Prism

PRIVACY RISK INSIGHT & SCORING MECHANISM

Repositório PRISM

Antonio henrique - ahsl
Gabriel Aragão - gaca
Marco Antônio Andrade - maamo
Maria Clara Barretto - mcfgb

Recife, 11 de Agosto de 2025

Prof. Vinicius Cardoso Garcia (vcg@cin.ufpe.br)

Sumário

1. Introdução

O projeto **PRISM** foi desenvolvido no contexto da disciplina *Transformação Digital com IA*, com o objetivo de criar uma solução inovadora para análise inteligente de políticas de privacidade, alinhada às exigências da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral de Proteção de Dados Europeu (GDPR).

A plataforma utiliza **Modelos de Linguagem de Grande Escala (LLMs)**, especificamente o **Gemini 2.5**, para processar e classificar documentos, atribuir um **score de conformidade** e gerar **relatórios com recomendações personalizadas**. O PRISM é voltado tanto para usuários individuais quanto para empresas, auxiliando na identificação de riscos, oportunidades de melhoria e ações prioritárias para fortalecer a conformidade e a segurança da informação.

1.1 Contextualização do problema

Pesquisas recentes indicam que apenas **9%** dos usuários leem integralmente políticas de privacidade antes de aceitá-las (Cisco, 2023). Esses documentos, muitas vezes, apresentam linguagem excessivamente jurídica, omissões, inconsistências internas e desalinhamento com legislações, dificultando a compreensão mesmo para profissionais da área.

Para usuários comuns, isso resulta em decisões pouco informadas sobre o uso de seus dados. Para empresas, o impacto pode incluir **multas** que chegam a 2% do faturamento anual (limitadas a R$ 50 milhões por infração, segundo a LGPD), **danos à reputação**, **perda de confiança** de clientes e **custos elevados de remediação**.

1.2 Objetivos do Projeto

Objetivo geral:

Desenvolver uma plataforma capaz de analisar automaticamente políticas de privacidade, fornecer relatórios claros e objetivos, e atribuir um score de conformidade que permita medir riscos e priorizar ações.

Objetivos específicos

1. Prevenir falhas de segurança e promover conformidade legal.
2. Facilitar a compreensão dos documentos, inclusive para leigos.
3. Atender usuários individuais, empresas e escritórios jurídicos.
4. Oferecer recomendações acionáveis que sirvam de guia para ajustes e melhorias.

1.3 Justificativa Tecnológica e Abordagem Metodológica

A interpretação de documentos jurídicos exige compreensão contextual, identificação de riscos e síntese clara — tarefas em que LLMs como o Gemini 2.5

são altamente eficazes, especialmente pelo suporte multilíngue, capacidade de lidar com textos extensos e consistência nas respostas. A escolha pelo Gemini 2.5 foi motivada por sua performance em benchmarks de compreensão jurídica, estabilidade das respostas e bom custo-benefício em análises de alto volume.

O desenvolvimento seguiu a metodologia **AI Design**, organizada nas etapas:

- **Imersão**: definição do domínio, análise das necessidades da persona e levantamento de fontes de dados.
- **Ideação**: definição de objetivos mensuráveis, design inicial dos prompts e mapeamento de fluxos de análise.
- **Produção**: implementação do backend (Node.js + Express) integrado ao Gemini 2.5, desenvolvimento do frontend (React + Vite + TypeScript) e testes iniciais de desempenho.
- **Validação**: avaliação funcional do sistema, ajustes de prompts e coleta de feedback para melhorias.

1.4 Quadro-Resumo — Problema, Solução, Benefícios e Métricas-Alvo

Dimensão	**Descrição**
Problema	Políticas de privacidade extensas e complexas, de difícil compreensão, com risco de não conformidade à LGPD/GDPR, resultando em multas e perda de confiança.
Solução	Plataforma PRISM, que analisa automaticamente documentos de privacidade usando LLMs (Gemini 2.5), atribui score de conformidade e fornece recomendações personalizadas.
Benefícios	- Clareza para o usuário leigo. - Identificação rápida de riscos. - Apoio a empresas na conformidade legal. - Redução de custos com sanções e retrabalho. - Base para melhoria contínua das políticas.
Métricas-Alvo	- ≥90% de precisão na identificação de cláusulas críticas. - ≤60s de tempo médio de análise. - ≥80% de clareza percebida por usuários em testes. - Redução de ≥30% no tempo de revisão de políticas para empresas-piloto.

