Exercício: Plano de Gerenciamento de Riscos

Gerenciamento de Riscos

Nome:	**Rodrigo Ottávio de Souza jordan**	**Nome:**	Lucas Santos de Jesus
RA:	**320124070**	**RA:**	320137646
Nome:	**Luiz Henrique Araujo**	**Nome:**	Adriano Junior Melo
RA:	**320135576**	**RA:**	320112085
Nome:	**Clayton Henrique Magalhaes**	**Nome:**	João Victor Calegário de Souza
RA:	**320135265**	**RA:**	**321219711**

Nome: João Pedro dos Santos Otero

RA: 320137042

- 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

Risco técnico: Vazamento de dados

- Gravidade do Risco: Gravíssima
- Descrição: O Telegram tem dados pessoais de seus usuários desde o momento do cadastro até o uso do aplicativo como mensagens, arquivos de mídia(fotos, vídeos) e até mesmo links. Por isso teria que ter uma segurança para não houver nenhum tipo de vazamento de dados.

- Impactos: Dados de usuários como CPF, número de Telefone e fotos podem ser usadas por outros usuários de maneira indevida e ficarem expostas publicamente.
- Indicadores: Usuários podem detectar se houve vazamento de dados através de recursos como Firefox Monitor, observando se seus dados foram utilizados em ocasiões não gerenciadas pelo usuário.
- Estratégia de (Mitigação): Desenvolvedores e os QA(Controle de Qualidade) fazem testes diariamente em busca de aberturas na segurança do software para aperfeiçoar a criptografia.
- Plano de Contingência: Encerramento do aplicativo.

Risco de Planejamento: Sobrecarga no servidor

- Gravidade do risco: Baixa
- Descrição: O telegram possui servidores para que as pessoas possam se conectar e utilizar o chat para comunicação e compartilhamento de dados.
- Impacto: O sistema pode ficar lento ou parar de funcionar devido ao alto número de usuários e dados trafegando simultaneamente.
- Indicadores: Perda de conexões, server crash, alto tempo de respostas.
- Estratégias de Diminuição (Mitigação): Implementar um descarte de solicitações que ultrapassem o tempo limite de resposta.
- Plano de contingência: Abertura de mais servidores com limite de usuários reduzidos.

Risco Tecnológico: Erro de Criptografia

- Gravidade do risco: Gravíssima.
- Descrição: Uma falha de criptografia do Telegram pode deixar os dados do usuário vulneráveis para acessos indevidos.
- Impacto: Violação de privacidade dos usuários.
- Indicadores: Problemas de reconhecimento de dados, avisos de erros ao iniciar o aplicativo.
- Estratégias de Diminuição (Mitigação): Remover o tráfego malicioso antes de fazer a descriptografia, e utilizar recursos mais avançados para esse processo, planejamento da capacidade total do tráfego de rede criptografado.
- Plano de contingência: Desativar o sistema até que a solução para a configuração da criptografia seja implementada.

Risco pessoas: Erro de Sintaxe (HW/SW)

- Gravidade do risco: médio

- Descrição: Erro Semântico(HW) é um erro na lógica de seu código digo", em sua semântica, o código está sintaticamente correto, porém não faz o que se esperava dele. Por isso, este tipo de erro é geralmente mais difícil de ser identificado e corrigido.

  Erros de sintaxe (SW) ocorrem quando a IDE está traduzindo o código fonte do seu programa em código executável. Eles usualmente indicam que você escreveu algo sintaticamente errado no seu programa.
- Impacto: Software poderá não funcionar em aparelhos mais antigos.
- Indicadores: Verificar se em determinado modelo de aparelho ocorre travamento durante uso do software ou até mesmo uma temperatura mais elevada que o normal durante o uso do aplicativo.
- Estratégias de Diminuição (Mitigação): Otimização em seu código-fonte para ter um melhor funcionamento em aparelhos mais legados.
- Plano de contingência: Encerramento do aplicativo para aparelhos com hardware desatualizado.

