

\_\_\_\_\_

PÓS-GRADUAÇÃO

**XP Educação**

**Relatório do Projeto Aplicado**

Centralizar Controle de Acesso

pelo SSO

[Guilherme Costa Santos]

Orientador(a): Reinaldo Galvão

[28/09/2025]



**Guilherme Costa Santos**

**XP EDUCAÇÃO**RELATÓRIO DO PROJETO APLICADO

Centralização de Acessos pelo SSO

Relatório de Projeto Aplicado desenvolvido para fins de conclusão do curso [...].  
  
Orientador (a): Reinaldo Galvão

**[São Bernardo do Campo -SP]  
[28/09/2025]**

**Sumário**

[1. CANVAS do Projeto Aplicado 6](#__RefHeading___Toc2033_4158205933)

[1.1 Desafio 7](#__RefHeading___Toc2031_4158205933)

[1.1.1 Análise de Contexto 7](#__RefHeading___Toc2035_4158205933)

[1.1.2 Personas 10](#__RefHeading___Toc2065_4158205933)

[1.1.2.1 Arquiteto 1 10](#__RefHeading___Toc2041_4158205933)

[1.1.2.2 Diretor Financeiro 11](#__RefHeading___Toc2039_4158205933)

[1.1.2.3 Desenvolvedor Senior 12](#__RefHeading___Toc2037_4158205933)

[1.1.3 Justificativas 13](#__RefHeading___Toc2063_4158205933)

[1.1.4 Hipóteses 16](#__RefHeading___Toc2061_4158205933)

[1.2 Solução 17](#__RefHeading___Toc2029_4158205933)

[1.2.1 Objetivo SMART 17](#__RefHeading___Toc2059_4158205933)

[1.2.2 Escopo do Projeto 19](#__RefHeading___Toc2057_4158205933)

[1.2.3 Cronograma de Ações Planejadas 21](#__RefHeading___Toc2055_4158205933)

[2. Área de Experimentação 22](#__RefHeading___Toc2015_4158205933)

[2.1 Sprint 1 24](#__RefHeading___Toc2027_4158205933)

[2.1.1 Solução 24](#__RefHeading___Toc2053_4158205933)

[Evidência da execução de cada requisito: 24](#__RefHeading___Toc2067_4158205933)

[Evidência dos resultados: 24](#__RefHeading___Toc2077_4158205933)

[2.1.2 Retrospectiva da Sprint 24](#__RefHeading___Toc2051_4158205933)

[2.2 Sprint 2 25](#__RefHeading___Toc2025_4158205933)

[2.2.1 Solução 25](#__RefHeading___Toc2049_4158205933)

[Evidência da execução de cada requisito: 25](#__RefHeading___Toc2075_4158205933)

[Evidência dos resultados: 25](#__RefHeading___Toc2073_4158205933)

[2.2.2 Retrospectiva da Sprint 25](#__RefHeading___Toc2047_4158205933)

[2.3 Sprint 3 26](#__RefHeading___Toc2023_4158205933)

[2.3.1 Solução 26](#__RefHeading___Toc2045_4158205933)

[Evidência da execução de cada requisito: 26](#__RefHeading___Toc2071_4158205933)

[Evidência dos resultados: 26](#__RefHeading___Toc2069_4158205933)

[2.3.2 Retrospectiva da Sprint 26](#__RefHeading___Toc2043_4158205933)

[3. Considerações Finais 27](#__RefHeading___Toc2017_4158205933)

[3.1 Resultados 27](#__RefHeading___Toc2021_4158205933)

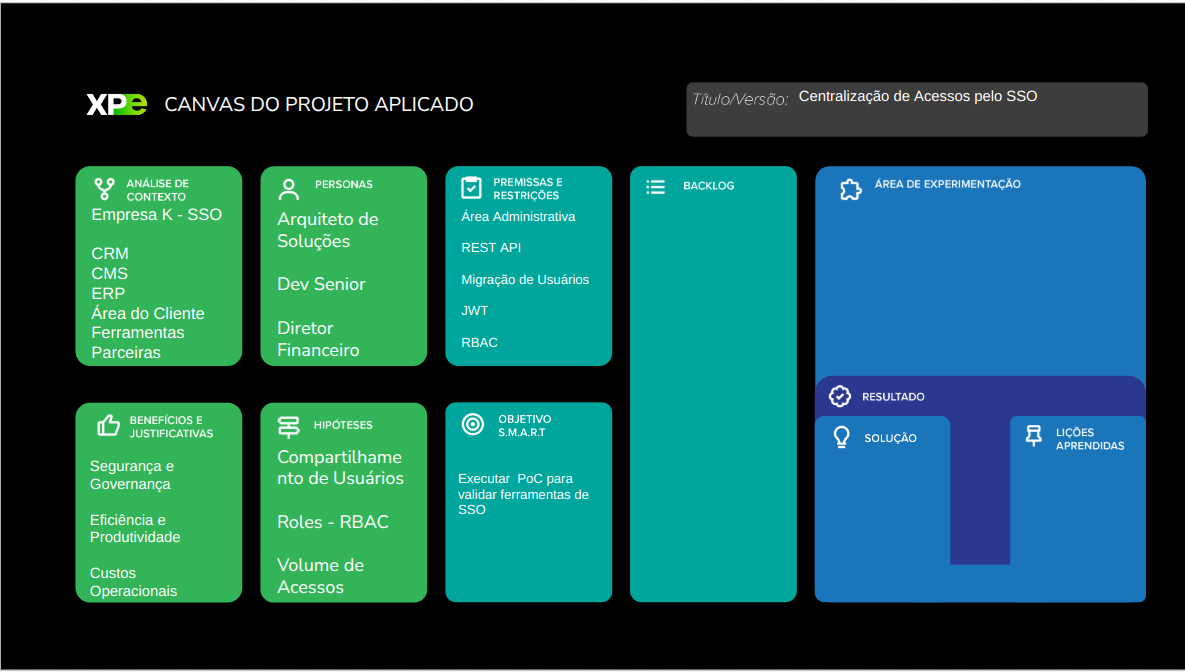
[3.2 Próximos passos 27](#__RefHeading___Toc2019_4158205933)

