Plano de Gestão de Risco

Gestão de Projetos de Software

São Paulo

2025

INTEGRANTES DO PROJETO e RA'S

Daniel Baptista Acioli Vanderlei	23025608
Fábio Oliveira Spíndola	22086131
Fabrício Cândido do Nascimento	23025273
Leonardo de Souza Mouzinho	23025627

Sumário

1. Introdução

A Pick Your Driver é uma plataforma que reúne informações de diversas empresas de transporte por aplicativo (como Uber, 99, entre outras), permitindo ao usuário comparar preços, tempo estimado de chegada e opções disponíveis. O crescimento do mercado de mobilidade urbana e a competitividade das tarifas tornam a ferramenta atraente para os usuários que buscam economia e praticidade.

Este Plano de Gestão de Risco tem como propósito identificar possíveis ameaças, avaliar a probabilidade e o impacto de cada uma delas, definir estratégias de mitigação e criar planos de contingência para manter a operação do site e garantir a satisfação de seus usuários.

2. Escopo e Objetivos

2.1. Escopo

Envolve todas as áreas da plataforma, incluindo infraestrutura tecnológica, banco de dados, integrações com APIs de terceiros, componentes de interface e experiência do usuário.

Abrange riscos financeiros, operacionais, de segurança da informação, legais e reputacionais.

2.2. Objetivos

- **Identificar** os principais riscos que podem afetar o Pick Your Driver;
- **Avaliar** o grau de probabilidade e impacto de cada risco;
- **Desenvolver** planos de resposta (mitigação, contingência) para reduzir ameaças e suas consequências;e
- **Monitorar e revisar** continuamente o ambiente de risco para aprimorar as estratégias de proteção.

3. Metodologia

1. **Identificação de Riscos:** Listar todos os eventos ou circunstâncias que possam afetar negativamente a operação do site, sejam eles internos ou externos;
2. **Análise e Avaliação de Riscos:** Determinar probabilidade e impacto de cada risco, classificando-os em categorias de prioridade;
3. **Planejamento de Resposta:** Definir ações para prevenir, reduzir ou responder a cada risco identificado;
4. **Implementação e Monitoramento:** Garantir a execução das ações definidas e monitorar a efetividade dessas medidas;
5. **Revisão Contínua**: Adaptar o plano conforme o ambiente de negócios e tecnologia evolui, atualizando a lista de riscos e estratégias de mitigação.

4. Identificação de Riscos

A tabela abaixo descreve os principais riscos identificados:

Categoria	Risco
Tecnologia	• Falhas de servidor ou indisponibilidade de infraestrutura. • Vulnerabilidades de segurança (ataques cibernéticos, vazamentos de dados).
Operacional	• Integração interrompida com APIs de parceiros (Uber, 99 etc.). • Lentidão no carregamento ou processamento das informações.
Legal e Compliance	• Falha no cumprimento de leis de proteção de dados (LGPD, GDPR). • Violações de propriedade intelectual e uso indevido de API.
Financeiro	• Redução de receita pela concorrência de plataformas similares. • Custos inesperados com infraestrutura ou parcerias.
Reputacional	• Reclamações públicas ou avaliações negativas de usuários. • Exposição negativa na imprensa por falhas de segurança.
Recursos Humanos	• Falta de pessoal especializado em TI e segurança. • *Turnover* alto na equipe de desenvolvimento e suporte.
Gerenciamento de Projetos	• Atrasos em lançamentos de funcionalidades críticas. • Falhas no cronograma de melhorias ou manutenção.

