

LUCAS BASTOS FRANCO – 2310622

# DevHealth Solutions

## Governança em TI

Matéria: Governança de Tecnologia da  
Informação

Docente: Talles Santos

2025 – Anápolis

# SUMÁRIO

INTRODUÇÃO .....	3
SOBRE A EMPRESA .....	3
DESAFIO.....	3
RISCOS PRINCIPAIS .....	3
ESTRUTURA ANALÍTICA DE RISCOS .....	4
ANÁLISE QUALITATIVA .....	4
ATRASOS DE ENTREGAS .....	4
PROBLEMAS DE SEGURANÇA.....	4
BAIXA ADOÇÃO PELOS USUÁRIOS .....	5
DIFICULDADES EM CONFORMIDADE REGULATÓRIAS.....	5
EM SUMA E PRIORIZAÇÃO .....	5
ANÁLISE QUALITATIVA .....	5
IMPACTOS .....	5
NÍVEL ACEITÁVEL.....	7
ESTRATÉGIAS DE RESPOSTA.....	7
EVITAR OS RISCOS .....	7
MITIGAR OS RISCOS .....	7

# INTRODUÇÃO

Você faz parte da equipe de TI da empresa DevHealth com o objetivo de levantar riscos no desenvolvimento do sistema

## SOBRE A EMPRESA

A DevHealth Solutions é uma empresa especializada no desenvolvimento de software para o setor da saúde, atendendo hospitais, farmácias, clínicas médicas e laboratórios. Apesar da experiência acumulada ao longo de 10 anos, a empresa enfrentou desafios em projetos anteriores, como atrasos na entrega, problemas de segurança, baixa adoção pelos usuários e dificuldades em conformidade regulatória. Agora, a empresa inicia um novo projeto para um cliente estratégico e precisa garantir que os erros do passado não se repitam. Para isso, foi solicitado à equipe de TI um levantamento detalhado dos riscos envolvidos no desenvolvimento do sistema e uma análise criteriosa para mitigar problemas antes que impactem o projeto. O projeto é uma solução web para uma clínica de psicologia, a solução que cadastra paciente, agendar uma consulta e armazena um relatório do psicólogo.