## 

## 

## 

## 1. CANVAS do Projeto Aplicado



## Desafio

### 1.1.1 Análise de Contexto

A **empresa K** atua como provedora de tecnologia para imobiliárias em expansão nacional e internacional, com presença nos Estados Unidos, Europa, Oriente Médio e Oceania. Seu portfólio de soluções é composto por:

* **CRM** – gestão de estoque, leads, equipe e integrações com portais e canais digitais.
* **CMS** – construção de sites imobiliários baseados no estoque.
* **ERP** – gestão administrativa de contratos, pagamentos, cobranças e assinaturas.
* **Área do Cliente** – gestão das assinaturas da empresa K, contratação de novos pacotes, upgrades e downgrades.
* **Ferramentas de Parceiros** – treinamentos e atendimentos com dependência da carga de usuários.

Com cada produto mantendo sua **base própria de usuários**, surgem dores relevantes:

* **Compartilhamento de sessão**: usuários únicos usados por várias pessoas, distorcendo métricas de consumo e prejudicando a definição correta de pacotes.
* **RPAs externos**: automações de terceiros usando credenciais compartilhadas, aumentando riscos de segurança.
* **Sobrecarga de infraestrutura**: acessos atípicos decorrentes de compartilhamento geram picos de requisições e ampliam custos de infraestrutura.
* **Gestão descentralizada de papéis**: permissões de usuários são definidas de forma isolada em cada produto.
* **Dificuldade na desativação**: a baixa de um usuário não reflete em todos os sistemas.

Essas dores reforçam a **necessidade estratégica** de adotar uma solução unificada de autenticação e autorização, com foco em segurança, governança e experiência de uso.

Para endereçar o problema, é necessário centralizar acessos via **SSO (Single Sign-On)**, permitindo que o usuário autentique-se uma única vez e acesse todas as aplicações de forma padronizada e segura.

Benefícios esperados:

* Redução de senhas e simplificação da experiência.
* Governança centralizada sobre acessos e permissões.
* Segurança reforçada com autenticação unificada.
* Menor esforço de TI na gestão de identidades.

Requisitos de Avaliação (com obrigatórios):

* **Área Administrativa (\*)** – gestão de usuários, aplicações e permissões.
* **REST API (\*)** – integração com microserviços para gestão de identidades.
* **OAuth 2.0 / OpenID Connect (OIDC)** – suporte a fluxos modernos de autenticação.
* **Federação com redes sociais** – login por Google, Facebook, LinkedIn etc.
* **Esqueci Minha Senha (\*)** – recuperação e redefinição seguras.
* **Cadastro de Usuários por E-mail** – autocadastro com validação e aprovação opcional.
* **Token Authentication (JWT) (\*)** – emissão, validação, renovação e revogação de tokens.
* **Multi-tenancy** – isolamento por cliente e possibilidade de compartilhamento controlado.
* **Customização de Login** – branding e campos adicionais conforme necessidade.
* **Impersonate** – suporte para acesso temporário de suporte com auditoria.
* **RBAC (\*)** – grupos, permissões e roles hierárquicas.
* **Rotação de Senha** – políticas de expiração e complexidade mínima.
* **Migração de Usuários sem Perda de Senha (\*)** – importação segura de hashes.

