**Cenários e Riscos**

**1. Riscos Técnicos**

* **Falhas de integração** com máquinas e sistemas legados (ERP, chão de fábrica).
* **Bugs no software** que podem comprometer a operação.
* **Segurança da informação**, risco de vazamento de dados de produção.
* **Escalabilidade**, sistema não suportar aumento da demanda.

**2. Riscos de Mercado**

* **Baixa adesão dos usuários internos** (funcionários resistirem à mudança).
* **Concorrência agressiva**, com soluções já consolidadas no mercado.
* **Custos de implantação** percebidos como altos pelos clientes.
* **Mudanças na legislação trabalhista ou de segurança**, impactando processos.

**3. Estratégias de Mitigação**

* Implantar **testes automatizados e manuais** para reduzir falhas críticas.
* Realizar **projetos-piloto em pequena escala** antes da implementação completa.
* Criar **treinamentos e manuais de uso**, garantindo maior aceitação dos funcionários.
* Fazer **pesquisa de mercado e validação contínua com clientes**, ajustando funcionalidades.
* Implementar **protocolos de backup e cibersegurança**.

**4. Planos Alternativos**

* Se a integração com máquinas não funcionar → adotar **módulo manual ou híbrido** até estabilizar.
* Se houver baixa adesão → **simplificar a interface** e incluir **etapas de capacitação**.
* Se os custos forem impeditivos → oferecer **versão modular** do sistema, com funcionalidades básicas e possibilidade de expansão.
* Caso a concorrência avance mais rápido → buscar **parcerias estratégicas** com fornecedores ou fabricantes.

# Matriz de Risco

| **Risco** | **Probabilidade** | **Impacto** | **Classificação** | **Estratégia de Mitigação** |
| --- | --- | --- | --- | --- |
| Falhas de integração | Alta | Alta | Crítico | Testes, pilotos, suporte técnico especializado |
| Bugs no software | Média | Alta | Alto | Testes automatizados, QA contínuo |
| Segurança da informação | Média | Alta | Alto | Criptografia, backups, firewalls |
| Escalabilidade insuficiente | Baixa | Alta | Médio | Arquitetura em nuvem, monitoramento de performance |
| Baixa adesão dos usuários | Alta | Média | Alto | Treinamentos, UX simplificada |
| Concorrência agressiva | Média | Média | Médio | Diferenciação de funcionalidades, foco no nicho |
| Custos de implantação altos | Média | Média | Médio | Versão modular, planos escaláveis |
| Mudanças legais/regulatórias | Baixa | Média | Baixo | Monitoramento contínuo da legislação |

### Importância da Gestão de Riscos

A gestão de riscos é fundamental para aumentar as chances de sucesso de qualquer projeto, especialmente em sistemas voltados para fábricas e metalúrgicas. Esse processo serve para **identificar, avaliar e se preparar para possíveis problemas**, de forma que eles causem o menor impacto possível.

Os **riscos técnicos** são um dos pontos mais importantes, já que falhas de integração com máquinas, erros no software ou até problemas de segurança podem afetar diretamente a produção. Além disso, existem os **riscos de mercado**, como a resistência dos funcionários em usar a nova solução, a concorrência de empresas já estabelecidas ou até a percepção de que o custo de implantação é muito alto.

Para reduzir esses riscos, é importante adotar **estratégias de prevenção**, como testes frequentes, projetos-piloto, treinamentos para os usuários e medidas de segurança digital. Também é essencial ter **planos alternativos**, que servem como rotas de ação caso algo não saia como esperado. Assim, o projeto não fica parado diante de um imprevisto.

Uma ferramenta que ajuda muito nesse processo é a **matriz de risco**, que cruza a probabilidade de um problema acontecer com o impacto que ele teria no projeto. Isso permite identificar rapidamente quais riscos são mais críticos e precisam de maior atenção.

No fim, a gestão de riscos garante mais **segurança, organização e confiabilidade**. Ela ajuda a reduzir custos inesperados, aumenta a confiança de todos os envolvidos e melhora as chances de o projeto ser bem-sucedido.