PLANO DIRETOR DE SEGURANCA, SIGILO E GOVERNANCA DE IA

Rolim Advogados (OAB/SP 44.680)

Endereco Oficial: Rua Adib Auada, 354, Bloco B - Granja Viana, Cotia/SP | Filial: Vila da Serra, Nova Lima/MG

Infraestrutura Dedicada Evolute Juris (Regiao sa-east-1 Sao Paulo) - Emissao: 16/11/2026

1. Criptografia Zero-Knowledge no Navegador (AES-256-GCM + ECDH P-256)

A chave mestra do cofre (KEK) e derivada exclusivamente no dispositivo do advogado via PBKDF2-SHA256 (310.000 iteracoes) e nunca trafega para os servidores. Documentos e pastas sensiveis sao cifrados com chaves unicas DEK (AES-256-GCM), garantindo inviolabilidade tecnica compativel com o Art. 7, II da Lei 8.906/1994 (Estatuto da Advocacia).

2. Isolamento Multi-Tenant Estrito no PostgreSQL 17 (ENABLE + FORCE RLS)

100% das 23 tabelas operacionais do banco dedicado operam com Row Level Security estrito e forcado (FORCE RLS). No ambiente da Dra. Melyne Castro, ha dupla derivacao criptografica independente entre o Cofre do Escritorio (office_pj) e o Cofre Pessoal (personal_pf). Em bancas societarias, aplica-se Ethical Wall por processo.

3. Escudo Zero-PII & Zero Data Retention nos Provedores de IA

Antes de qualquer inferencia em LLMs (Anthropic Claude Sonnet 4.6, Google Gemini 3.8 Flash / 2.5 Pro ou OpenAI GPT-5.1), nomes de partes, CPFs, CNPJs, contas e valores sensiveis sao substituidos localmente por tokens efemeros ([PARTE_1], [CPF_1]) e reidratados apenas no navegador do socio. Contratos de API operam sob politica Zero-Training.

4. RAG Juridico Hibrido Verificado Anti-Alucinacao (CNJ 615/2025 & CFOAB 001/2024)

O Enclave combina busca vetorial densa (text-embedding-3-large 1536d), busca lexical em Portugues (GIN tsvector) e reranking cruzado (Cohere rerank-v4.0-fast) sobre legislacao vigente, sumulas vinculantes e playbooks privados da banca, bloqueando invencao de precedentes ou relatores.

5. Defesa Ativa Contra Indirect Prompt Injection (OWASP LLM01)

Peticoes adversas, anexos externos e PDFs de terceiros sao confinados em sandbox XML <untrusted_external_evidence> com tool_choice=none. Comandos ocultos ou tentativas de exfiltracao sao neutralizados e gravados instantaneamente no log forense de seguranca.

6. Dupla Trava Causal Deterministica & Biometria FIDO2 WebAuthn (Passkeys)

Nenhuma operacao financeira, pagamento de guia, split Asaas ou agendamento critico ocorre de forma autonoma pela IA. O protocolo exige preparacao da proposta seguida de confirmacao humana posterior assinada via Windows Hello, Touch ID, Face ID ou sensor biometrico Android.

7. Trilha Forense Imutavel Encadeada por Hash SHA-256 & Residencia Nacional (LGPD)

Todos os bancos, vetores, segredos (Supabase Vault) e backups residem em Sao Paulo (sa-east-1), cumprindo os Arts. 33 e 46 da LGPD e resolucoes da ANPD. Cada evento critico recebe carimbo criptografico encadeado ao hash anterior (tamper-evident).

ATESTADO CRIPTOGRAFICO EM TEMPO REAL (POSTGRESQL RPC verify_juris_chain_public)

Status da Cadeia: INTEGRA E VERIFICADA | Eventos Encadeados: 52

`Ultimo Hash SHA-256: 92a2ee04aebd3d97b35a06df828808e96679b623b7d670d0b7cfaa10ea9f8fee`

Conformidade: Estatuto OAB Art. 7 | Provimento CFOAB 205/2021 | Recomendacao CFOAB 001/2024 | Res. CNJ 615/2025