Plano de Gerenciamento de Riscos

Gerenciamento de Riscos

Um projeto, assim como a vida, é incerto.

Os riscos não devem ser simplesmente listados; eles devem ser identificados para que sejam previstos e se possível:

1. **Diminuídos**: caso sejam ameaças;
2. **Maximizados**: caso sejam oportunidades;
3. **Controlados**: quando houver poucas estratégias para o seu enfrentamento.

O risco controla os planos de iteração no processo de desenvolvimento de software, ou seja, as iterações são planejadas considerando riscos específicos na tentativa de agir sobre os riscos. A lista de riscos é revista periodicamente para avaliar a eficácia das estratégias de resposta a riscos e, consequentemente, orientar as revisões no plano de projeto e nos planos de iteração subsequentes.

> O segredo do gerenciamento de riscos não é esperar que o risco aconteça, e, torne-se um problema ou defeito, para decidir o que fazer em relação a ele.

Assim como, uma mudança de alguns graus no percurso de um voo internacional produz um efeito significativo no local de aterrissagem do avião; de modo semelhante, gerenciar o risco antecipadamente é quase sempre menos dispendioso e penoso do que tentar solucioná-lo depois que virar um fato.

Estratégias de Gerenciamento de Riscos

Para os **riscos negativos** ou **ameaças**, há três estratégias principais:

- **Prevenção de risco:** Reorganizar o projeto de modo que não seja afetado por um risco.
- **Transferência de risco:** Reorganizar o projeto de modo que alguém ou algo assuma o risco (o cliente, o fornecedor, o banco, um outro elemento etc.).

- **Aceitação de risco:** Decidir conviver com o risco como uma contingência. Monitore o sintoma do risco e escolha um plano de contingência que oriente sobre o procedimento a ser tomado em caso de risco.

No caso dos **riscos positivos** ou **oportunidades**, as opções de estratégias são as seguintes:

- **Exploração de risco**: eliminar a incerteza associada a um risco positivo, fazendo com que a oportunidade efetivamente aconteça.
- **Compartilhamento de risco**: atribuir parte da propriedade do risco a terceiros que possam capturar melhor a oportunidade em benefício do projeto.
- **Melhoramento do risco**: aumentar a exposição ao risco positivo, através do aumento da probabilidade e/ou do impacto caso ocorra. Isso se dá pela identificação e maximização dos acionadores dos riscos de impacto positivo.

Se decidir **aceitar** o risco, pode ser que você ainda deseja reduzi-lo, ou seja, tomar alguma ação imediata para reduzir seu impacto.

Tipos de Riscos

É importante fazer distinção entre riscos diretos e indiretos, então, em poucas palavras:

1. **Risco Direto**: é aquele que permite um certo grau de controle;
2. **Risco Indireto:** é o que não pode ser controlado.

Embora não se possa ignorar os riscos indiretos, sua consequência é pequena no sentido prático: como não é possível alterá-los, não perca tempo se preocupando com eles. O mundo *pode* acabar amanhã, mas também *pode não* acabar. Então, se não acabar, é melhor que o trabalho não pare!

Algumas vezes, um risco indireto pode realmente ser um risco direto disfarçado. Por exemplo, a dependência de um fornecedor externo em relação a um ou mais componentes. Isso parece ser um risco indireto, mas se forem desenvolvidos planos de contingência para esses componentes, será possível controlar o risco: fornecedores alternativos podem ser escolhidos ou a funcionalidade pode ser desenvolvida por conta própria. Em vários casos, temos mais controle do que imaginamos.

No caso dos riscos indiretos, você deve tentar obter algum tipo de controle sobre eles ou simplesmente reconhecê-los e continuar o trabalho. Não adianta se preocupar com uma situação que você não pode mudar.

1. Riscos de Recursos

1.1 Organização

- Há um compromisso suficiente neste projeto (incluindo gerenciamento, testadores, QA e outras partes externas, porém envolvidas)?
- Este é o maior projeto desta organização?
- Existe algum processo bem definido para a engenharia de software? Há captura e gerenciamento de requisitos?

1.2 Financeiro

- Os recursos financeiros estão disponíveis para a conclusão do projeto?
- Os recursos financeiros foram alocados para treinamento e acompanhamento de mentores?
- Existe alguma limitação em termos de orçamento, por exemplo, existe algum custo fixo estipulado para o sistema ou o sistema está sujeito a cancelamento?
- As estimativas de custo são precisas?

1.3 Pessoas

- Há pessoal suficiente disponível?
- Elas possuem capacidades e experiência apropriadas?
- Elas já trabalharam juntas antes?
- Elas acreditam no sucesso do projeto?
- Há representantes dos usuários disponíveis para as revisões?
- Há especialistas de domínio disponíveis?

1.4 Tempo

- O planejamento é realista?
- A funcionalidade pode ser gerenciada pelo escopo para cumprir as programações?
- Quando é a data de liberação?
- Há tempo para "*fazer isso corretamente*"?