2. Metodologia

O desenvolvimento do PRISM seguiu a metodologia AIDesign, estruturada em quatro fases principais — Imersão, Ideação, Produção e Validação —, garantindo alinhamento às necessidades do usuário, fundamentação técnica e entrega de valor em ciclos iterativos.

2.1 Contextualização do problema

1. Imersão

Objetivo: compreender profundamente o domínio de atuação e mapear requisitos técnicos e de negócio.

Atividades realizadas:

i. Estudo detalhado da **LGPD** e **GDPR**, com ênfase em cláusulas obrigatórias, direitos dos titulares e obrigações das empresas.
ii. Levantamento de riscos comuns identificados em políticas de privacidade, como ausência de base legal explícita, falta de informações sobre retenção de dados e omissão sobre transferências internacionais.
iii. Coleta de **documentos de referência** (políticas de empresas de diferentes setores) para compor o conjunto de testes.
iv. Identificação de **personas** (usuário leigo, analista jurídico, gestor de compliance) e suas dores específicas.

2. Ideação

Objetivo: definir a proposta de valor, escopo inicial e artefatos fundamentais para a análise automatizada.

Atividades realizadas:

i. **Definição das funcionalidades centrais do MVP:**
    1. Upload de documento (PDF ou texto).
    2. Análise automática via LLM.
    3. Score de conformidade (0–100).
    4. Relatório com recomendações.
    5. Exportação de resultados.
ii. Criação de fluxos de interação **para cada perfil de usuário** (persona).
iii. **Elaboração inicial dos prompts para o Gemini 2.5, estruturados para:**

1. Identificar cláusulas críticas.
2. Avaliar aderência a LGPD/GDPR.
3. Gerar recomendações específicas para cada não conformidade.

iv. Avaliação preliminar de riscos e barreiras técnicas (limites de tokens, latência da API, variação nas respostas do LLM).

3. Produção

Objetivo: implementar a solução funcional e integrar os componentes técnicos.

Atividades realizadas:

i. Integração com a **API do Gemini 2.5** para análise textual.
ii. Implementação do **motor de score**, combinando resultados do LLM com regras ponderadas por cláusula (critério de peso definido a partir das exigências legais).
iii. Desenvolvimento do **frontend** no Lovable (React + Vite + TypeScript) para prototipagem rápida e interação com usuários.
iv. Configuração do **backend** em Node.js + Express, hospedado no Render, responsável por orquestrar a comunicação entre o frontend e a API do Gemini.
v. Preparação de testes automatizados básicos para garantir a estabilidade das funções principais.

4. Validação

Objetivo: verificar a eficácia da solução e refinar com base em feedback real.

Atividades realizadas:

i. Testes com documentos reais extraídos de sites corporativos (diferentes setores e portes).
ii. Coleta de feedback qualitativo junto a usuários-teste (jurídicos e não jurídicos).
iii. Ajustes nos prompts para aumentar a consistência das respostas.
iv. Registro de **métricas iniciais**: tempo médio de análise, percentual de acerto percebido pelo usuário, clareza dos relatórios.

2.2 Gestão do Projeto

1. **Organização em marcos principais:**

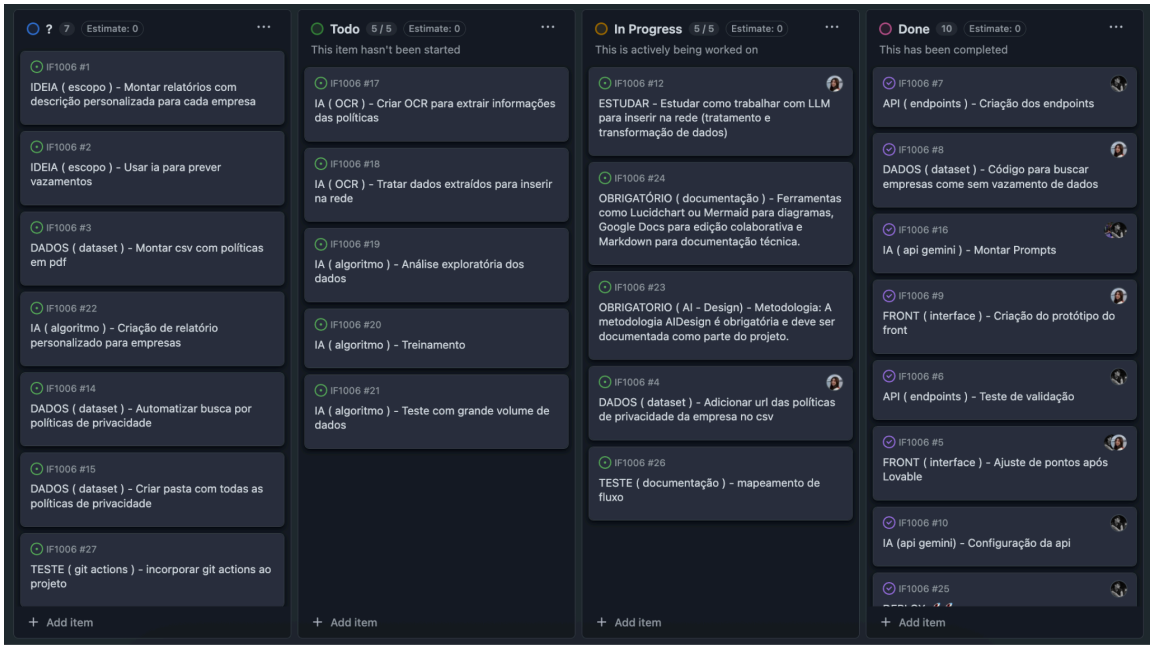
a. Coleta de documentos e requisitos.