Ferramentas avaliadas para PoC:

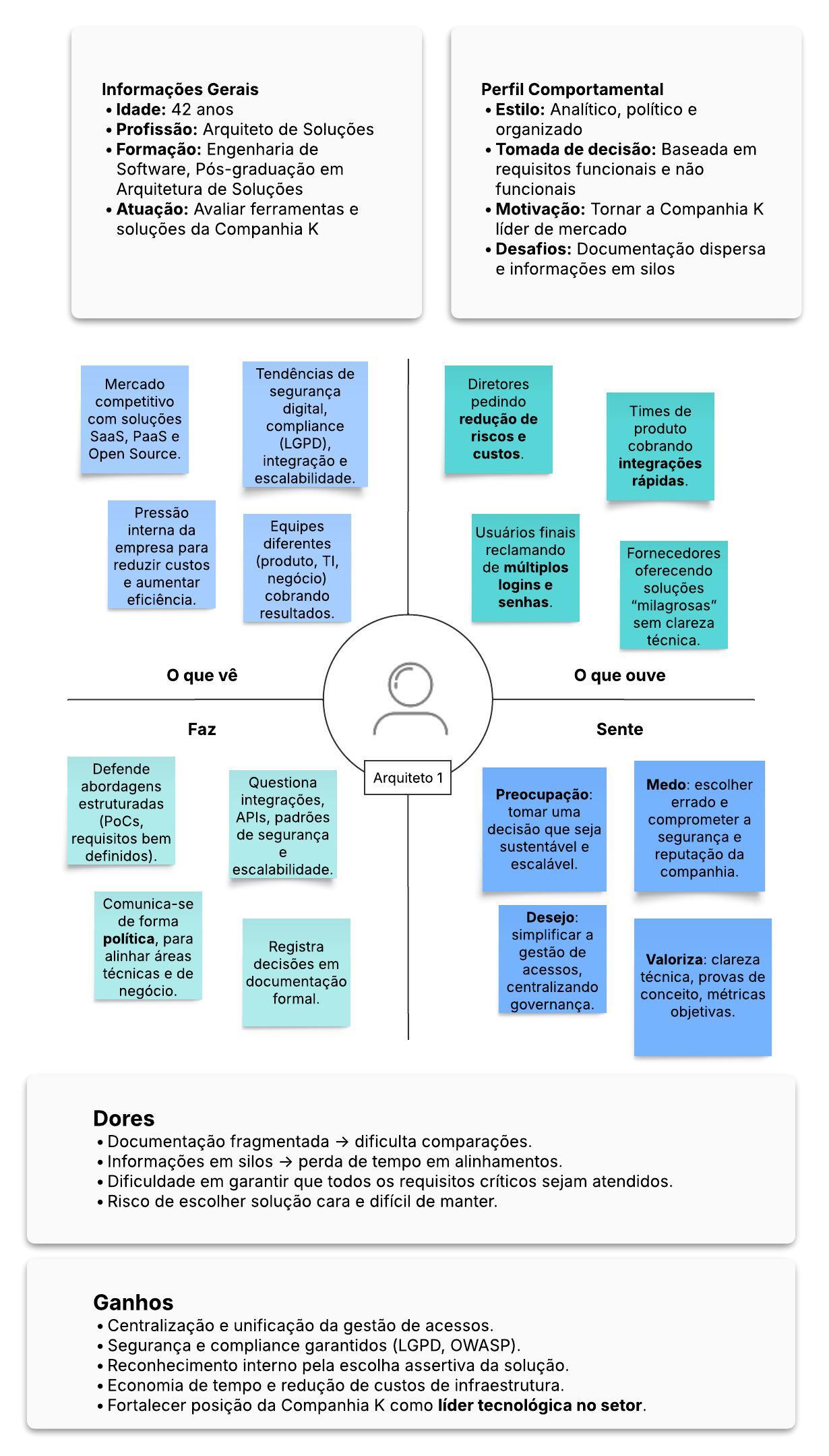
* Firebase Authentication (PaaS)
* KeyCloak (IaaS/Open Source)
* GCP IAM (PaaS)
* Auth0 by Okta (SaaS)
* Microsoft Entra ID (SaaS)