2. Riscos do Negócio

- E se um concorrente conseguir obter primeiro a liderança no mercado?
- E se o orçamento para o projeto estiverem comprometidos (uma outra forma de fazer esta pergunta é "*O que pode garantir recursos financeiros adequados*")?
- O valor projetado para o sistema é maior que o custo projetado? (não se esqueça de considerar o valor temporal do dinheiro e o custo de capital).
- E se não puderem ser feitos contratos com os principais fornecedores?

3. Riscos de Escopo

- É possível medir o sucesso?
- Existe algum consenso sobre como medir o sucesso?
- Os requisitos são relativamente estáveis e foram bem compreendidos?
- O escopo do projeto é estável ou continua sendo expandido?
- As escalas de tempo de desenvolvimento do projeto são curtas e inflexíveis?

4. Riscos Tecnológicos

- A tecnologia foi aprovada?
- Os objetivos de reutilização são razoáveis?
    - Um produto de trabalho deve ser utilizado uma vez antes de poder ser reutilizado.
    - É possível que, somente após vários releases, um componente esteja estável o suficiente para ser reutilizado sem causar mudanças significativas.
- Os volumes de transações nos requisitos são razoáveis?
- As estimativas de taxa de transação merecem crédito? Elas são muito otimistas?

- Os volumes de dados são razoáveis? Os dados podem ser mantidos nos servidores disponíveis atualmente? Se os requisitos indicarem que uma máquina em específico ou um sistema de um departamento fará parte do projeto, os dados podem ser mantidos nesse local de forma razoável?
- Há requisitos técnicos diferentes ou desafiadores que exijam que a equipe de projeto resolva problemas com os quais não está familiarizada?
- O sucesso depende de produtos, serviços ou tecnologias novas ou não experimentadas, ou de hardware, software ou técnicas novas ou não aprovadas?
- Existem dependências externas das interfaces com outros sistemas, inclusive aqueles fora da corporação? As interfaces necessárias existem ou devem ser criadas?
- Há requisitos de disponibilidade e segurança extremamente inflexíveis, por exemplo: "o sistema nunca deve falhar"?
- Os usuários do sistema são inexperientes em relação ao tipo de sistema que está sendo desenvolvido?
- Há um risco crescente devido ao tamanho ou à complexidade do aplicativo ou à inovação da tecnologia?
- Existe algum requisito para suporte ao idioma nacional?
- É possível projetar, implementar e executar este sistema? Alguns sistemas são muito grandes ou complexos para funcionarem apropriadamente.

5. Riscos de Planejamento

A experiência mostra que 85% dos riscos causam um impacto direto ou indireto no planejamento e, portanto, causam implicitamente um impacto no custo. É possível que 5% causem apenas um impacto no custo. O restante não causa impacto direto no custo nem na programação, mas, na qualidade, por exemplo.

Se o prazo de entrega for considerado um empecilho, faça liberações gradativamente. Evite fazer uma liberação enorme na tentativa de cumprir a programação.

Alguns projetos têm prazos finais realmente "inalteráveis". O software para analisar ao vivo o resultado de uma eleição durante a noite, por exemplo, terá pouco valor se for lançado na semana seguinte à eleição. Ou o software pode tornar-se obsoleto em relação aos dos concorrentes: eles lançam um produto melhor que o seu, enquanto você ainda está no meio da construção. De repente, você não está mais no jogo e não pode fazer quase nada em relação a isso. Entretanto, normalmente poucos projetos têm um prazo de entrega tão crítico. Os atrasos na maioria das vezes afetam o custo. Em geral, faça com que o compromisso com a programação seja igual à melhor estimativa e considere alguma contingência razoável.

$$compromisso = estimativa + contingência$$

Algumas pessoas sugerem definir as expectativas de planejamento do mesmo modo que a estratégia de recuo, ou seja, baseá-las nos planos de contingência, porém isso é pessimista demais, pois *nem* todos os riscos irão realmente se concretizar.

Os riscos de programação são integrados a algumas ferramentas de estimativa e custo. Por exemplo, no modelo COCOMO (*Constructive Cost Model*), vários geradores de custo são fatores de risco reais, tais como:

- complexidade (cplx)
- restrições de tempo real (time)
- restrições de armazenamento (stor)
- experiência (Vexp)
- disponibilidade de ferramentas apropriadas (tool)
- pressão de programação (sced)

O objetivo do Plano de Gerenciamento de Risco é garantir que os riscos do projeto sejam devidamente identificados, analisados, documentados, mitigados, monitorados e controlados. Ele descreve a abordagem que será usada para identificar, analisar, priorizar, monitorar e mitigar riscos.

1. Sumário de Riscos

Considerando o mesmo sistema da atividade FURPS, escreva um texto com uma breve descrição do projeto e um resumo do risco total envolvido no projeto

O projeto é um sistema de gerenciamento com foco na precisão de dados e cálculos, incluindo juros e multas. Ele visa melhorar a performance na emissão de relatórios e cálculos fiscais. A equipe de desenvolvimento e teste trabalha em estreita colaboração com os usuários, personalizando o sistema para atender às necessidades de diferentes segmentos. Além disso, o sistema é integrado com sites do governo para transmissão de documentos.