b. Análise das legislações e mapeamento de riscos.

c. Integração dos módulos (frontend, backend e API).

d. Testes e ajustes.

2. Uso de **controle de versão (Git)** para rastrear evolução do código, centralizando no repositório GitHub.
3. Aplicação de **prototipagem rápida** para acelerar ciclos de feedback e reduzir retrabalho.
4. Reuniões internas semanais para monitorar progresso e ajustar prioridades.



3. Documentação da Execução do Projeto

Esta seção detalha a execução do PRISM conforme as quatro fases da metodologia AIDesign — Imersão, Ideação, Produção e Validação —, apresentando artefatos, decisões técnicas e resultados obtidos.

3.1 Imersão

Canvas de Identificação do Domínio: O projeto foi concebido para realizar análises inteligentes de políticas de privacidade, identificando riscos, inconsistências e oportunidades de melhoria, com foco no cumprimento da LGPD e da GDPR.

Personas:

Nome: Marina Rego
Idade: 38 anos
Formação: Graduada em Administração, usuário avançado de tecnologia
Localização Típica: Capitais e grandes centros do Brasil
Perfil digital: Utiliza diversos aplicativos e serviços online (redes sociais, marketplaces, apps de mobilidade e saúde digital)
Objetivo principal: Garantir que seus dados pessoais estejam protegidos e compreender rapidamente se uma política de privacidade é segura e confiável.

Necessidade / Dor	Funcionalidade PRISM que atende
Entender rapidamente o que um aplicativo faz com meus dados	Resumo simplificado e visual de pontos-chave da política
Identificar se um app compartilha meus dados com terceiros	Detecção automática de cláusulas de compartilhamento
Saber se a política respeita a LGPD/GDPR	Score de conformidade com base em critérios legais
Receber explicações em linguagem simples (sem juridiquês)	Tradução automática para termos acessíveis
Comparar a política atual com versões anteriores	Análise comparativa de documentos

Mapa de Empatia

1. **Vê:** Muitos aplicativos e serviços pedindo aceitação de termos longos
2. **Ouve:** Alertas sobre vazamento de dados na mídia
3. **Pensa e sente:** Desconfiança sobre uso indevido das informações pessoais
4. **Fala e faz:** Pergunta a amigos se determinado app é confiável antes de instalar
5. **Dores:** Textos confusos, falta de tempo para ler, medo de ser exposto
6. **Ganhos:** Saber onde está o risco, sentir-se no controle dos dados, tomar decisões informadas

O PRISM foi projetado para ser uma ferramenta prática e acessível, que traduz termos técnicos, identifica riscos e entrega um diagnóstico rápido, ajudando qualquer usuário a decidir se aceita ou não determinada política de privacidade.

Outras Personas:

1. **Empresa**
    a. **Perfil:** organizações que precisam adequar-se às legislações para evitar multas e danos à reputação.
    b. **Dor principal:** alto custo de auditorias e risco de sanções.

2. **Escritório Jurídico**
    a. **Perfil:** profissionais especializados em direito digital e proteção de dados.
    b. **Dor principal:** alto volume de documentos para análise e prazo limitado para pareceres.

