

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: Lucas Tadeu Gonçalves Lodi

RA: 320246039

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

Nesta atividade iremos detalhar a lista dos 10 principais riscos identificados na atividade do Plano de Gerenciamento de Risco. Então, para cada risco você deverá especificar:

1. **Importância ou Ordenação do Risco:** um indicador da importância do risco para ajudar a ordenar os riscos, desde os riscos que são mais perigosos para o projeto aos que têm menor relevância;
2. **Descrição:** uma breve descrição do risco;
3. **Impactos:** liste os impactos no projeto ou produto;
4. **Indicadores:** descreva como monitorar e detectar que o risco ocorreu ou está prestes a ocorrer. Por exemplo, através de métricas e limites, resultados de teste, eventos específicos etc;

5. **Estratégias de Diminuição (Mitigação):** descreva o que está sendo feito no projeto, no momento, para reduzir o impacto do risco;
6. **Plano de Contingência:** descreva que ação será executada se o risco realmente se materializar: solução alternativa, redução da funcionalidade etc.

Exemplo: Sistema de Paginação de Esportes Universitários

Esse sistema permite que os assinantes sejam notificados sobre eventos esportivos universitários ou sobre as equipes (times) às quais se inscreveram para receber as suas últimas atualizações.

Risco Técnico: Capacidade e Recurso

- **Descrição:** As áreas de risco incluem a incapacidade de fornecer uma solução que atenda aos requisitos de capacidade ou de emitir uma página para um dispositivo de paginação. Embora exista uma tecnologia que forneça tal recurso, a capacidade de enviar até 500.000 páginas em 5 minutos precisará ser comprovada.
- **Impactos:** Sistema não funcional, provavelmente resultante da perda dos usuários assinantes.
- **Indicadores:** Entrega de mensagens com falha ou atraso dentro do período de tempo estabelecido de 5 minutos.
- **Estratégia de Mitigação:** A equipe de desenvolvimento implementou uma funcionalidade de paginação semelhante para outros projetos; portanto, essa área de risco técnico é relativamente baixa. A equipe deve fornecer uma estimativa de tempo necessária para processar e enviar informações aos assinantes com base nas cargas de trabalho projetadas médias e máximas, que atualmente são de 200.000 a 500.000 assinantes. Os desenvolvedores implementarão um sistema escalável, no entanto, será necessário fornecer recursos de hardware necessários para atender aos requisitos de processamento. Pois, a equipe de desenvolvimento não pode garantir a capacidade de cada serviço de gateway de paginação de fornecer os níveis de serviço dentro das especificações desejadas.

- **Plano de Contingência:** A tentativa de localizar um serviço que pode, no momento de processamento de pico, aceitar e enviar até 500.000 pedidos de página.

Risco de Planejamento: Implantação Atrasada do Sistema Ultrapassando Março de 2020

- **Gravidade do Risco:** Danos Maiores
- **Descrição:** A não implantação por parte da WebNewsOnline de seu sistema dentro do planejamento estabelecido é considerada pelo gerenciamento uma falha e pode resultar no cancelamento do projeto.
- **Impactos:** O projeto será cancelado.
- **Indicadores:** Falha ao implantar antes de março de 2020.
- **Estratégia de Mitigação:** A linha de tempo do projeto deve ser cuidadosamente calculada e, se for limitada pelo tempo, o planejamento distribuível deve conduzir à redução do escopo ou da escala, como um exemplo: a WebNewsOnLine pode optar por não implementar alguma funcionalidade definida na primeira liberação para atingir a data de entrega.
- **Plano de Contingência:** Nenhum.

Risco Técnico: Interoperabilidade com a Plataforma Existente

- **Gravidade do Risco:** Baixa
- **Descrição:** O Web site existente do WebNews Online é baseado em IIS; será necessário fornecer um meio de capturar imediatamente cada artigo recém-publicado e transferi-lo para o sistema para análise e avaliação dos assinantes.
- **Impactos:** A quantidade de codificação que fornece as interfaces deve aumentar.

- **Indicadores:** Nenhum
- **Estratégia de Mitigação:** A equipe de desenvolvimento precisará trabalhar com a equipe técnica para determinar o nível de integração que está disponível com o sistema existente de edição de conteúdo.
- **Plano de Contingência:** Desenvolva um processo baseado em Windows que detecte os documentos residentes no IIS recém-publicados e os transfira para o servidor.

1. Lista de Riscos

Segurança de acesso ao sistema de ponto;

Importância ou Ordenação do Risco: Alto

Descrição: O sistema deve garantir a confidencialidade dos dados e os mesmos só podem ser acessados por usuários credenciados, garantindo assim a confiança e integridade dos dados contidos no sistema.

Impactos: O acesso ao sistema por usuários não credenciados pode acarretar em vazamentos e alterações indevidas dos dados

Indicadores: O acesso ao sistema por parte do usuário ou administrador deve sempre ser autenticado através do login feito com seu usuário/senha e após o login o usuário receberá uma notificação de acesso, para que o mesmo seja confirmado.

