

Desafios Tecnológicos do Chatbot Inova

1. Confiabilidade e Atualização da Base de Conhecimento

- Risco Técnico: A base de conhecimento, composta por editais, normas e jurisprudência, é altamente dinâmica. O fornecimento de informações desatualizadas compromete a confiabilidade do sistema e a credibilidade do serviço.
- Impacto no Negócio: Alto. Respostas incorretas podem induzir pesquisadores a erro, resultando em perda de prazos ou submissão de propostas inadequadas.
- Estratégias de Mitigação:
 - Implementar pipelines automatizados para ingestão contínua de novos editais e documentos de fontes confiáveis.
 - Desenvolver um painel administrativo que permita a curadoria e a atualização manual da base de conhecimento de forma simplificada, atendendo ao requisito de manutenibilidade.

2. Segurança e Confidencialidade da Propriedade Intelectual

- Risco Técnico: A plataforma lidará com informações de invenções potencialmente inéditas e dados pessoais dos pesquisadores. Um vazamento de dados é um incidente crítico de segurança.
- Impacto no Negócio: Muito Alto. Causa perda total de credibilidade, além de potenciais implicações legais e financeiras severas.
- Estratégias de Mitigação:
 - Adotar criptografia de ponta a ponta para dados em trânsito e em repouso.
 - Implementar uma política de privacidade clara e acessível.
 - Oferecer a opção de sessões anônimas, sem armazenamento de histórico de conversas.
 - Realizar a anonimização de dados sensíveis em logs e durante o treinamento de modelos internos.

3. Geração de Informações Factualmente Incorretas (Alucinações)

- Risco Técnico: Modelos de linguagem (LLMs) podem gerar respostas plausíveis, mas factualmente incorretas, como citar leis, editais ou cláusulas inexistentes.
- Impacto no Negócio: Alto. A precisão é um critério de aceitação chave. Informações inventadas podem invalidar todo o propósito orientador do chatbot.

- Estratégias de Mitigação:
 - Utilizar uma arquitetura de Geração Aumentada por Recuperação (RAG) estrita, forçando o modelo a basear suas respostas exclusivamente no conteúdo recuperado da base de conhecimento.
 - Implementar um mecanismo de fallback que, na ausência de informações, responda de forma transparente ("Não encontrei uma resposta para sua pergunta") e ofereça transferência para atendimento humano.
 - Implementar a citação de fontes, onde cada resposta gerada aponte para o documento ou edital específico da base de conhecimento de onde a informação foi extraída, aumentando a confiança do usuário.

4. Latência e Desempenho da Interface

- Risco Técnico: Consultas complexas em uma base de dados vetorial extensa podem resultar em um tempo de resposta lento, afetando negativamente a fluidez da conversa.
- Impacto no Negócio: Médio. Uma experiência de usuário lenta pode levar à baixa adesão ao sistema, violando o critério de aceitação de resposta em até 3 segundos.
- Estratégias de Mitigação:
 - Utilizar um sistema de indexação vetorial de alta performance, como Qdrant ou Elasticsearch.
 - Implementar um sistema de cache (ex: Redis) para armazenar e servir rapidamente as respostas de consultas frequentes.

5. Escalabilidade de Custos Operacionais

- Risco Técnico: O custo de inferência de LLMs e a infraestrutura associada podem aumentar exponencialmente com o crescimento do número de usuários e da complexidade das consultas.
- Impacto no Negócio: Médio/Alto. Custos não controlados podem inviabilizar a sustentabilidade e a escalabilidade do projeto a longo prazo.
- Estratégias de Mitigação:
 - Priorizar o uso de modelos de linguagem open source (fine-tuned) para tarefas específicas, reduzindo a dependência de APIs pagas.
 - Implementar um roteador de modelos (ex: usar um modelo menor e mais barato para classificar a intenção do usuário e acionar um modelo maior apenas para tarefas complexas, como a redação de patentes).
 - Adotar uma política de otimização de prompts para reduzir o número de tokens por chamada.

6. Complexidade da Jornada do Usuário e Adoção

- Risco Técnico: O domínio de Propriedade Intelectual é inherentemente técnico e burocrático. Usuários podem se sentir perdidos em uma interface puramente conversacional ou não compreender os termos técnicos.
- Impacto no Negócio: Médio. Se a ferramenta não for percebida como útil e fácil de usar, terá baixa adesão, comprometendo seu objetivo principal.
- Estratégias de Mitigação:
 - Desenvolver fluxos conversacionais guiados para tarefas complexas, como o simulador de patenteabilidade e a busca de fomento, usando checklists e formulários interativos.
 - Incorporar uma camada de pós-processamento para simplificar a linguagem técnica, garantindo que as respostas sejam acessíveis para não especialistas.