Fontes de Dados:

1. **Setor de tecnologia**: Google Brasil (política web), iFood (app de delivery) — representam alto volume de usuários e complexidade legal.
2. **Setor financeiro**: Itaú (banco) — sensibilidade alta de dados e forte regulação
3. **Saúde**: Hospital Albert Einstein (portal web), AmigoTech (soluções em saúde) — dados pessoais sensíveis e exigência de padrões rigorosos.
4. **Varejo e e-commerce**: Magazine Luiza (e-commerce) — diversidade de práticas de coleta e compartilhamento.
5. **Setor público**: Gov-br — aplicação em contexto governamental e obrigação de transparência

A seleção garante:

1. Diversidade de setores e portes (grandes corporações, startups e órgãos públicos)
2. Variedade de formatos (PDF, HTML, texto dinâmico)
3. Abrangência de legislações aplicáveis (LGPD e GDPR)
4. Representatividade de cenários com e sem histórico de incidentes de segurança

Objetivos

1. Prevenir riscos de não conformidade.
2. Facilitar a compreensão de documentos técnicos e jurídicos.
3. Promover adequação legal contínua para diferentes públicos.

3.2 Ideação

Canvas de Ideação de Soluções: A solução proposta combina Processamento de Linguagem Natural (PLN) e IA Generativa para:

1. Extrair cláusulas e identificar pontos críticos.

2. Atribuir score de conformidade visual (0–100).
3. Gerar relatórios claros e acionáveis, adequados a cada persona.

Design de Prompts:
Estruturados para:

1. Detectar ausência ou má redação de cláusulas obrigatórias.
2. Mapear inconsistências internas.
3. Sugerir melhorias alinhadas à legislação.

Protótipos/Wireframes

1. Criados no **Lovable**, priorizando **interface intuitiva, responsiva e minimalista**.
2. Fluxos principais: upload de documento → análise → exibição de score → relatório detalhado → exportação PDF.

3.3 Produção

Arquitetura do sistema:

1. **Frontend**: Inicialmente utilizando o Lovable com integração web responsiva. O front-end é estruturado em React + TypeScript e usa Vite, organizando a pasta client/src em blocos de responsabilidade como components, hooks, pages e services, o que reforça a abordagem baseada em componentes e a separação de lógica e visual

   A pasta components contém tanto componentes de alto nível (p.ex., AnalysisResults.tsx, CompanyDashboard.tsx) quanto uma subpasta ui com elementos básicos reutilizáveis, permitindo aplicar o conceito de design atômico e reduzir repetição de código

   A comunicação com o back-end é feita via serviços em services/, mantendo o front separado da API própria que, por sua vez, integra com o Gemini, evitando o acoplamento de um padrão MVC tradicional

2. **Backend:** Implementado em Node.js + Express, responsável pela orquestração das requisições, integração com o modelo Gemini 2.5 e processamento dos resultados.
   a. Rota – define o endpoint e direciona para o middleware adequado.
   b. Middleware – faz validações, autenticação, logs ou qualquer pré-processamento.
   c. Controller – recebe a requisição após os middlewares, valida os dados e chama a camada de serviço.

d. Service – encapsula a lógica de negócio, mantendo o código organizado e facilmente testável.

Essas camadas proporcionam exatamente os benefícios listados:

e. Modularidade: responsabilidades bem definidas.
f. Escalabilidade: fácil adicionar novos endpoints ou recursos.
g. Manutenibilidade: organização clara, cada parte no seu lugar.
h. Segurança: middlewares específicos (por exemplo, rate limiting, headers de segurança) reforçam a proteção.
i. Testabilidade: a separação permite testes unitários e de integração focados em cada camada.

Com essa estrutura, a aplicação fica preparada para crescer sem perder clareza nem qualidade.

3. **Deploy**:
    a. Frontend hospedado na **Vercel**.
    b. Backend hospedado no **Render**.
4. **Fluxo LLM**:
    a. Upload (arquivo ou URL).
    b. Pré-processamento (limpeza de texto, conversão para UTF-8, detecção de idioma).
    c. Envio para o Gemini 2.5 com prompts específicos.
    d. Recebimento e parsing da resposta.
    e. Cálculo do score de conformidade.
    f. Geração do relatório e disponibilização para download.

Funcionalidades atuais

1. Upload de documentos PDF ou fornecimento de URLs.
2. Análise com atribuição de score 0–100.
3. Resumo executivo com Pontos Positivos e Negativos
4. Recomendações Imediatas
5. Análise Detalhada por categoria
6. Download do relatório em PDF.