Estratégia de Mitigação: Se for notada alguma atividade suspeita no ato de acesso, será solicitado ao usuário a autenticação de dois fatores, onde o usuário deverá inserir o código enviado por email ou SMS.

Plano de Contingência: Caso ocorra o acesso indevido ao sistema, o administrador será notificado e deverá isolar o servidor invadido para que outros servidores não sejam prejudicados, logo após o administrador deverá assegurar a integridade do backup garantindo a reposição dos dados perdidos ou corrompidos.

Determinação e padronização de ferramentas para o desenvolvimento do sistema.

Importância ou Ordenação do Risco: Média

Descrição: O risco da não padronização do desenvolvimento de um sistema inclui o sistema não sair como planejado.

Impactos: A entrega do sistema não está de acordo com o que o cliente deseja, atraso no desenvolvimento e custos não esperados.

Indicadores: Durante o processo de desenvolvimento o projeto não está saindo como planejado.

Estratégia de Mitigação: Traçar estratégias claras e bem definidas, monitorar as atividades que estão sendo desenvolvidas.

Plano de Contingência: Adotar metodologias já existentes para a padronização do projeto e investir na capacitação dos colaboradores.

Má elaboração UX/UI;

Importância ou Ordenação do Risco: Baixo

Descrição: Interação do cliente com o produto ou serviço a partir de elementos disponibilizados, oferecendo conteúdo relevante ao usuário/cliente para que o mesmo possa utilizá-lo.

Impactos: Uma experiência negativa com UX/UI pode levar ao usuário/cliente a desistência de utilização do produto/serviço. Um sistema não intuitivo também pode impossibilitar que o usuário realize suas tarefas dentro do próprio sistema.

Indicadores: Feedbacks da equipe de testes do sistema e reportes dos próprios usuários sobre a utilização da plataforma.

Estratégia de Mitigação: Contratação de um especialista em UX/UI para o desenvolvimento de uma plataforma mais intuitiva e agradável ao usuário. Disponibilidade de um campo de sugestões dentro da própria plataforma, no intuito de receber feedback e sugestões dos próprios usuários, no intuito de melhorar a experiência dos mesmos.

Plano de Contingência: Tratativa dos reportes dos usuários e da equipe de teste, trabalhando para que os problemas informados possam ser tratados pela equipe de desenvolvimento e pelo especialista UX/UI.

Baixo orçamento para o desenvolvimento do projeto.

Importância ou Ordenação do Risco: Médio

Descrição: O Risco de Baixo orçamento ocorre quando os custos e o escopo do projeto não são definidos com precisão.

Impactos: O cronograma mal estabelecido do projeto pode causar um grande impacto e possível cancelamento do projeto.

Indicadores: Desvio de Custo, Índice de produtividade, Desvio de esforço e Desvio de Prazo.

Estratégia de Mitigação: A verificação dos fornecedores pode contribuir muito para estabelecer um orçamento mais realista que possa ser cumprido, mesmo que haja circunstâncias imprevistas que afetem os custos.

Plano de Contingência: Criação ou aquisição de um Banco de Dados (Servidor) que atenda a parte orçamentária do projeto, que consiga atender a demanda reduzindo os gastos.

Erros de lógica em funções e funcionalidades do sistema;

Importância ou Ordenação do Risco: Alto

Descrição: Erros de lógica podem levar o REP a uma inconsistência ou até mesmo a indisponibilidade do mesmo.

Impactos: Em caso de indisponibilidade do sistema pode impossibilitar o funcionário de realizar o registro de sua jornada de trabalho, impossibilitar o fechamento do banco de horas e consequentemente gerar enganos sobre horas trabalhadas durante o mês do colaborador e falhas/erros ao utilizar as funcionalidades do sistema.

Indicadores: Relato dos usuários que utilizam o sistema.

Estratégia de Mitigação: Ter uma equipe profissional em testes de sistema.

Plano de Contingência: Correção do erro de lógica diretamente no código.

Canal de comunicação ativo entre os departamentos para estabelecer processos e critérios para aquisição de sistemas.

Importância ou Ordenação do Risco: Médio

Descrição: A comunicação entre departamentos, os procedimentos e os processos organizacionais, são de extrema importância para que a aquisição dos sistemas seja assertiva junto aos processos e critérios estabelecidos, como as tecnologias disponibilizadas, as normas para qualidade e de segurança da informação, além dos procedimentos específicos para lidar com os dados financeiros.

Impactos: A falha na transmissão das informações pode induzir a equipe a cometer diversos erros e, conseqüentemente, levar uma boa proposta ao fracasso.

Indicadores: Problemas no momento da utilização da ferramenta por falta de comunicação entre os setores envolvidos no sistema.