Como critério de decisão

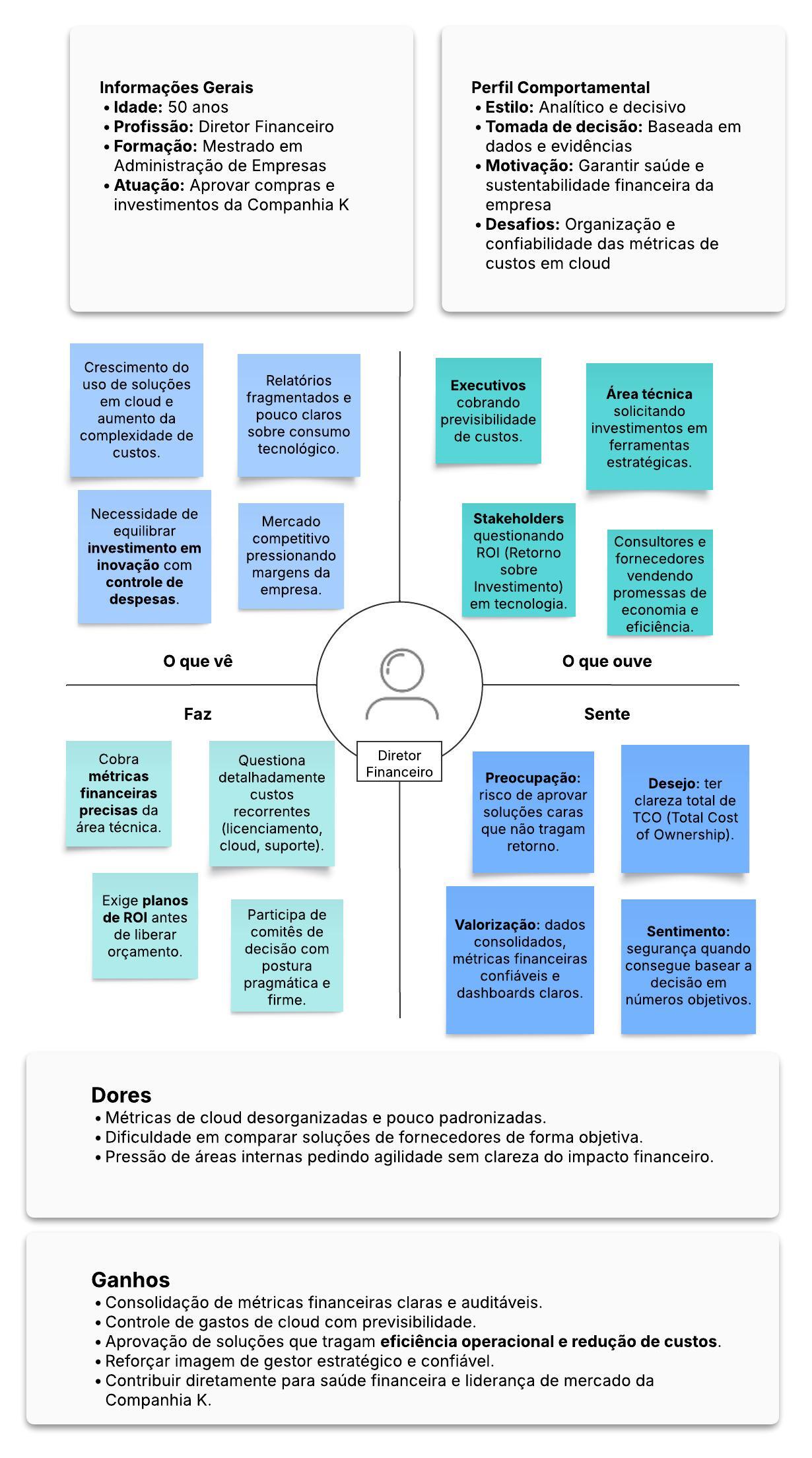
|  |  |  |
| --- | --- | --- |
| **Critério** | **Peso** | **Métrica de Avaliação** |
| Custo Operacional | Alto | Menor custo por usuário |
| Tempo de Implementação | Médio | Facilidade de integração |
| Segurança e Compliance | Alto | LGPD, OWASP Top 10 |
| Flexibilidade (RBAC, SAML) | Médio | Suporte a cenários complexos |