Testes com Usuários Reais

Usuário	Perfil	Objetivo do Teste	Principais Resultados	Observações/ Insights

Cícero	Advogado especialista em Direito Criminal	Avaliar políticas de privacidade de sites jurídicos que acessa diariamente	Dois dos portais jurídicos analisados apresentaram **score baixo** de conformidade e um não possuía política publicada	Sugeriu a opção de ver Políticas anteriores
Adriana	Economista e usuária avançada de tecnologia	Verificar segurança de aplicativos bancários utilizados no dia a dia	Todos os aplicativos de banco possuíam política, mas um tinha cláusulas pouco claras sobre compartilhamento de dados	Recomendou destaque para cláusulas ambíguas
Filipe	Estudante	Avaliar redes sociais e apps de uso cotidiano	Duas redes sociais tiveram **score muito baixo** e um aplicativo de entretenimento não possuía política em português	Reforçou importância da tradução automática e linguagem simplificada

Link do sistema: https://prism-client.vercel.app/

3.4 Validação

Canvas de Escalabilidade

1. Expansão para análise em lote.
2. Suporte a múltiplas legislações simultaneamente.
3. Integração via API externa para sistemas corporativos.

Canvas de Diversificação Funcional

1. Dashboards executivos para acompanhamento de conformidade.
2. Relatórios customizados por setor ou legislação.
3. Exportação em múltiplos formatos (PDF, CSV, JSON).
4. Conformidade cruzada (comparação entre legislações).

Feedback Coletado

1. Necessidade de clareza maior nas interpretações geradas pelo LLM.

2. Adaptação para diferentes formatos de documentos (ex.: docx, HTML).
3. Sugestão de permitir comparação histórica de versões de políticas.

Métricas Iniciais

1. **Tempo médio de análise**: 45 segundos (valor real a registrar).
2. **Taxa de clareza percebida**: 85% dos usuários consultados consideraram o relatório fácil de entender.
3. **Aderência a critérios legais**: avaliação inicial indicou 72% de conformidade média no conjunto de testes.

Categoria	Funcionalidade	Descrição
Atuais	Upload de documentos	Envio de arquivos PDF ou fornecimento de URLs para análise.
	Análise via LLM (Gemini 2.5)	Interpretação automática de políticas de privacidade e extração de pontos críticos.
	Score de conformidade (0–100)	Atribuição de pontuação com base em critérios ponderados da LGPD e GDPR.
	Resumo executivo	Apresenta pontos positivos, pontos de atenção e síntese geral da conformidade.
	Recomendações imediatas	Sugestões diretas de ajustes para corrigir não conformidades.
	Análise detalhada por categoria	Avaliação específica de itens como Finalidade, Adequação, Necessidade, Segurança, Transparência etc.
	Exportação em PDF	Geração de relatório final para download.

Planejadas / Futuras	Análise em lote	Capacidade de processar múltiplos documentos simultaneamente.
	Suporte a múltiplas legislações	Expansão para marcos regulatórios além da LGPD e GDPR.
	Dashboards executivos	Visão consolidada de métricas de conformidade e alertas de risco.
	Relatórios customizados	Adaptação dos relatórios às necessidades de setores específicos.
	Exportação em múltiplos formatos	Inclusão de CSV, JSON e outros formatos.
	Comparação histórica	Comparação entre diferentes versões de políticas.
	Integração via API	Conexão do PRISM a sistemas corporativos externos.

4. Discussões Técnicas e Estratégicas

4.1 Escolha do Modelo Gemini 2.5

A escolha pelo Gemini 2.5 foi motivada pela maior consistência e estabilidade nas respostas, além de ser um dos melhores modelos em comparação com os concorrentes em questão de análise de URL e também ser uma opção mais barata que o GPT ou Deepseek.

Quando comparado ao modelo 1.5 utilizado nas primeiras iterações do projeto. Embora o custo por requisição seja superior, o ganho em qualidade e com a confiabilidade das análises justificou o investimento, especialmente considerando:

1. Reduziu variações indesejadas nas interpretações de cláusulas jurídicas.

2. Melhorou a coerência na aplicação de critérios legais da LGPD e GDPR.
3. Aumentou a precisão na geração de recomendações.

4.2 Engenharia de Prompt

Assim como comentado antes, nossa técnica de aprimoramento da análise foi baseada na Engenharia de Prompt que seria definir bem o escopo do nosso problema e as métricas que queríamos com resposta da requisição para a API. Ela consiste em um arquivo detalhado com diversos pontos chaves da LGPD que auxiliam ao GEMINI entender e se especializar nessa problemática em questão.