Estratégia de Mitigação: O plano do canal de comunicação ativo entre os departamentos do projetos terá a função identificar quais são as necessidades comunicativas dos interessados e definir a maneira mais apropriada para que a sua distribuição e orientação ocorra. Esses requisitos precisam ser documentados e trabalhados corretamente com os seus colaboradores.

Plano de Contingência: Serão elaborados processos para melhoria da comunicação junto a tecnologias utilizadas para armazenar e recuperar as informações corporativas em caso de perda de dados.

Compatibilidade de Hardware e Software.

Importância ou Ordenação do Risco: Baixo

Descrição: A incompatibilidade de hardware e software atinge o usuário em sua rotina diária de registro de ponto, pois se o browser e ou, aparelho utilizados não for compatível com o sistema, o usuário não terá acesso à plataforma, através desse erro o usuário não consegue acessar o sistema pois a máquina ou o S.O. não o suportará.

Impactos: O usuário terá acesso ao sistema, mas o mesmo não funcionará corretamente, apresentará bugs de funcionamento e problemas no layout durante o uso.

Indicadores: a fase de portabilidade do sistema em multiplataformas, na qual apresentará erros de incompatibilidade ou o sistema não funcionará corretamente. Outra forma de detectar incompatibilidades do sistema será com reports e feedback da equipe de testes e dos próprios usuários do sistema.

Estratégia de Mitigação: Indicar ao usuário qual sistema operacional será adequado para que o sistema funcione corretamente.

Plano de Contingência: Caso ocorra, o sistema mostrará um pop-up ou mensagem de alerta orientando o usuário qual o tipo de incompatibilidade se encontra, e o que ele deverá fazer para que o sistema funcione adequadamente.

Confidencialidade.

Importância ou Ordenação do Risco: Alto

Descrição: O risco de confidencialidade inclui a privacidade dos dados dos colaboradores da organização, tais como dados pessoais e dados das jornadas de trabalho.

Impactos: Vazamento de dados.

Indicadores: Através do monitoramento dos acessos ao banco de dados.

Estratégias de Diminuição (Mitigação): A equipe responsável pela segurança do sistema deve utilizar uma senha segura para acesso ao banco de dados contendo letras com números e também caracteres especiais (como !@#\$+), evitar utilização da mesma senha em outros locais, monitorar atividades suspeitas e investir em ferramentas de prevenção contra ameaças, como firewall e antivírus.

Plano de Contingência: Investigar a fonte do vazamento dos dados e fazer uma comunicação efetiva às partes afetadas no vazamento.

Robustez do sistema.

Importância ou Ordenação do Risco: Médio

Descrição: O sistema deve manter as suas funcionalidades mesmo se submetido a alguma situação adversa.

Impactos: Queda ou mal funcionamento do sistema.

Indicadores: Se o sistema começar a apresentar lentidão no acesso, falha ou lentidão no registro dos dados e lentidão nas consultas em momentos de muitos acessos simultâneos isso indicará pouca robustez do sistema.

Estratégia de Mitigação: Sempre que o sistema atingir 80% dos acessos simultâneos ele emitirá um aviso, para que assim a capacidade de acessos seja aumentada conforme o número de usuários do sistema aumenta.

Plano de Contingência: Caso ocorra alguma anormalidade que implique na falha do sistema por pouca robustez, todos os acessos deverão ser finalizados pelo administrador e posteriormente o mesmo deverá aumentar a robustez do sistema.

Disponibilidade do sistema.

Descrição: A disponibilidade do sistema é um dos riscos mais importantes, trata-se da disponibilidade de acesso dos usuários e do tratamento dos dados internos dentro do software.

Importância ou Ordenação do Risco: Alto

Impactos: Caso o Software esteja indisponível, todos os usuários não conseguirão registrar sua jornada de trabalho, nem tratar os dados já registrados. Este problema pode ocasionar em retrabalho dos usuários do sistemas, visto que a jornada é computada a partir da hora da marcação, caso não consiga registrar o ponto no horário ideal, será necessário o ajuste manual do mesmo posteriormente.

Indicadores: A indisponibilidade do sistema pode ser detectada a partir de oscilações e lentidão pontuais do sistema (internamente). Caso o sistema não esteja suportando o tratamento de dados interno, o mesmo apresentará lentidão antes de estar indisponível. Além deste ponto, só será possível tratar o caso depois que o sistema já estiver indisponível.

Estratégia de Diminuição (Mitigação): Para redução dos riscos, é necessário a revisão contínua do código, no intuito de otimizar o processamento das tarefas do sistema (busca do código limpo). É também, de suma importância, o monitoramento constante do sistema, para detectar as oscilações previamente e evitar a indisponibilidade do mesmo.

Plano de Contingência: O foco principal é tornar o sistema novamente disponível, por este motivo, no momento da indisponibilidade do sistema, a primeira ação é direcioná-lo para um servidor backup, caso o problema não seja solucionado, retornar o sistema para a versão anterior utilizada. Em seguida, verificar os logs do sistema no intuito de identificar a causa raiz do problema e trabalhar para que o mesmo não ocorra novamente.