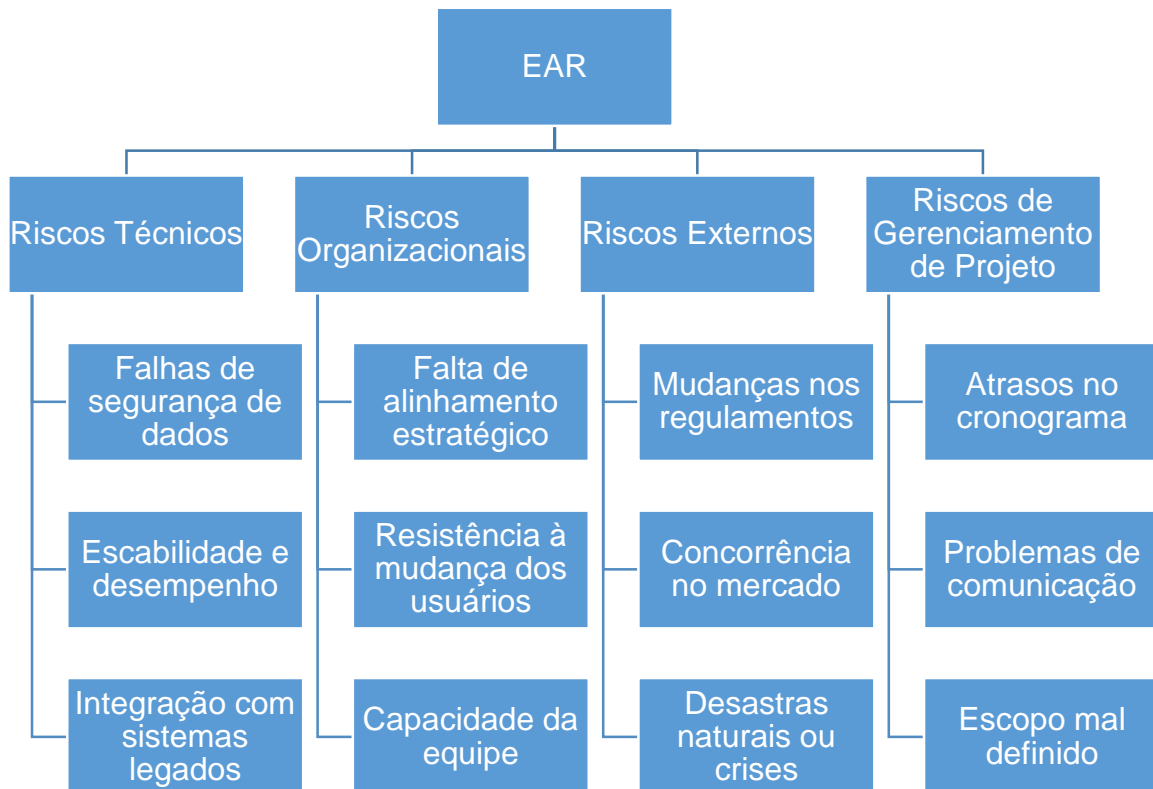
## DESAFIO

O objetivo da equipe de TI da DevHealth Solutions é identificar, analisar e mitigar proativamente os riscos associados ao desenvolvimento do novo sistema, garantindo a entrega dentro do prazo, a segurança dos dados, a conformidade regulatória e a adoção eficiente pelos usuários. Para isso, a equipe realizará um levantamento detalhado dos riscos, priorizando aqueles com maior impacto e probabilidade, aplicando análises qualitativas e quantitativas para mensurar seus efeitos e definir estratégias de resposta adequadas. Dessa forma, busca-se assegurar um projeto mais robusto, alinhado com as necessidades do cliente e com menor exposição a falhas críticas.

## RISCOS PRINCIPAIS

1. Atrasos de entregas
2. Problemas de segurança
3. Baixa adoção pelos usuários
4. Dificuldades em conformidade regulatórias

## ESTRUTURA ANALÍTICA DE RISCOS



## ANÁLISE QUALITATIVA

### ATRASOS DE ENTREGAS

Ao verificarmos com os Devs, mesmo sabendo que os riscos são contextuais, podemos previamente dizer que os seus impactos são uma ameaça ao projeto. Pois quando existem mais demorar na entrega do projeto, mais pode existir do cliente abandonar o projeto, que também é um risco de ameaça. Entretanto, sua probabilidade podemos considerá-la média, pois embora é um problema que vem ocorrendo, podemos separá-la em sprint menos. Concluindo que esse risco é de probabilidade média, mas com uma ameaça alta, sendo assim, seu risco é alto.

### PROBLEMAS DE SEGURANÇA

Quando falamos de segurança, é um tópico muito sensível dentro de uma empresa, sendo assim, o seu impacto é também uma ameaça para empresa. Sua

possibilidade também é alta, pois mexe com os dados dos clientes do projeto. Concluindo que esse risco é tem probabilidade alta com uma ameaça alta, sendo assim, seu risco é alto.

**BAIXA ADOÇÃO PELOS USUÁRIOS**

Quando falamos de segurança, é um tópico muito sensível dentro de uma empresa, sendo assim, o seu impacto é também uma ameaça para empresa. Sua possibilidade também é alta, pois mexe com os dados dos clientes do projeto. Concluindo que esse risco é tem probabilidade alta com uma ameaça alta, sendo assim, seu risco é alto.

**DIFICULDADES EM CONFORMIDADE REGULATÓRIAS**

Essa dificuldade, ao analisar o projeto pelo o que é, elas têm um impacto de ameaça alta, pois mexe como a legislação, se caso o risco vier a ser tonar um problema, e muito difícil de se contornar. Entretanto, elas têm uma probabilidade de ser baixa, pois se for feito um estudo e explorar a legislação vigilante, o risco pode ser anulado. Concluindo que esse risco é tem probabilidade baixa com uma ameaça alta, sendo assim, seu risco é alto.