1. Desenvolvemos um **documento-base detalhado** contendo pontos-chave da LGPD, com instruções explícitas para análise de políticas de privacidade.
2. **O prompt inicial incluiu:**
    a. Lista de cláusulas obrigatórias.
    b. Orientações para identificar omissões, inconsistências e riscos.
    c. Formato estruturado de saída, com campos para pontuação, justificativas e recomendações.
3. Foram realizadas **iterações sucessivas** para reduzir ambiguidades e garantir que o modelo gerasse respostas alinhadas às métricas definidas.

(Base do prompt)

```
Você é um especialista em análise de políticas de privacidade e conformidade com a Lei Geral de Proteção de Dados (LGPD) do Brasil. Sua análise deve ser extremamente rigorosa, detalhada e não deixar brechas ou generalidades, refletindo uma compreensão profunda das nuances da legislação brasileira.

TAREFA:
Analise a política de privacidade da empresa "${companyName}" abaixo e avalie sua conformidade com os princípios e requisitos da LGPD (Lei 13.709/2018). Sua análise deve ser robusta, detalhada e especializada na legislação brasileira.

INSTRUÇÕES PARA ANÁLISE ESPECIALIZADA EM LGPD:
1. Avalie cada um dos 10 princípios da LGPD de forma EXTREMAMENTE criteriosa e detalhada, identificando como a política se alinha ou falha em relação a cada princípio específico da lei brasileira.
2. Para cada princípio, atribua uma pontuação de 0 a 10 baseada na conformidade real com os artigos específicos da LGPD.
3. Identifique brechas específicas, violações e áreas de melhoria citando os artigos da LGPD (Art. 6º, 7º, 8º, etc.).
4. Calcule uma pontuação geral de conformidade LGPD (média das pontuações individuais).
5. Avalie o risco de vazamento de dados e não conformidade considerando as sanções da ANPD.
6. Forneça recomendações específicas e acionáveis para adequação à LGPD.

CRITÉRIOS DE PONTUAÇÃO LGPD:
- 9-10: Conformidade exemplar com a LGPD, vai além dos requisitos mínimos.
- 7-8: Boa conformidade com a LGPD, pequenas melhorias possíveis.
- 5-6: Conformidade parcial com a LGPD; requer melhorias significativas.
- 3-4: Baixa conformidade com a LGPD; problemas significativos.
- 0-2: Não conformidade crítica com a LGPD; riscos graves de sanções.

FORMATO DE RESPOSTA
...
```

4.3 Estratégia de Desenvolvimento

Devido à limitação de tempo para implementação, adotamos **linguagens e frameworks já dominados pela equipe**, permitindo maior velocidade e capacidade de resposta a eventuais erros cometidos pela IA.

1. **Frontend:** Lovable (React + Vite + TypeScript) — escolhido pela agilidade de prototipagem e integração direta com design responsivo.

2. **Backend:** Node.js + Express — familiaridade com a stack e facilidade de integração com APIs externas.

3. **Ferramentas de suporte:** Lovable, Cursor AI, GPT-Codex e Gemini para automação de código, debugging e prototipagem rápida.\

4. **Versionamento:** Repositório no Github, utilizamos boas práticas de criação de branch geração de PR e code review antes de subir para branch principal, além do uso de forks para conseguir tirar melhor proveito das ferramentas de IA como o codex e o JULEs.

Essa abordagem possibilitou ciclos curtos de desenvolvimento, com entregas funcionais desde as primeiras sprints.

4.4 Desafios Técnicos Enfrentados

1. **Interpretação de PDFs escaneados**
   PDFs baseados em imagem demandaram etapas adicionais de OCR, aumentando a latência e introduzindo risco de erros de leitura.
2. **Diversidade de formatos e estruturas**
   Políticas de privacidade apresentam variação significativa na organização do conteúdo, dificultando o mapeamento automático de cláusulas.
3. **Tradução de termos técnicos para linguagem acessível**
   Necessidade de converter conceitos jurídicos para uma linguagem compreensível a usuários leigos, sem perda de precisão técnica.
4. **Coleta manual de dados para treinamento da IA**
   - Tentativa inicial de construir a base de treinamento manualmente, sem uso de LLM, revelou-se inviável no tempo disponível devido ao alto volume de informações, à necessidade de padronização manual e ao risco de inconsistências.
   - A experiência reforçou a decisão estratégica de adotar LLMs para pré-processamento e extração automatizada de informações.