### 1.1.2 Personas

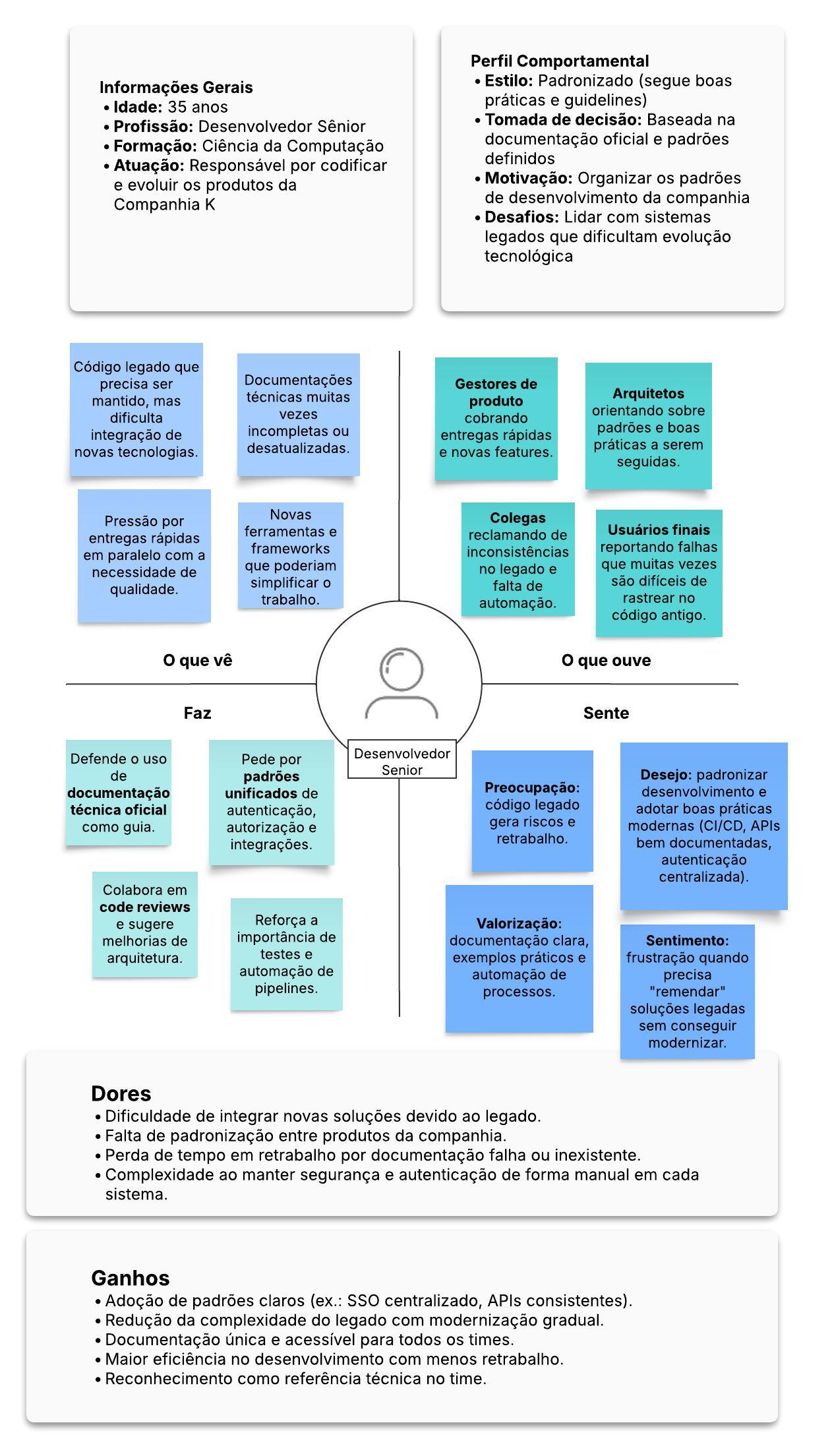
### 1.1.2.1 Arquiteto 1



### 1.1.2.2 Diretor Financeiro



### 1.1.2.3 Desenvolvedor Senior



### 1.1.3 Justificativas

A Companhia K atua no setor imobiliário com soluções tecnológicas que incluem CRM, CMS, ERP, Área do Cliente e Ferramentas de Parceiros. Cada produto possui sua própria base de usuários, gerando problemas críticos:

* **Compartilhamento de credenciais** entre múltiplos usuários e RPAs, resultando em riscos de segurança.
* **Gestão descentralizada de permissões**, tornando difícil controlar e auditar acessos.
* **Sobrecarga de infraestrutura** causada por acessos fora do padrão.
* **Dificuldade na desativação de usuários** em todos os sistemas de forma sincronizada.
* **Documentação fragmentada** e processos manuais que aumentam retrabalho.

Esse cenário impacta diretamente áreas técnicas, financeiras e operacionais, refletindo em **maiores custos de manutenção, riscos de segurança e insatisfação de usuários**.

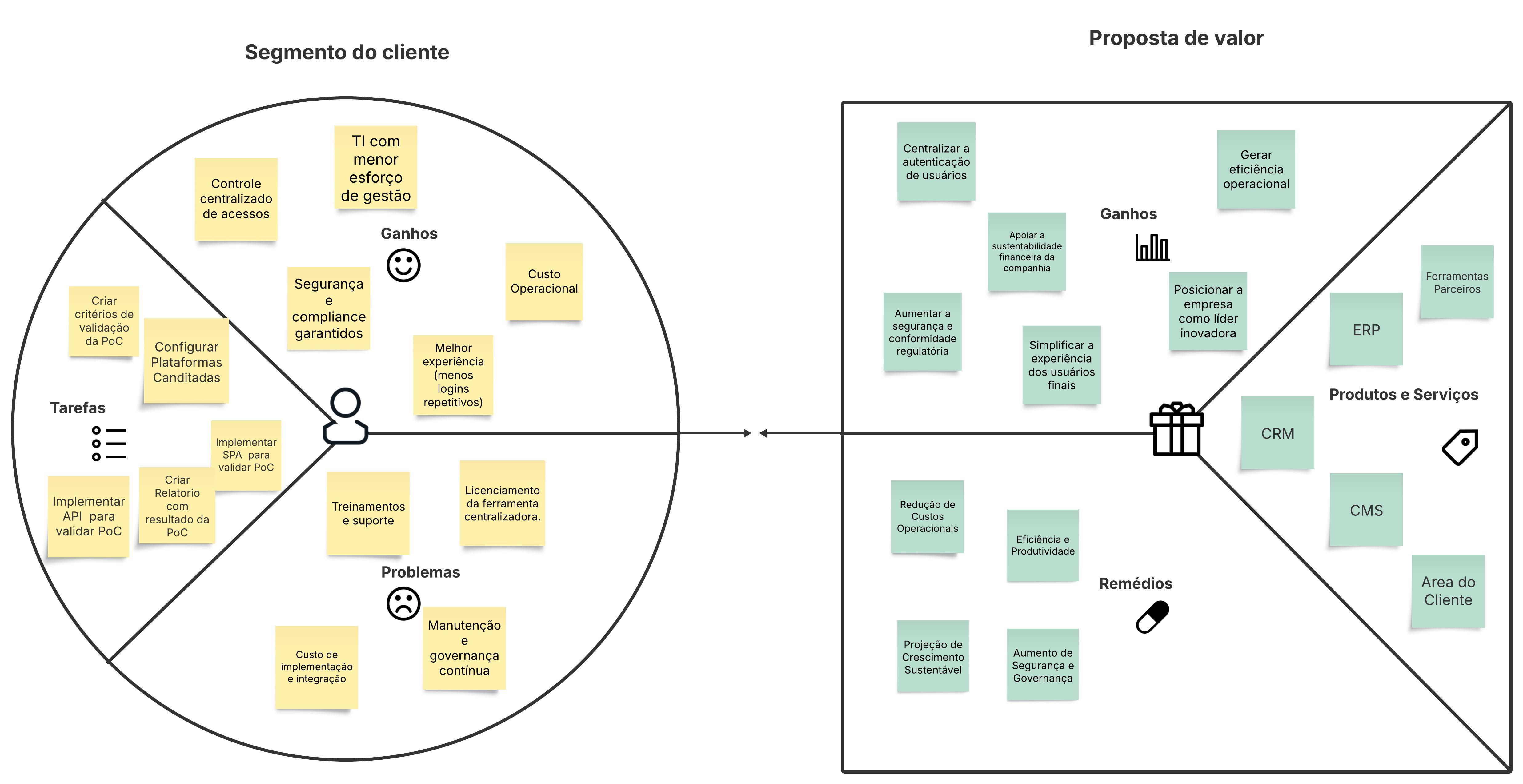
Fatores que Justificam a Implantação:

* **Redução de Custos Operacionais**
  + Eliminação de sobrecarga de infraestrutura causada por acessos indevidos.
  + Menor esforço da TI na gestão de usuários, roles e permissões.
  + Otimização de pacotes de licenciamento pela contabilização correta de usuários ativos.
* **Aumento de Segurança e Governança**
  + Autenticação unificada reduz vulnerabilidades do compartilhamento de credenciais.
  + Auditoria centralizada para conformidade com **LGPD e OWASP Top 10**.
  + Maior rastreabilidade e visibilidade de acessos.
* **Eficiência e Produtividade**
  + Usuários com menos fricção: apenas um login para acessar múltiplas soluções.
  + Times técnicos ganham agilidade ao adotar padrões claros (SSO, RBAC, APIs).
  + Redução do retrabalho com documentação e integrações descentralizadas.
* **Alinhamento Estratégico e Financeiro**
  + O Arquiteto de Soluções (Persona 1) terá ferramentas padronizadas para modernizar sistemas.
  + O Diretor Financeiro (Persona 2) contará com métricas claras de consumo em cloud e ROI.
  + O Desenvolvedor Sênior (Persona 3) terá guidelines técnicos unificados, reduzindo a complexidade do legado.
* **Projeção de Crescimento Sustentável**
  + Escalabilidade para suportar expansão internacional.
  + Capacidade de integração com provedores externos (Google, Microsoft, etc.).
  + Diferencial competitivo ao posicionar a Companhia K como referência tecnológica no setor imobiliário.

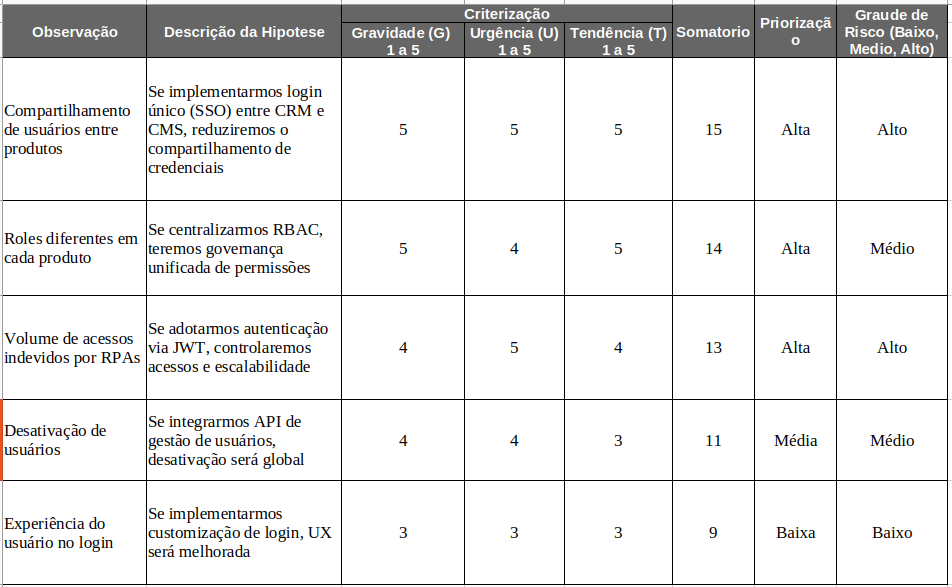
Proposta de Valor

A implantação de uma solução de **SSO (Single Sign-On)** permitirá à Companhia K:

* **Centralizar a autenticação de usuários** em todos os produtos e parceiros.
* **Aumentar a segurança e conformidade regulatória**, reduzindo riscos de compartilhamento indevido.
* **Simplificar a experiência dos usuários finais**, melhorando satisfação e engajamento.
* **Gerar eficiência operacional**, reduzindo custos e esforços da TI.
* **Apoiar a sustentabilidade financeira da companhia**, com previsibilidade de custos e ROI mensurável.
* **Posicionar a empresa como líder inovadora**, ao adotar práticas modernas de gestão de identidades e acessos.

