

# Gerenciamento de Riscos

## Planejamento

O projeto utilizará “brainstorming” e “checklists” para a identificação de riscos e uma Matriz de Probabilidade e Impacto 3x3 para análise qualitativa, além das quatro estratégicas principais de resposta (evitar, mitigar, transferir, aceitar). Serão agendadas reuniões de 30 minutos a cada 2 semanas para as atividades de gerenciamento de riscos com todos os membros da equipe para discutir riscos nas categorias técnico e gerencial, além de 1 reunião de 30 minutos contendo os principais “stakeholders” para alinhar os ricos nas categorias comercial e externo. Os riscos serão classificados através da matriz de riscos durante a análise qualitativa onde será relacionado 1 dos 3 níveis de probabilidade possíveis (baixo, médio e alto) e 1 dos 3 níveis de impacto possíveis (insignificante, moderado e catastrófico) para classificar o risco. Esse documento estará disponível no repositório remoto localizado em [Github: Gerencia de riscos, Gerencia de projeto Hotel Green Garden](#), onde o mesmo poderá ser visto e editado pelos membros da equipe. Os membros da equipe de desenvolvimento ficarão responsável pela análise e identificação dos riscos, o membro identificado como proprietário do risco ficará responsável pelo seu devido monitoramento e controle e a Gerencia do Projeto ficará responsável pela liderança dos processos.

## Identificação

	Riscos técnicos, de qualidade, ou de desempenho	Riscos do gerenciamento do projeto	Riscos organizacionais	Riscos externos
Risco	Vulnerabilidades nas tecnologias escolhidas que possam causar problemas de performance, segurança, disponibilidade e consistência dos serviços.	Insatisfação do cliente dada por falta de cobertura dos requisitos.	Afastamento de funcionários.	Problemas de infraestrutura que atrasem o desenvolvimento do projeto como falta de luz, internet.
				Saída do cliente do ramo, como por exemplo falência, problemas ambientais que afetam o negócio ou decisões políticas que afetem o mesmo.
				Interesse de terceiros no sistema desenvolvido.

## Análise qualitativa

Probabilidade	Impacto		
	Baixo	Médio	Alto
Baixo	<b>4. Problemas de infraestrutura</b>		
Médio		<b>3. Afastamento de funcionários</b>	<b>1. Vulnerabilidades nas tecnologias 2. Insatisfação do cliente</b>
Alto			<b>5. Saída do cliente do ramo 6. Interesse de terceiros</b>

## Resumo da Análise

**Riscos Altos (Prioridade Máxima):** Os riscos relacionados a vulnerabilidades técnicas e à insatisfação do cliente são os mais críticos. Eles possuem uma chance razoável de ocorrer e seu impacto pode comprometer seriamente o sucesso do projeto. Requerem planos de mitigação e monitoramento constantes.

**Riscos Moderados (Atenção Necessária):** O afastamento de funcionários, a saída do cliente do ramo e o interesse de terceiros necessitam de atenção. Planos de contingência devem ser desenvolvidos para lidar com esses eventos caso ocorram.

**Risco Baixo (Monitoramento Mínimo):** Problemas de infraestrutura representam a menor ameaça ao projeto, exigindo apenas um monitoramento ocasional.

## Análise quantitativa

### Escala de Probabilidade

A probabilidade de alguns riscos, como a insatisfação do cliente, aumenta em projetos curtos devido à pressão e menor tempo para correções.

- **Baixa:** 10% de chance de ocorrer.
- **Média:** 50% de chance de ocorrer
- **Alta:** 70% de chance de ocorrer.

### Escala de Impacto (Financeiro)

O impacto é relativo ao orçamento de R\$ 251.043,13.

- **Baixo:** Custo adicional de R\$ 15.000,00 (um pequeno atraso ou retrabalho que consome parte da margem de lucro).
- **Médio:** Custo adicional de R\$ 75.000,00 (um problema sério que exige alocação de mais recursos e ameaça a rentabilidade do projeto).

- **Alto:** Custo adicional de R\$ 200.000,00 (um evento catastrófico que consome a maior parte do orçamento, inviabilizando o projeto ou causando perdas severas).

Rank	Risco	Probabilidade	Impacto (R\$)	Valor Monetário Esperado (VME)
1	Saída do cliente do ramo	70%	R\$ 200.000,00	R\$ 140.000,00
2	Interesse de terceiros no sistema	70%	R\$ 200.000,00	R\$ 140.000,00
3	Insatisfação do cliente por falta de cobertura dos requisitos	50%	R\$ 200.000,00	R\$ 100.000,00
4	Vulnerabilidades nas tecnologias escolhidas	50%	R\$ 200.000,00	R\$ 100.000,00
5	Afastamento de funcionários	50%	R\$ 75.000,00	R\$ 37.500,00
6	Problemas de infraestrutura	10%	R\$ 15.000,00	R\$ 1.500,00

## Planejamento das Respostas

### Riscos de Prioridade Crítica/Alta

Risco (Prioridade)	VME	Estratégia de Resposta	Responsável
<b>3. Insatisfação do cliente por falta de cobertura dos requisitos</b>	R\$ 100.000,00	Mitigar	Gerente de Projetos

### Ações de Resposta

1. **Prototipação Rápida:** Antes de iniciar o desenvolvimento de uma funcionalidade complexa, criar um protótipo navegável (usando ferramentas como Figma) para validação visual e funcional com o cliente.
2. **Ciclos Curtos de Feedback:** Implementar sprints de 1 semana, com uma cerimônia de Sprint Review obrigatória ao final de cada ciclo para apresentar o incremento e obter feedback formal.
3. **Critérios de Aceite Claros:** Não iniciar nenhuma tarefa sem que seus critérios de aceite estejam claramente definidos e validados pelo Product Owner (PO) ou pelo cliente.
4. **Gerenciamento de Mudanças:** Formalizar todo e qualquer pedido de alteração de escopo, analisando seu impacto no prazo e custo antes da aprovação.