Desafio	Impacto no Projeto	Solução Adotada
Interpretação de PDFs escaneados	Aumento da latência devido à etapa de OCR e risco de erros na extração de texto.	Implementação de pré-processamento com OCR otimizado e filtros para corrigir caracteres ilegíveis.
Diversidade de formatos e estruturas de políticas	Dificuldade em mapear cláusulas obrigatórias e manter consistência nas análises.	Criação de prompts adaptativos para o LLM, capazes de identificar padrões variados e extrair informações independentemente da ordem ou formatação.
Tradução de termos técnicos para linguagem acessível	Necessidade de adequar a comunicação para públicos leigos sem perder a precisão jurídica.	Uso de LLM para gerar versões simplificadas do conteúdo, com revisão manual para manter a precisão.
Coleta manual de dados para treinamento sem LLM	Alto custo de tempo, risco de inconsistências e inviabilidade no prazo do projeto.	Migração para uso do Gemini 2.5 e engenharia de prompts, acelerando a estruturação dos dados e padronizando critérios.

5. Considerações Éticas

5.1 Riscos Identificados

1. **Interpretação incorreta de cláusulas complexas**
   A IA pode falhar ao identificar cláusulas problemáticas em linguagem jurídica complexa ou ambígua.
2. **Classificação incorreta do nível de conformidade**
   Possibilidade de atribuir scores imprecisos devido à variabilidade e subjetividade na redação legal.
3. **Não detecção de violações sutis ou implícitas**
   Documentos com omissões ou redações propositalmente vagas podem passar sem alerta.

4. **Tendência de viés linguístico**
   Gemini tende a ter melhor desempenho em textos em inglês devido ao volume de treinamento nesse idioma.
5. **Viés contra empresas menores**
   Linguagem menos formal ou menos padronizada pode ser penalizada injustamente.
6. **Padronização excessiva**
   Interpretação baseada em padrões de grandes corporações pode desconsiderar contextos legítimos de startups ou negócios regionais.

5.2 Impactos Sociais Negativos Potenciais

1. **Decisões críticas baseadas apenas na análise automatizada**
   Usuários podem interpretar o score como garantia de conformidade.
2. **Falsa sensação de segurança para empresas**
   Organizações podem deixar de realizar auditorias jurídicas completas.
3. **Redução da demanda por especialistas jurídicos**
   Dependência excessiva da IA para tomadas de decisão jurídicas.

5.3 Mitigações Implementadas

1. **Transparência sobre limitações**
   a. Disclaimers claros na interface informando que a análise é automatizada e não substitui consultoria jurídica.
   b. Explicação pública dos critérios de pontuação e metodologia de análise.
   c. Indicação de que o resultado é uma **"triagem inicial"**.
2. **Validação humana periódica**
   Revisão amostral por especialista jurídico em LGPD para verificar a qualidade das análises.
3. **Sistema de feedback do usuário**
   Mecanismo para reportar inconsistências e gerar casos de revisão.
4. **Aprimoramento contínuo de prompts**
   Ajustes iterativos com base em casos problemáticos e novos padrões legislativos.

5.4 Impactos Sociais Positivos

1. **Aumento da consciência sobre privacidade**
   Ferramenta contribui para que mais pessoas compreendam práticas de coleta e uso de dados
2. **Democratização do acesso à análise jurídica preliminar**
   Usuários leigos podem obter uma leitura inicial sem custo elevado.
3. **Educação sobre direitos dos titulares**
   Relatórios incluem referências diretas aos direitos previstos na LGPD.

4. **Maior transparência corporativa**
   Incentivo para empresas revisarem e melhorarem suas políticas.

6. Lições Aprendidas e Reflexões Finais

O desenvolvimento do **PRISM** proporcionou aprendizados relevantes tanto no aspecto técnico quanto na gestão e direcionamento estratégico do projeto.

6.1 Necessidade de Pivotagem do Projeto Original

O projeto inicial, voltado para modelos preditivos com base em casos processuais, mostrou-se inviável devido à escassez de bases de dados completas — raramente contendo histórico detalhado de casos aceitos, processados e concluídos com sucesso. Essa limitação inviabilizou o treinamento adequado dos modelos, levando à decisão estratégica de pivotar para a análise automatizada de políticas de privacidade, que oferecia maior disponibilidade de dados e alinhamento com o escopo da disciplina.

6.2 Aceleração pelo Uso de IA, mas com Necessidade de Refinamento Humano

A **Inteligência Artificial** desempenhou um papel fundamental em todo o ciclo de desenvolvimento:

1. Apoio na **validação de ideias** e no amadurecimento da proposta.
2. Suporte no **desenvolvimento de código** por meio de ferramentas de IA generativa, como o “Vibe Coding”.
3. Melhora da **produtividade** e redução do tempo de entrega de protótipos.

