

Exercício: Plano de Gerenciamento de Riscos

Gerenciamento de Riscos

Nome: **Markcell Schwenck Rodrigues**

RA: **321112119**

Nome: Abraão Vieira Oliveira Paiva

RA: 320253456

Nome: **Guilherme de Almeida Ventura**

RA: **321122689**

Nome: Kaik Nonato Pena

RA: 321140239

Nome: **Herik Henrique da Silva Santos**

RA: **32018258**

Nome: Matheus César Amaral Silva

RA: 321111658

- Após terminar a atividade:
 - Adicione esse arquivo no formato PDF no repositório;
 - Cada integrante do grupo, poste o arquivo PDF no ulife.

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.

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.

$$\text{compromisso} = \text{estimativa} + \text{contingência}$$

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, faça uma breve descrição do projeto e um resumo do risco total envolvido no projeto.

O principal foco do sistema é o registro da jornada de trabalho do usuário e o gerenciamento da mesma, e por este motivo, é de suma importância a segurança na armazenagem destas informações.

O Software deve conter um sistema robusto de realização de login, pois com as credenciais do usuário, o mesmo terá acesso a todas as funcionalidades para ele propostas referente ao sistema.

O Software deve ter uma infraestrutura também bem encorpada, para suportar o acesso simultâneo de diferentes usuários, um código bem otimizado, para não ocorrer falhas e bugs durante o processamento das informações e emissão dos relatórios, e também sem aberturas, para que as informações dos usuários não possam ser acessadas externamente por pessoas maliciosas.

O Software deve ser intuitivo para o usuário, pois os dados ali gerenciados e emitidos serão também utilizados como documentação oficial para determinadas atividades na vida do funcionário, e por esse motivo deve ser estruturado de tal forma a evitar o máximo possível erros por dúvidas do usuário.

A otimização do sistema também deve ser bem polida, para que possa ser acessada a partir de diferentes sistemas operacionais e navegadores, fazendo com que funcione corretamente e sem falhas em todos os sistemas propostos.

Como é um sistema utilizado continuamente pelos usuários, e também de forma constante pela corporação contratante, a infraestrutura do sistema, como o banco de dados, servidores, domínios e multiplataformas do sistema, devem ser constantemente monitoradas para evitar problemas estruturais e de processamento do Software.

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.

A- Uma forma é identificar os riscos planejando de modo que o projeto não seja afetado. Aceitando os riscos, decidindo conviver com o risco como uma contingência. Monitorando o sintoma do risco e escolhendo um plano de contingência que oriente sobre o procedimento a ser tomado caso esse risco aconteça. É de extrema importância identificar os riscos que podem impedir que o sistema funcione. É recomendado a abordagem top-down, começando de cima para baixo após listar todos os riscos e dar devida importância para tal.

A listagem deve ser sempre feita de macro para micro.

B- Realizar revisão do código a fim de prevenir possíveis bugs;

Realizar e documentar casos de testes com o intuito de ter registro do que estava funcionando em cada versão do software;

Fazer uso de nobreak a fim de evitar perda de dados em caso de queda de energia nas máquinas dos colaboradores;

Utilizar as normas da ISO 27001 como guia para o tratamento de riscos;

Terceirizar o processo de segurança da informação com empresas especializadas no ramo;

C- Após ter feito uma listagem dos riscos, é necessário dar um status para o mesmo. Riscos que devem ter uma maior importância são aqueles que impedem o funcionamento do registro de jornada dos funcionários. Logo, é preciso definir o tratamento que será implementado para diminuir o impacto gerado pelo risco e detalhar ao máximo a forma, o prazo e os responsáveis pelas medidas de tratamento.

O monitoramento é importante pois nele iremos validar se tudo está saindo de acordo com o planejamento.

D - Realizar periodicamente um relatório contendo os casos de testes da versão atual do sistema (fazer o relatório sempre antes de entregar uma nova versão) ;

3. Orçamento

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

Visto que o sistema funcionará hospedado em um site, o mesmo terá gastos contínuos para evitar riscos estruturais:

R\$40,00

Gastos com consultoria de segurança:
R\$ 22.000,00

Gastos com desenvolvimento:
R\$ 30.000,00

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.

Escreva sua resposta aqui

1. Segurança de acesso ao sistema de ponto;
2. Determinação e padronização de ferramentas para o desenvolvimento do sistema.
3. Má elaboração UX/UI;
4. Baixo orçamento para o desenvolvimento do projeto.
5. Erros de lógica em funções e funcionalidades do sistema;
6. Canal de comunicação ativo entre os departamentos para estabelecer processos e critérios para aquisição de sistemas.
7. Compatibilidade de Hardware e Software.
8. Confidencialidade.
9. Robustez do sistema.
10. Disponibilidade do sistema.