Whitepaper de Segurança

1. Introdução

O Figno foi projetado sob o princípio de **Privacidade por Design**, garantindo que a eficiência da Inteligência Artificial não comprometa a confidencialidade de segredos industriais e dados sensíveis. Este documento detalha as medidas técnicas e organizacionais adotadas para proteger o ciclo de vida dos dados dentro da plataforma.

2. Arquitetura de Isolamento (Single-Tenant)

Diferente de soluções SaaS convencionais, o Figno utiliza uma arquitetura de isolamento lógico rigoroso:

- **Ambiente Privado e Isolado**: Cada instância de cliente opera em um ambiente dedicado (Single-Tenant), impedindo a coexistência de dados de diferentes usuários no mesmo contexto de processamento.
- **Segregação de Memória**: O processamento de consultas e a recuperação de documentos são isolados, garantindo que o contexto de um cliente nunca vaze para outro.

3. Segurança nas Integrações (Google Drive & OneDrive)

Como o Figno acessa diretórios diretamente na nuvem do cliente, a segurança da ponte de dados é prioridade:

- **Protocolo OAuth 2.0**: A conexão é feita via tokens de autorização segura. O Figno nunca armazena senhas dos colaboradores; ele apenas solicita permissão de leitura para as pastas selecionadas.
- **Sincronização Sob Demanda**: O sistema lê os arquivos para gerar os vetores de busca, mantendo a fonte da verdade segura no ambiente original (OneDrive/Google Drive).

4. IA Ética e Proteção de Dados

O maior diferencial do Figno é o tratamento dos dados frente aos modelos de linguagem:

- **Não-Treinamento de Modelos Públicos**: Seus dados **não** são usados para treinar modelos públicos (como GPT-4 ou Gemini). A informação enviada serve apenas para responder à sua consulta específica.
- **Bancos de Dados Vetoriais Privados**: Utilizamos tecnologias como PostgreSQL com pgvector em instâncias privadas para armazenar os índices dos seus documentos, garantindo que a inteligência de busca seja exclusiva da sua empresa.

5. Criptografia de Padrão Militar

Implementamos protocolos de segurança para todos os estados do dado:

- **Dados em Repouso (At Rest)**: Documentos e índices são criptografados com **AES-256**.
- **Dados em Trânsito (In Transit)**: Toda comunicação entre o navegador do usuário e o Figno é protegida por **TLS 1.2+** com criptografia de ponta a ponta.

6. Controle de Acesso e Governança

- **Controle Granular**: Administradores podem definir níveis de acesso por usuário, limitando quais departamentos podem consultar quais bases de conhecimento.
- **Transparência**: O sistema permite auditoria sobre quais documentos foram consultados pela IA para gerar cada resposta.

Conclusão

O Figno não apenas analisa documentos; ele cria um cofre digital inteligente. Ao unir segurança de infraestrutura com uma política rigorosa de isolamento de IA, o Figno se posiciona como a solução ideal para os setores jurídico, contábil e de TI que não podem abrir mão do sigilo.