem risco de alucinação ou inconsistência técnica. A iniciativa visa promover a padronização e a elevação da qualidade técnica das peças processuais em todas as promotorias e procuradorias do Estado, democratizando o acesso ao conhecimento especializado dos CAOs, com foco em alta disponibilidade, segurança e prevenção de falhas.

3. Oportunidades de Mercado

Arquitetura desenvolvida para a plataforma Atena.IA possui altíssimo potencial de escalabilidade e aplicabilidade interinstitucional, abrangendo diversos setores: MPRS (Validação Inicial) com implementação e validação para aproximadamente 5.000 usuários qualificados, incluindo membros e servidores; Ecossistema de Justiça Público com expansão para os demais 26 Ministérios Públicos Estaduais, ramos do Ministério Público da União (MPU), Defensorias Públicas e Tribunais de Justiça; Administração Pública e Controle através da adoção por Ministérios, Agências Reguladoras e Tribunais de Contas para difusão de pareceres normativos; e Setor Privado e Advocacia (LegalTech) com comercialização para grandes bancas de advocacia, consultorias e departamentos de inteligência comercial.

4. Requisitos Funcionais

ID	Descrição	PoC	Homologação
01	Integracao como aplicativo ou Bot conversacional, especializado no banco de dados dos CAOs para consultas em linguagem natural (NLP), com modulo integrado a interface do Microsoft Teams (admitindo-se simulador web na fase de PoC).	Sim	Sim
02	Interface capaz de interpretar jargão jurídico, abreviações forenses e linguagem natural.	Sim	Sim
03	Interface com painel consolidado (Web e Teams) contendo informacoes gerais, chat e modulo 'Estudio' simplificado para geracao automatizada de sumarios executivos baseados no conteudo pesquisado, postergando artefatos complexos para fases posteriores.	-	Sim
04	Interface administrativa web para upload de documentos, gestão de metadados, curadoria de conteúdo e exportação de relatórios de usabilidade e consumo em formatos estruturados (CSV/JSON).	10	Sim

ID	Descrição	PoC	Homologação
05	Módulo de busca híbrida (vetorial e por palavras-chave) com suporte a filtros facetados baseados na taxonomia institucional e respostas baseadas exclusivamente nas fontes institucionais. Recusa explícita de resposta quando a base não contiver a informação, prevenindo invenções. Exibição de hiperlinks e citação precisa das fontes institucionais nas respostas geradas.	Sim	Sim
06	Módulo de ingestão e processamento de documentos estruturados e desestruturados (PDF, DOCX, TXT), com capacidade de classificação taxonômica automatizada e sumarização. Na fase de Homologação, incluir suporte a formatos adicionais (HTML, PPTX, MD, JSON, MP3, MP4), extração de tabelas complexas, OCR para peças digitalizadas e identificação automatizada de duplicidades.	Sim	Sim
07	Módulo de alerta de obsolescência para documentos que atinjam data de validade ou cite leis revogadas, fluxo de aprovação (Human-in-the-loop) para curadores validarem rascunhos antes da	-	40

ID	Descrição	PoC	Homologação
	publicação e controle de versionamento de documentos, permitindo restaurar ou auditar o histórico.		
08	Interface de Fóruns Temáticos Dinâmicos integrados à plataforma, organizados com base na taxonomia institucional.	-	Sim
09	Módulo de Captura de Conhecimento Tácito que monitora fóruns e sugere converter consensos em Notas Técnicas oficiais.	-	20
10	Módulo de IA participante com capacidade de marcar o Bot no fórum (ex: @Atena.IA) para resumir discussões ou recuperar jurisprudência e teses relevantes.	-	Sim
11	Prevenção contra injeção de prompt (jailbreak) e mecanismos anti-vazamento de instruções internas, com registro de logs detalhados de cada etapa das trilhas de agentes para permitir auditoria técnica.	Sim	Sim
12	Integração profunda com Active Directory do MPRS para sincronização de grupos e lotações e segregação rigorosa de acesso (prevenção de vazamento de contexto de documentos e fóruns sigilosos).	-	Sim

ID	Descrição	PoC	Homologação
13	Módulo para disparo de boletins informativos e convites de eventos via push notification no Teams, com uso de cards interativos com botões de ação.	-	Sim
14	Segmentação avançada de disparos por cruzamento de tags da taxonomia ou grupos de usuários, agendamento de envios de boletins informativos e convites para datas e horários específicos.	-	Sim
15	Módulo de avaliação rápida da IA pelo usuário ("útil / impreciso") em cada resposta gerada, com campo opcional para o usuário justificar textualmente por que uma resposta da IA foi avaliada como incorreta.	-	Sim
16	Módulo de escalonamento humano, com botão que transforma dúvida não resolvida pela IA em ticket para o Centro de Apoio específico.	5	Sim
17	Mapa de Calor de Consultas: relatórios identificando os temas e termos mais frequentemente pesquisados.	-	25
18	Painel com perguntas recorrentes e perguntas que a IA não conseguiu responder com base no acervo.	5	Sim
19	Painel de relatório de desambiguação, que aponta para o CAO peças/documentos	-	20