****

### 1.1.4 Hipóteses

****

## 1.2 Solução

### 1.2.1 Objetivo SMART

**O objetivo da PoC é validar a integração de uma solução de Single Sign-On (SSO) para unificar o processo de autenticação entre os sistemas corporativos da Companhia K (S), garantindo um login único, seguro e eficiente. A iniciativa busca unificar a base de usuários, eliminar autenticações múltiplas e reduzir em 60% o esforço de gestão de usuários (M). A implementação do SSO é fundamental para melhorar a experiência do usuário, fortalecer o controle de acesso e aumentar a eficiência operacional (R). O projeto será executado com recursos existentes e validado em 3 sprints (T). O critério de aceite será a validação de uma das ferramentas, com demonstração de uso em uma aplicação SPA e em uma API, acompanhada da formatação e apresentação dos resultados da avaliação (A).**

### 1.2.2 Escopo do Projeto

**Este projeto tem como objetivo aplicar uma Prova de Conceito (PoC) em ferramentas de Single Sign-On (SSO), com o propósito de unificar as bases de usuários dos produtos da Companhia K.**

**A seguir, são apresentadas as premissas, restrições e consequências consideradas para o andamento do projeto.**

****Premissas****

1. **Considerando o tempo limitado, a infraestrutura para execução do projeto será configurada em ambiente local, utilizando Docker e VS Code.**
2. **Haverá acesso às aplicações de teste (SPA e API), que permitirão a validação completa do login único.**
3. **Será utilizada a ferramenta open-source Keycloak para demonstração dos requisitos obrigatórios.**
4. **As ferramentas SaaS com custos atrelados serão apresentadas apenas quanto ao cumprimento dos requisitos, sem utilização prática, devido ao custo envolvido.**

**Restrições**

1. **O projeto será desenvolvido apenas com recursos internos da Companhia K, sem aquisição de novas licenças ou infraestrutura adicional.**
2. **O prazo para execução está limitado a 3 sprints, conforme o planejamento inicial.**
3. **As validações estarão restritas ao ambiente local, não abrangendo implantação em produção.**
4. **O escopo da PoC se limita à autenticação e unificação de usuários, não incluindo autorização detalhada por papéis ou permissões.**
5. **As integrações serão testadas apenas em uma aplicação SPA e uma API REST, conforme critérios de aceite definidos.**

**Recursos, habilidades e conhecimentos necessários**

* ****Recursos**: Docker, imagem Keycloak, VS Code, Node.js 22, ReactJS.**
* ****Habilidades**: integração via protocolos OAuth2 e OpenID Connect, configuração de identidade federada, gestão de tokens e aplicação de boas práticas de segurança.**
* ****Conhecimentos**: arquitetura de autenticação corporativa, segurança da informação e APIs RESTful.**

### 1.2.3 Cronograma de Ações Planejadas

**O cronograma do projeto foi estruturado em 3 sprints semanais, totalizando 3 semanas de execução da Prova de Conceito (PoC) para integração de Single Sign-On (SSO).**

**Cada sprint contempla atividades técnicas, validações e checkpoints para garantir a entrega incremental dos resultados.**

****Sprint 1** – Configuração e Preparação do Ambiente**

**Duração: 1 semana  
**Atividades Principais**:**

* **Configuração do ambiente local utilizando Docker e VS Code.**
* **Implantação da imagem Keycloak e configuração inicial do servidor de identidade.**
* **Criação de usuários de teste e mapeamento dos atributos necessários para autenticação.**
* **Integração inicial com uma aplicação SPA para validação do fluxo Oauth2.**

****Entregas**: ambiente local funcional com Keycloak configurado e autenticação inicial validada na aplicação SPA.**

**Sprint 2 – Integração e Validação Técnica**

**Duração:** 1 semana  
**Atividades Principais:**

* Integração do SSO com a API REST utilizando OpenID Connect.
* Implementação de controle de sessão e renovação de tokens.
* Registro dos fluxos de autenticação e tratamento de erros.
* Validação da unificação dos usuários entre SPA e API.

