FECAP – Fundação Escola Álvares Penteado

Levantamento de Riscos, Vulnerabilidades e Ameaças

Adriano Xu Ming Hui

Cauã Willian Brandão – 24025752

Gabriel Orlandi Portes – 24026407

Karoline Lemos Avelar – 24026456

Matheus Santoro Veiga - 19020057

Sumário

1. Introdução

Este documento apresenta o levantamento de riscos, vulnerabilidades e ameaças relacionados ao projeto em andamento. O objetivo é identificar potenciais fatores que possam comprometer o cronograma, o orçamento, a qualidade e a segurança da execução, bem como propor recomendações que minimizem impactos negativos. Esse processo é fundamental para o gerenciamento de projetos, pois fornece subsídios para tomadas de decisão mais seguras e para a elaboração de planos de contingência.

2. Definições

2.1. Risco

Qualquer evento incerto que possa impactar negativamente o cronograma, o orçamento, a qualidade ou o desempenho do projeto. Os riscos podem ser internos ou externos e devem ser constantemente monitorados.

2.2. Vulnerabilidade

Fragilidade do projeto ou do ambiente de desenvolvimento que pode ser explorada por uma ameaça. A existência de vulnerabilidades aumenta a probabilidade de ocorrência de riscos.

2.3. Ameaça

Evento ou condição, interna ou externa, que pode afetar negativamente o sucesso do projeto. As ameaças podem ser de natureza tecnológica, humana, ambiental ou regulatória.

3. Identificação dos Riscos

Durante a análise, foram identificados os seguintes riscos principais:

- - Perda de informações relevantes devido à inexistência de políticas de backup adequadas.
- - Atrasos no cronograma em decorrência de falhas técnicas, indisponibilidade de recursos ou imprevistos.
- - Custos adicionais causados por incidentes de segurança, retrabalho ou necessidade de correções emergenciais.
- - Erros humanos, como falhas de operação, preenchimento incorreto de dados ou má interpretação de requisitos.
- - Interrupções prolongadas do sistema, impactando diretamente o andamento e a entrega final do projeto.
- - Desalinhamento entre áreas envolvidas, podendo gerar retrabalhos e conflitos de prioridade.
- - Dependência de fornecedores externos para componentes críticos, o que pode gerar atrasos adicionais.

4. Identificação das Vulnerabilidades

As principais vulnerabilidades observadas durante a avaliação do projeto incluem:

- - Ausência de processos automáticos de backup e recuperação de dados.
- - Falta de atualização periódica de softwares, frameworks e bibliotecas utilizadas.
- - Controles de acesso insuficientes, permitindo possibilidade de acessos não autorizados.
- - Equipe ainda em fase de adaptação, gerando riscos de execução com baixa eficiência.
- - Documentação parcial e incompleta, dificultando a continuidade do projeto em caso de troca de equipe.
- - Ausência de monitoramento contínuo da infraestrutura e aplicações.
- - Dependência excessiva de determinados membros da equipe, criando pontos únicos de falha.
- - Processos de testes insuficientes, aumentando a probabilidade de erros em produção.

5. Identificação das Ameaças

As ameaças que podem comprometer a execução e o sucesso do projeto incluem:

- - Ataques cibernéticos: phishing, ransomware, malware ou exploração de vulnerabilidades.
- - Desastres naturais: enchentes, incêndios, tempestades ou outros eventos ambientais.
- - Sabotagem interna: mau uso proposital ou indevido de recursos por parte de colaboradores ou usuários.
- - Quedas de energia: falhas prolongadas na infraestrutura elétrica, afetando prazos e produtividade.
- - Roubo de equipamentos: perda de dispositivos contendo dados sensíveis do projeto.
- - Falhas de terceiros: interrupções em serviços de parceiros ou fornecedores críticos.
- - Mudanças regulatórias: alterações legais ou normativas que impactem a conformidade do sistema.
- - Oscilações econômicas: variação de custos de infraestrutura ou serviços contratados.

6. Conclusão e Recomendações

O levantamento realizado evidencia que o projeto está exposto a riscos técnicos, organizacionais e externos. Para reduzir a probabilidade e o impacto desses fatores, são recomendadas as seguintes ações:

- - Implantação de políticas de backup com mecanismos automáticos e testes periódicos de recuperação.
- - Reforço nos controles de acesso, incluindo autenticação multifator e segregação de perfis de usuário.
- - Atualização contínua de softwares e dependências críticas, com aplicação de patches de segurança.
- - Capacitação da equipe por meio de treinamentos regulares e disseminação de boas práticas.
- - Documentação completa e atualizada, assegurando rastreabilidade e suporte em mudanças de equipe.
- - Elaboração de planos de contingência para lidar com incidentes críticos, interrupções ou desastres naturais.
- - Monitoramento proativo da infraestrutura, sistemas e processos, permitindo resposta rápida a incidentes.
- - Definição de métricas e indicadores para acompanhamento do nível de exposição a riscos.