**EM SUMA E PRIORIZAÇÃO**

TIPO	PROBABILIDADE	AMEAÇA	NÍVEL
Problemas de segurança	Alta	- Alta	Alta
Atraso de entregas	Médio	- Alta	Alta
Dificuldades em conformidade regulatórias	Baixo	- Alta	Média
Baixa adoção pelos usuários	Média	- Baixa	Baixo

**ANÁLISE QUALITATIVA**

**IMPACTOS**

**1. Atrasos de entregas:**

- IMPACTO FINANCEIRO: Mão de obra adicionais “horas extras”, penalidades contratuais e perda de oportunidade. Ou seja, ele vai ter uns custos adicional, tendo por volta de uns 10 mil.
- IMPACTO OPERACIONAL: Afetar o cronograma de trabalho da equipe, prejudicando a produtividade e o planejamento. Sem falar de comprometer a credibilidade da empresa com o stakeholders.
- REFERENCIA: [Falhas na Gestão dos Stakeholders](#)

## **2. Problemas de segurança:**

- IMPACTO FINANCEIRO: De acordo com a LGPD, artigo 7º, se caso a multa for simples, de acordo com a Lei LGPD, é de 2% do faturamento da empresa, limitada a 50 milhões por infração.
- IMPACTO OPERACIONAL: Perda de dados dos pacientes, além disso, há custos com a correção dos problemas, reestruturação da infraestrutura de segurança e tempo de inatividade.
- REFERENCIA: [Regulamento de Aplicação de Sanções](#)

## **3. Baixa adoção dos usuários:**

- IMPACTO FINANCEIRO: Se caso menos de 50% dos clientes adotarem o sistema, em sua fase final, a empresa pode ter uma redução 30% na receita esperada, gerando um prejuízo por volta de 5 mil mensais.
- IMPACTO OPERACIONAL: Desperdício de recurso, como por exemplo em campanhas de marketing e treinamento de usuários. Além disso, têm o ajuste e reformulação do produto.
- REFERENCIA: [Fatores Críticos de Adoção](#)

## **4. Dificuldades em conformidade regulatórias:**

- IMPACTO FINANCEIRO: A não conformidade, como a LGPD ou normas de saúde, podem resultar em multas significativas, custos com assessoria jurídica, além de comprometer a confiança de pacientes e parceiros.
- IMPACTO OPERACIONAL: Impedir o funcionamento do sistema ou obrigar a empresa a realizar ajustes substanciais. Isso pode resultar em atraso no lançamento do produto, além de aumentar os custos
- REFERENCIA: [Desafios de Compliance no Setor](#)

## NÍVEL ACEITÁVEL

Com base na análise, a empresa deve manter um nível de risco aceitável de até **R\$100.000,00** em impactos financeiros e garantir conformidade total com normas regulatórias, pois falhas nesses aspectos podem inviabilizar o projeto.

## ESTRATÉGIAS DE RESPOSTA

A estratégia é que a gente vai tentar evitar todos os riscos da melhor forma possível e a todo custo. Se caso não seja possível evita-lo, iremos mitigar para que os danos ou que os problemas sejam menores, mas só em último caso, como um plano B.

### EVITAR OS RISCOS

**Atrasos na entrega:** Utilizar metodologias ágeis para entregas incrementais e monitoramento contínuo do cronograma.

**Problemas de segurança:** Implementar políticas rigorosas de criptografia e acesso restrito desde o início.

**Baixa adoção dos usuários:** Realizar testes de usabilidade contínuos e envolver stakeholders na fase inicial do projeto.

**Dificuldades em conformidade regulatórias:** Contratar consultores especializados para validar requisitos legais antes do desenvolvimento.

### MITIGAR OS RISCOS

**Atrasos na entrega:** Alocar recursos extras em períodos críticos do projeto.

**Problemas de segurança:** Implementar auditorias de segurança regulares e planos de resposta a incidentes.

**Baixa adoção dos usuários:** Treinamento e suporte contínuo pós-implantação para incentivar a aceitação do sistema.

**Dificuldades em conformidade regulatórias:** Realizar testes contínuos de conformidade e ajustes incrementais.