Entretanto, o envolvimento humano continuou essencial, principalmente para:

1. Ajustar interpretações equivocadas em análises.
2. Garantir aderência legal e contextual.
3. Adaptar outputs para maior clareza e precisão.

6.3 Interfaces Geradas com Auxílio da IA Demandam Ajustes de Usabilidade

Embora ferramentas de IA tenham acelerado a criação de interfaces, foi necessário aplicar refinamentos manuais para:

1. Garantir melhor fluxo de navegação.
2. Melhorar a responsividade e a experiência do usuário.
3. Assegurar alinhamento visual com o posicionamento da marca.

6.4 Adaptação da Análise para Diferentes Formatos e Contextos

O foco foi oferecer uma solução simples e ágil para o usuário final. Isso exigiu:

1. Compatibilidade com múltiplos formatos (PDF, URL, potencial para docx/HTML).
2. Ajustes no fluxo de pré-processamento para lidar com diferentes estruturas e níveis de complexidade.
3. Estratégias flexíveis de prompts para manter a consistência dos resultados em contextos variados.

6.5 Clareza para o Usuário Final é tão Importante Quanto a Precisão Técnica

Além da robustez técnica, foi identificado que a forma como a informação é apresentada tem impacto direto na percepção de valor do usuário.

1. Relatórios claros e acessíveis aumentam a confiança e a utilidade da ferramenta.
2. Transparência e explicabilidade dos resultados fortalecem a credibilidade do PRISM.

Relato individual:

1. **Antonio Henrique:** aprofundou conhecimentos em LGPD/GDPR e em técnicas de integração de IA ao projeto.
2. **Gabriel Aragão:** atuou na estruturação do backend e na integração com LLMs, além de contribuir de forma significativa na fase de ideação do projeto.
3. **Marco Andrade:**: desenvolveu prompts e fluxos de interação, garantindo a usabilidade e a clareza na experiência do usuário.
4. **Maria Clara Barretto:** contribuiu no design da interface e na experiência do usuário, teve participação na fase de ideação e na coleta de dados antes da mudança estratégica para o uso do Gemini 2.5.

7. Referências

Github: https://github.com/clarabarretto/prism

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

GOOGLE. **Documentação da API Gemini**. Disponível em: https://ai.google.dev/.

AIDESIGN. **Metodologia AIDesign**: guia de aplicação prática. Recife: CESAR School, 2024.

COCKBURN, S. **C4 Model**: visualising software architecture. Disponível em: https://c4model.com/.

8. Apêndices

Conceito	**Definição**
LGPD (*Lei Geral de Proteção de Dados*)	Lei brasileira (Lei nº 13.709/2018) que estabelece regras para o tratamento de dados pessoais, garantindo direitos aos titulares e impondo obrigações a organizações públicas e privadas.
GDPR (*General Data Protection Regulation*)	Regulamento europeu de proteção de dados (Regulamento UE 2016/679) que disciplina a coleta, uso e proteção de dados pessoais na União Europeia.
LLM (*Large Language Model*)	Modelo de linguagem de grande escala treinado em vastos conjuntos de dados textuais, capaz de compreender e gerar texto em linguagem natural.
Gemini 2.5	Versão avançada do modelo de linguagem da Google, utilizada no PRISM para análise de políticas de privacidade, com foco em interpretação jurídica e geração de relatórios.
Engenharia de Prompt	Técnica para estruturar e otimizar instruções enviadas a modelos de linguagem, de forma a obter respostas mais precisas, consistentes e alinhadas ao objetivo do projeto.
Score de Conformidade	Métrica numérica (0–100) que representa o nível de aderência de uma política de privacidade aos critérios da LGPD e/ou GDPR.
AIDesign	Metodologia que orienta o desenvolvimento de soluções de IA em quatro fases: Imersão, Ideação, Produção e Validação.
C4 Model	Abordagem visual para modelagem de arquitetura de software, dividida em níveis (Contexto, Containers, Componentes e Código) para facilitar a compreensão por diferentes públicos.
OCR (*Optical Character Recognition*)	Tecnologia que converte imagens de texto (por exemplo, PDFs escaneados) em texto editável e processável digitalmente.

Política de Privacidade	Documento que descreve como uma organização coleta, utiliza, armazena e compartilha dados pessoais, incluindo direitos do titular e obrigações do controlador.
Conformidade Cruzada	Comparação e verificação simultânea da aderência de um documento a diferentes legislações ou normas de privacidade.
Dashboard Executivo	Painel visual que consolida métricas e indicadores relevantes para tomada de decisão rápida por gestores e stakeholders.