ID	Descrição	PoC	Homologação
	que estão gerando conflito lógico nas respostas da IA.		
20	Autocomplete preditivo especializado: sugestão de termos jurídicos, tipos de documentos e dúvidas frequentes baseadas no acervo dos CAOs.	-	20
21	Possibilidade de criação de coleções/pastas pessoais de documentos e respostas dentro da plataforma.	5	20
22	Possibilidade de compartilhamento rápido: o usuário encaminha a resposta da IA, com as fontes, para outro colega com um clique.	5	20
23	Atualização incremental da base (novos documentos entram na busca sem reprocessar toda a base).	-	Sim
24	Interface de Rastreabilidade: Visualização gráfica do fluxo de raciocínio da IA, exibindo a relação entre os documentos recuperados (nós) e a resposta gerada.	-	Sim
25	Capacidade do sistema de gerar uma análise crítica da própria resposta, apresentando teses antagonistas ou pontos de atenção jurídica baseados no acervo.	10	40
26	Interface de upload ad-hoc que permite ao usuário submeter	-	Sim

ID	Descrição	PoC	Homologação
	arquivos locais (PDF, DOCX, XLSX) para análise comparativa imediata e cruzamento direto com a base de conhecimento dos CAOs, atuando estritamente como a camada de interface do usuário.		
27	Pipeline de processamento de retaguarda (back-end) multimodal capaz de extrair texto, tabelas e metadados de múltiplos formatos (incluindo Markdown, JSON, áudio e vídeo) para subsidiar as análises do usuário.	-	Sim
28	Implementação de camada lógica para gestão e orquestração de estados, encadeamento de agentes especializados e persistência de contexto, com interface de monitoramento em tempo real do status de cada etapa do processamento, coordenando a execução sequencial ou paralela de múltiplos agentes (triagem por atribuição, pesquisa, crítica e redação) para uma única requisição complexa.	10	Sim
29	[Trilha] Identificador do CAO: Mapeamento semântico das palavras-chave extraídas para direcionamento e seleção dos CAOs	5	Sim

ID	Descrição	PoC	Homologação
	com base em suas respectivas atribuições institucionais.		
30	[Trilha] Buscador de Acervo: Execução de consultas vetorizadas no banco de dados dos CAOs selecionados para extração de documentos e trechos relevantes.	5	Sim
31	[Trilha] Compilador de Base: Sintetização das informações recuperadas pelo Buscador em um documento base unificado temporário.	5	Sim
32	[Trilha] Revisor (Deduplicação): Filtragem do documento base para eliminação de redundâncias, garantindo coesão lógica e completude do texto.	-	Sim
33	[Trilha] Pesquisador: Execução de buscas externas (APIs do CNJ, bases legislativas abertas) para atualização de jurisprudência e legislação complementar à base do CAO.	-	Sim
34	[Trilha] Jurídico: Aplicação de raciocínio jurídico sobre o documento base atualizado, estruturando a argumentação e o embasamento legal primário.	-	Sim
35	[Trilha] Analista Crítico: Simulação de contraditório (Red Teaming jurídico). Análise da argumentação do	-	Sim

ID	Descrição	PoC	Homologação
	Agente Jurídico para formular teses antagonistas e identificar fragilidades.		
36	[Trilha] Revisor Jurídico: Refinamento da resposta final, incorporando refutações sólidas às teses levantadas pelo Agente Crítico, fortalecendo a fundamentação.	-	Sim
37	[trilha] Verificador (Fact-checking): Validação autônoma de todas as citações normativas, súmulas e julgados, confrontando-as com fontes oficiais para eliminar alucinações de conteúdo ou referências inexistentes.	-	Sim
38	[trilha] Redator: Polimento final do texto gerado, adequação ao padrão culto da linguagem jurídica e fechamento do ciclo de resposta.	-	Sim
39	[Trilha] Gerador de Resumo: Geração de sínteses executivas (Executive Summaries) com os pontos focais da pesquisa.	-	20
40	[Trilha] Gerador de Relatórios Técnicos: Consolidação de informações do acervo em documentos estruturados (PDF/Docx), com sumários executivos e organização temática de dados extraídos.	-	25

ID	Descrição	PoC	Homologação
41	[Trilha] Gerador de Tabela de Dados: Conversão de informações textuais não estruturadas em matrizes tabulares (CSV/Excel) estruturadas.	-	20

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):	-	Sim

ID	Item	Descrição	PoC	Homologação
		Implementação de RBAC para segmentação granular e rastreabilidade.		
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	Containerização e Serverless: Imagens Docker/OCI com execução portátil, permitindo serviços	-	Sim

ID	Item	Descrição	PoC	Homologação
		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 manipulação (jailbreak) e	-	Sim

ID	Item	Descrição	PoC	Homologação
		vazamento de system prompts.		
17	6.4.2	Mitigação de Alucinações (Grounded Generation): Condicionar respostas às fontes e evitar invenção de fatos/normativas.	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.	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	-	Sim

ID	Item	Descrição	PoC	Homologação
		bloqueio contra desativação de segurança por comandos.		
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 limites configuráveis de autonomia e recursos, e bloqueio auditável de operações sensíveis ou escalonamento indevido de privilégios.	-	Sim
26	6.4.9	Métricas de Média: 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