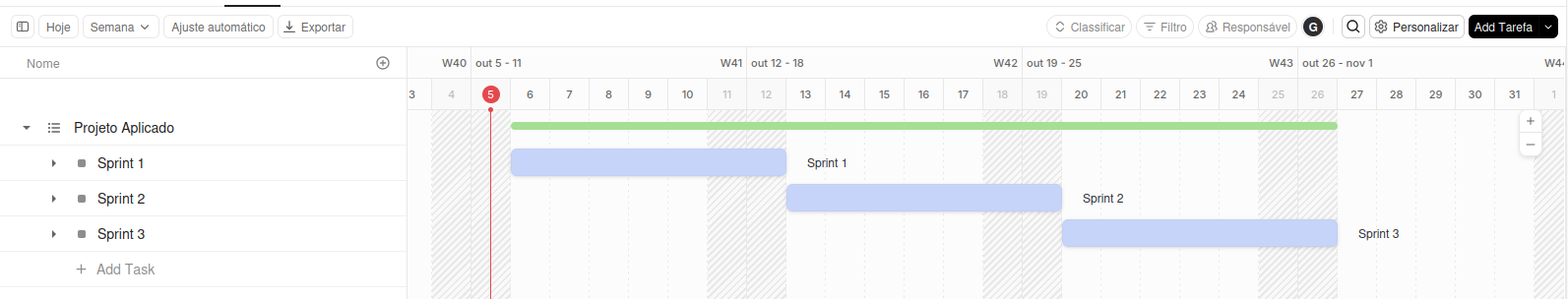
**Entregas:** autenticação integrada e validação técnica completa do fluxo SSO nas aplicações de teste.

**Sprint 3 – Avaliação, Documentação e Demonstração**

**Duração:** 1 semana  
**Atividades Principais:**

* Documentação dos resultados e evidências da PoC.
* Elaboração de relatório comparativo entre Keycloak e alternativas SaaS (Auth0, Okta).
* Preparação da demonstração final com login único funcionando entre SPA e API.
* Apresentação dos resultados e critérios de aceitação.

**Entregas**: relatório técnico consolidado e demonstração funcional da PoC de SSO.



# 2. Área de Experimentação

**O que significa esta seção?**

Esta seção tem o objetivo de apresentar as evidências do planejamento dos requisitos selecionados do Backlog de Produto, além de mostrar a maneira como eles foram desenvolvidos e registrar os resultados alcançados.

É necessário expor a execução e a validação dos experimentos relacionados ao desenvolvimento da solução, ou seja, testar se você está no caminho certo ou se algo precisa ser modificado (pivotar).

**Quais etapas já devem estar finalizadas no momento do preenchimento desta seção? (Pré-requisitos)**

No momento do preenchimento, é esperado que você já tenha cursado a disciplina de Inovação e Design Thinking, em especial as etapas do processo de Design Thinking, além de estar se preparando para desenvolver a solução idealizada no seu Projeto Aplicado.

Você também já deve ter preenchido o primeiro capítulo deste relatório (CANVAS do Projeto Aplicado).

**Como esta seção deve ser preenchida?**

Esta seção é a área mais dinâmica do CANVAS do Projeto Aplicado. Nela você deverá inserir os experimentos necessários para desenvolver e validar cada Sprint. Ao final do experimento, você deverá preencher o item “**Solução**” da seguinte maneira:

* **Evidência da execução de cada requisito**: para cada requisito planejado, adicione um artefato que comprove o cumprimento da etapa. Podem ser anexados, por exemplo, códigos, documentos, modelos, scripts, capturas de tela, entre outros. *Importante: o número de artefatos adicionados deve ser o mesmo que o número de requisitos planejados.*
* **Evidência da solução**: os requisitos implementados contribuem para o alcance de um resultado geral, que deverá ser comprovado neste campo. Isso será feito por meio de capturas de tela, gráficos, modelos, textos, figuras, tabelas, testes, entre outros.

Para cada Sprint, cite no item “**Retrospectiva da Sprint**” o que não foi validado, mas forneceu insights para ajuste da rota.

**Quais ferramentas devem ser utilizadas?**

Obs.: para realização desta seção, você deverá utilizar o Trello, Planner, Excel ou similares, de modo que apresente uma linha do tempo para a execução das ações planejadas.

## 2.1 Sprint 1

### 2.1.1 Solução

#### Evidência da execução de cada requisito:

#### Evidência dos resultados:

### 2.1.2 Retrospectiva da Sprint

## 2.2 Sprint 2

### 2.2.1 Solução

#### Evidência da execução de cada requisito:

#### Evidência dos resultados:

### 2.2.2 Retrospectiva da Sprint

## 2.3 Sprint 3

### 2.3.1 Solução

#### Evidência da execução de cada requisito:

#### Evidência dos resultados:

### 2.3.2 Retrospectiva da Sprint

# 3. Considerações Finais

## 3.1 Resultados

Por meio de um texto detalhado, apresente os principais resultados alcançados pelo seu Projeto Aplicado.

Cite os pontos positivos e negativos, as dificuldades enfrentadas e as experiências vivenciadas durante todo o processo.

## 3.2 Próximos passos

Descreva quais são os próximos passos que poderão contribuir com o aprimoramento da solução apresentada pelo seu Projeto Aplicado.