### Gatilho/Indicador

- Pedidos de alteração frequentes em funcionalidades já entregues.
- Feedback negativo recorrente nas Sprint Reviews.
- Cliente demonstra dificuldade em descrever o que espera.

Risco (Prioridade)	VME	Estratégia de Resposta	Responsável
4. Vulnerabilidades nas tecnologias escolhidas	R\$ 100.000,00	Evitar	Desenvolvedores, Analistas

## Ações de Resposta

- Análise Estática de Código (SAST):** Integrar uma ferramenta de SAST (ex: SonarQube, Snyk) ao pipeline de integração contínua (CI) para identificar vulnerabilidades automaticamente a cada novo *commit*.
- Revisão de Código (Code Review):** Tornar o processo de *Pull Request* com revisão por pares obrigatório para 100% do código que será integrado à base principal.
- Testes de Segurança:** Alocar tempo no final do projeto (ex: última semana) para a realização de testes de penetração básicos nos pontos mais críticos do sistema.
- Bibliotecas Confiáveis:** Manter uma política de utilizar apenas bibliotecas e frameworks com suporte ativo da comunidade e sem vulnerabilidades conhecidas.

## Gatilho/Indicador

- Aumento no número de vulnerabilidades críticas apontadas pela ferramenta de SAST.
- Descoberta de uma falha de segurança durante os testes de QA.
- Publicação de uma vulnerabilidade grave (CVE) em uma dependência do projeto.

## Riscos de Prioridade Média

Risco (Prioridade)	VME	Estratégia de Resposta	Responsável
1. Saída do cliente do ramo	R\$ 140.000,00	Transferir / Aceitar (Ativo)	Gerente de Projeto

## Ações de Resposta

- Cláusulas Contratuais (Transferir):** Garantir que o contrato inclua cláusulas de pagamento por entregas parciais (marcos) e uma multa por rescisão antecipada que cubra os custos incorridos até o momento.
- Monitoramento (Aceitar):** Acompanhar notícias e indicadores de mercado sobre a saúde financeira do cliente e seu setor de atuação.

## Gatilho/Indicador

- Atrasos recorrentes nos pagamentos.
- Notícias negativas sobre o mercado de atuação do cliente.
- Comunicação do cliente sobre reestruturação interna.

Risco (Prioridade)	VME	Estratégia de Resposta	Responsável
3. Interesse de terceiros no sistema	R\$ 100.000,00	Mitigar / Transferir	Gerente de Projeto

## Ações de Resposta

- Boas Práticas de Segurança (Mitigar):** Implementar controles de acesso robustos (RBAC), criptografia para dados sensíveis (em trânsito e em repouso) e logs de auditoria.
- Acordo de Confidencialidade (Transferir):** Firmar um Acordo de Não Divulgação (NDA) com todos os membros da equipe e com o cliente, estabelecendo responsabilidades legais sobre o sigilo das informações.

## Gatilhos/Indicador

- Logs do sistema indicando tentativas de acesso não autorizado. - Vazamento de informações sobre o projeto.

	Risco (Prioridade)	VME	Estratégia de Resposta	Responsável
<b>5. Afastamento de funcionários</b>		R\$ 37.500,00	<b>Mitigar</b>	Gerente de Projeto

## Ações de Resposta

- Documentação e Conhecimento Compartilhado:** Incentivar a documentação contínua e a prática de programação em par em tarefas críticas para evitar que o conhecimento fique centralizado em uma única pessoa.
- Mapeamento de Sucessão:** Identificar os membros-chave e garantir que pelo menos mais uma pessoa tenha conhecimento básico sobre suas responsabilidades.

## Gatilho/Indicador

- Sinais claros de desmotivação de um membro da equipe.
- Comunicação de um membro sobre participação em outros processos seletivos.

## Risco de Prioridade Baixa

	Risco (Prioridade)	VME	Estratégia de Resposta	Responsável
<b>6. Problemas de infraestrutura</b>		R\$ 1.500,00	<b>Aceitar (Ativo)</b>	Gerente de Projeto

## Ações de Respostas

- Plano de Contingência de Trabalho Remoto:** Ter uma política clara para que a equipe possa trabalhar de casa imediatamente em caso de problemas no escritório.
- Infraestrutura em Nuvem:** Garantir que todo o ambiente de desenvolvimento, repositório de código (Git) e comunicação esteja baseado em nuvem, acessível de qualquer local.

## Gatilho/Indicador

- Aviso da concessionária de energia sobre manutenção programada.
- Previsão de eventos climáticos severos que possam afetar a infraestrutura local.

## Gestão da Reserva de Contingência

A análise quantitativa indicou uma exposição total de **R\$ 519.000,00**, valor superior ao orçamento. A soma dos VMES dos dois principais riscos é de **R\$ 280.000,00**.

**Ação:** É fundamental apresentar esta análise aos patrocinadores do projeto e negociar a criação de uma reserva de contingência de, no mínimo, **R\$ 62.500,00** (30% do orçamento).

**Justificativa:** Esta reserva não é um custo adicional, mas sim um valor provisionado para ser utilizado na execução das ações de resposta caso um dos riscos se materialize, garantindo que o projeto possa absorver o impacto sem fracassar.