Risco: Erro de processamento

- Gravidade:
- Descrição: É qualquer imperfeição ou inconsistência no produto do software ou em seu processo, um defeito é também uma não conformidade.
- Impactos: Problemas no processamento podem causar riscos à saúde fo software de uma empresa, mas não apenas isso há o desgaste dos usuarios e também pode criar uma crise de credibilidade perante o mercado.
- Indicadores: Produtividade, eficiência, eficácia, efetividade, qualidade, entre outros substantivos, não estão satisfazendo os usuários do software.
- Estratégias de Diminuição (Mitigação): A gestão organizacional é um fator importante no desenvolvimento de qualquer processo, e uma forma de alcançá-la é com uma lista de tarefas. Porém, não pode ser uma composição aleatória, sem uma linha de raciocínio, pois, caso contrário, essa elaboração será uma perda de tempo por si só.
- Plano de contingência: Retornar para a versão anterior onde não ocorre esse erro.

Risco Tecnológico: Ataque DDOS(Ataque hacker)

- Gravidade do risco: Gravissimo
- Descrição: Ataque DDOS: Esse tipo de ataque sobrecarrega os limites de capacidade específicos de uma rede, como a infraestrutura que suporta o site de uma empresa. O ataque DDoS envia várias solicitações para o site

Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto.

- Impactos: Sobrecarga de servidores;
- Indicadores: Um ataque do tipo DDoS é um ataque malicioso que tem como objetivo sobrecarregar um servidor ou um computador, esgotar seus recursos como memória e processamento e fazê-lo ficar indisponível para acesso de qualquer usuário a internet.
- Estratégias de Diminuição (Mitigação): Refere ao processo de proteger o alvo de Ataques de negação de serviço distribuído. Ataques DDoS estão evoluindo constantemente como é da natureza da tecnologia, e também, a motivação dos atacantes também está mudando.
- Plano de contingência: Melhorar a infraestrutura do servidor.

Risco técnico: Roubo de dados(Phishing)

- Gravidade: Gravissíma
- Descrição: Trata-se de um vazamento/roubo de dados do sistema, seja por pessoas internas ou externas.
- Impactos: Este tipo de problema causa instabilidade na confiabilidade do usuário em relação ao sistema, podendo ocasionar uma perda massiva de clientes do sistema, gerando fragilidade no “Nome” da corporação e por fim suceder a perca progressiva de arrecadação monetária.
- Indicadores: Uma das formas precaver esse vazamento de dados, é utilizar a autenticação de dois fatores, sendo eles: A tentativa de entrada em um dispositivo e a autorização em outro dispositivo previamente cadastrado.
- Estratégias de Diminuição (Mitigação): Realizar backups periódicos (save in the cloud), ajuda a mitigar a perda das conversas, arquivos e mídias em geral.
- Plano de contingência: Oferecer uma uma recompensa em troca dos dados vazados

Risco de planejamento: Estrutura ruim para hardware e equipamentos

- Gravidade: Grave
- Descrição: A não implantação de recursos capazes, para a melhor eficiência dos equipamentos, ocasiona a incapacidade do sistema atuar em seu máximo desempenho.
- Impactos: Podem ocorrer lentidões e congelamento do sistema.
- Indicadores: Falha de funcionamento das estruturas.
- Estratégias de Diminuição (Mitigação): Compra e manutenção das estruturas que sustentam o hardware.
- Plano de contingência: Compra e renovação total de toda a estrutura utilizada

Risco de planejamento: Incompatibilidade de sistemas

- Gravidade: Gravíssima
- Descrição: Não funcionamento do sistema no dispositivo do usuário.
- Impactos: Esse tipo de erro, pode ocasionar atraso na entrega do projeto, e possivelmente, perca de todo o trabalho realizado na construção do sistema.
- Indicadores: Sistema não abre no dispositivo.
- Estratégias de Diminuição (Mitigação): Testes em todos os tipos de sistema, podem evitar esse tipo de erro.
- Plano de contingência: congelamento do sistema até que o problema de incompatibilidade seja resolvido

Risco técnico: Perda de backups de dados

- Gravidade: Gravíssima
- Descrição: O risco consiste em uma perca de backups de informações que a empresa mantém em seu banco de dados.
- Impactos: Paralização das atividades corporação, causando retrabalhos e desperdício de recursos e prejuízo pela perca de dados de valor inestimado.
- Indicadores: O desaparecimento dos backups na nuvem/provedor da corporação.
- Estratégias de Diminuição (Mitigação): O recurso mais utilizado é o salvamento dos backups em vários locais diferentes, desta maneira, pode-se evitar a perca de todos os dados.
- Plano de contingência: Cadastramento de novos dados, desta vez, com mais locais para armazenamento dos backups