5. Avaliação de Riscos

Os riscos foram avaliados utilizando os conceitos da Matriz GUT, conforme exemplificado na tabela abaixo:

Descrição	Probabilidade (P)	Impacto (I)	Prioridade (P × I)
Falhas de servidor ou indisponibilidade de infraestrutura	2 (Médio)	3 (Alto)	6 (Prioridade Alta)
Vulnerabilidades de segurança (ataques cibernéticos, vazamentos de dados)	2 (Médio)	3 (Alto)	6 (Prioridade Alta)
Falha na integração com APIs de parceiros	3 (Alto)	2 (Médio)	6 (Prioridade Alta)
Lentidão no carregamento ou processamento das informações	2 (Médio)	2 (Médio)	4 (Média)
Não cumprimento de leis de proteção de dados (LGPD, GDPR)	2 (Médio)	3 (Alto)	6 (Prioridade Alta)
Violações de propriedade intelectual e uso indevido de API	1 (Baixo)	2 (Médio)	2 (Baixa)
Redução de receita pela concorrência	2 (Médio)	2 (Médio)	4 (Média)
Custos inesperados com infraestrutura ou parcerias	2 (Médio)	2 (Médio)	4 (Média)
Reclamações públicas ou avaliações negativas de usuários	3 (Alto)	2 (Médio)	6 (Prioridade Alta)
Exposição negativa na imprensa por falhas de segurança	2 (Médio)	3 (Alto)	6 (Prioridade Alta)
Falta de pessoal especializado em TI e segurança	2 (Médio)	2 (Médio)	4 (Média)
Turnover alto na equipe de desenvolvimento e suporte	2 (Médio)	2 (Médio)	4 (Média)
Atrasos em lançamentos de funcionalidades críticas	2 (Médio)	2 (Médio)	4 (Média)
Falhas no cronograma de melhorias ou manutenção	2 (Médio)	2 (Médio)	4 (Média)

6. Planejamento de Resposta

6.1. Riscos prioritários (Alta Severidade)

Envolvem falhas de infraestrutura, vulnerabilidades de segurança, problemas de integração com APIs de parceiros, descumprimento de leis de proteção de dados, reclamações públicas de usuários e exposição negativa na imprensa.

As principais estratégias de mitigação incluem redundância de servidores em nuvem, testes de segurança (*pentests*), monitoramento de SLA das APIs, adequação às legislações (LGPD/GDPR), canais de suporte eficientes e práticas de comunicação transparente.

As contingências abrangem planos de recuperação de desastre (DRP), isolamento de sistemas comprometidos, notificações legais em casos de vazamento de dados, mensagens de alerta ao usuário sobre indisponibilidade de APIs, respostas rápidas a reclamações e declarações oficiais para a imprensa.

6.2. Riscos de severidade média ou baixa

Tratam de lentidão no carregamento, concorrência financeira, custos imprevistos, falta de pessoal especializado, turnover de equipe e atrasos em cronogramas de desenvolvimento. As respostas incluem otimização de desempenho, reserva de orçamento emergencial, recrutamento e treinamento, retenção de talentos e adoção de metodologias ágeis.

7. Monitoramento e Controle

1. **Reuniões Periódicas de Risco:** A equipe de gestão se reúne mensalmente para revisar o status dos riscos, avaliar o surgimento de novos e verificar a eficácia das ações de mitigação;
2. **Ferramentas de Monitoração e Log:** Utilizar soluções de *logging* para acompanhar métricas de infraestrutura, desempenho e segurança;
3. **Indicadores de Risco**: Definir *Key Risk Indicators* (KRIs) que possam sinalizar, com antecedência, a elevação do nível de risco;
4. **Auditorias e Testes de Penetração:** Realizar periodicamente para garantir o cumprimento das normas de segurança e detectar vulnerabilidades antecipadamente;
5. **Relatórios Regulares:** Emitir relatórios para a equipe de gestão e partes interessadas, informando sobre incidentes, ações corretivas e indicadores de desempenho.

8. Conclusão

A Pick Your Driver depende fortemente de disponibilidade, segurança e transparência para manter a confiança de seus usuários e parceiros. Este Plano de Gestão de Risco fornece uma estrutura para prevenção e resposta a eventos adversos, promovendo uma cultura de melhoria contínua e responsabilidade compartilhada na organização.

A eficácia do plano depende do compromisso de toda a equipe em monitorar, reportar e agir de forma proativa frente aos riscos. Revisões constantes e atualizações de procedimentos são cruciais para acompanhar a evolução do mercado e das tecnologias, garantindo o sucesso e a longevidade da Pick Your Driver.