No entanto, a empresa G-Tech Sistemas, que fornece um Sistema ERP, enfrenta riscos, como competição acirrada, desafios financeiros, mudanças nas preferências dos clientes e mudanças de leis. Esses riscos precisam ser gerenciados com acompanhamento contábil e jurídico para sempre estar atualizado com o mercado.

2. Tarefas de Gerenciamento de Riscos

Faça uma breve descrição das tarefas de gerenciamento de riscos a serem executadas durante o projeto. Nesta seção, você deve descrever o seguinte:

A. A abordagem a ser adotada para identificar riscos e como a lista de riscos será analisada e priorizada;

B. As estratégias de gerenciamento de riscos que serão usadas, incluindo estratégias de diminuição, anulação e/ou prevenção para os riscos mais significativos;

C. Como o status de cada risco significativo e as respectivas atividades de diminuição serão monitorados;

D. Cronogramas de revisão e relatório de riscos. Uma revisão dos riscos deve fazer parte da revisão de aceitação de cada iteração ou fase.

Identificação de Riscos: O primeiro passo é identificar os potenciais

problemas que podem afetar o sistema ERP, abrangendo desde falhas técnicas, como problemas de hardware e software, até riscos operacionais, como erros humanos, falta de treinamento adequado e interrupções nos processos de negócios.

Avaliação de Riscos: Em seguida, é necessário avaliar a probabilidade de ocorrência e o impacto de cada um desses riscos. Isso pode ser feito usando uma matriz de riscos para classificá-los como baixos, médios ou altos com base em sua gravidade e probabilidade.

Estratégias de Mitigação: Para cada risco identificado, é importante desenvolver estratégias de mitigação. Isso envolve a implementação de medidas como redundâncias de sistema, treinamento de pessoal, políticas de segurança de dados e procedimentos de backup.

Plano de Contingência: Deve-se elaborar um plano de contingência que descreva as ações a serem tomadas caso um risco se concretize. Isso inclui procedimentos para restaurar o sistema a partir de backups, ativar equipes de resposta a incidentes e adotar medidas corretivas específicas.

Monitoramento Contínuo: É essencial estabelecer um sistema de monitoramento constante para o sistema ERP. Isso pode envolver a configuração de alertas para atividades suspeitas, auditorias regulares e avaliação constante da segurança do sistema.

Auditorias de Segurança: Para identificar vulnerabilidades no sistema ERP, é importante realizar auditorias regulares de segurança. Isso inclui avaliações de penetração, verificações de conformidade com padrões de segurança e revisões das políticas de segurança.

Backup e Recuperação de Dados: Procedimentos robustos de backup e

recuperação de dados são fundamentais para garantir a disponibilidade e a integridade dos dados do sistema ERP em caso de falhas ou desastres.

Treinamento e Conscientização: Certificar-se de que os usuários e a equipe de TI estejam devidamente treinados e conscientes dos riscos é crucial. Isso pode incluir treinamento em segurança cibernética e boas práticas de uso do sistema.

Gerenciamento de Acesso: Implementar controles rigorosos de acesso ao sistema ERP é vital para garantir que apenas pessoas autorizadas tenham acesso a informações e funcionalidades críticas.

Revisão Periódica da Estratégia de Risco: Deve-se revisar regularmente a estratégia de gerenciamento de riscos à medida que novos riscos surgem ou as circunstâncias mudam na organização.

Comunicação de Incidentes: Estabelecer um protocolo claro para relatar e comunicar incidentes de segurança ou problemas no sistema ERP é essencial para garantir que as partes interessadas sejam informadas prontamente.

Seguro contra Riscos: Considerar a aquisição de um seguro contra riscos cibernéticos ou de sistema é uma opção para mitigar os custos associados à recuperação após incidentes graves.

3. Orçamento

Especifique em reais o orçamento disponível para o gerenciamento dos riscos do projeto

O valor do orçamento disponível para o gerenciamento será de 5% do valor, R$100.000,000

4. Itens de Risco a Serem Gerenciados

Crie uma lista dos itens de risco que foram identificados; uma das melhores práticas do setor é publicar e manter visível uma lista dos 10 principais riscos que são considerados significativos o bastante para o projeto empregar recursos para o seu gerenciamento. Você poderá manter uma lista maior se assim for exigido pela prática organizacional ou pelo contrato.

1. Complexidade do sistema (funcionalidades, implementação, desenvolvimento, manutenção, etc)
2. Sobrecarga de dados
3. Falta de documentação adequada
4. Falta de recursos técnicos/financeiros
5. Requisitos mal definidos
6. Adaptação dos usuários
7. Segurança dos dados
8. Custos inesperados/adicionais
9. Gerenciamento de mudanças
10. Competição no mercado