Exercício: Plano de Gerenciamento de Riscos

Gerenciamento de Riscos

Nome:	**Larissa Rayane Braga da Paz**	**Nome:**	**Gabriel Jorge Benevides**
RA:	**321115521**	**RA:**	**321222943**
Nome:	**Vinícius Meireles Oliveira**	**Nome:**	**Dayane Fonseca**
RA:	**320131605**	**RA:**	**321122433**
Nome:	**Vítor Ian dos Santos Gonçalves**	**Nome:**	**Ivan Kabuto**
RA:	**321140627**	**RA:**	**320136231**

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

7. 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 pro

8. **Indicadores:** descreva como monitorar e detectar que o risco ocorreu ou está prestes a ocorrer. jetadas 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.

Lista de Riscos

1- Risco de Planejamento | Risco de tempo.

- **Gravidade do Risco:** Média.
- **Descrição:** A ToolsNet não desenvolve sob demanda para empresas o que gera mais flexibilidade no prazos estabelecidos.
- **Impactos:** Acúmulo de demandas.
- **Indicadores:** Tarefas acumuladas no kanban, aumento na fila de revisão de código.
- **Estratégia de Mitigação:** Ajustar os prazos de acordo com as tarefas repassadas e realizar o acompanhamento das demandas
- **Plano de Contingência:** Aumento no número de desenvolvedores.

2 - Risco Técnico | Risco de vírus.

- **Gravidade do Risco:** Grave
- **Descrição:** Em termos mais técnicos, um vírus de site é um tipo de programa ou código malicioso criado para alterar a forma como um computador funciona e desenvolvido para se propagar de um computador para outro.
- **Impactos:** Um site infectado por vírus é um sério problema. Além de prejudicar o seu posicionamento no Google, o vírus pode solicitar informações dos seus dados e isso se torna algo mais grave. Dependendo do vírus o mesmo pode prejudicar seu computador
- **Indicadores:** Autoconsumo de processamento, Autoconsumo de memória
- **Estratégia de Mitigação:** Mantenha o seu site atualizado, Proteja contra ataques XSS(Os ataques de script entre sites (XSS) injetam JavaScript mal-intencionado em suas páginas, que são executadas nos navegadores de seus usuários e podem alterar o conteúdo da página ou roubar informações para serem enviadas de volta ao invasor), Observar as

mensagens de erro, Evite uploads de arquivos, Usar HTTPS, Obtenha ferramentas de segurança para sites

- **Plano de Contingência:** Tirar portal do ar, rastrear o arquivo malicioso, realizar a limpeza do arquivo na rede.

3 - Risco Técnico | Risco de ataques de ransomware.

- **Gravidade do Risco:** Grave
- **Descrição:** Ransomware é um malware projetado para acessar um computador/sistema para pegar dados importantes de uma empresa e realizar a criptografia ou bloquear o acesso do colaborador, impedido de utilizar esses dados o que leva a corporação a pagar pelo o resgate.
- **Impactos:** Disseminar para os usuários da plataforma.
- **Indicadores:** Criptografia de dados, alto consumo de processamento.
- **Estratégia de Mitigação:** Realização de verificação de vulnerabilidade recorrente, Backup de dados.
- **Plano de Contingência:** Tirar portal do ar, rastrear o arquivo malicioso, realizar a limpeza do arquivo na rede.

4 - Risco de Planejamento | Risco de funcionários não especializados/ erros humanos.

- **Gravidade do Risco:** Médio
- **Descrição:** Erros humanos e simples podem gerar não conformidades na plataforma.
- **Impactos:** Queda da plataforma, ferramentas não funcionando corretamente.
- **Indicadores:** Cálculos e ferramentas executados de maneira errada.

- **Estratégia de Mitigação:** Revisão de código pela equipe sênior, versionamento dos arquivos e ambiente de homologação.
- **Plano de Contingência:** Voltar a versão no sistema de produção.

5 - Risco Técnico | Risco de Phishing.

- **Gravidade do Risco:** Médio.
- Descrição: O phishing consiste em clonar uma página web para obter dados de forma maliciosa dos usuários, a ToolsNet não solicita e nem armazena nenhum dados dos seus usuários.
- **Impactos:** Processos direcionados de forma equivocada para empresa.
- **Indicadores:** Reclamações dos usuários.
- **Estratégia de Mitigação:** Deixar claro na plataforma que nenhum dado será coletado ou solicitado ao usuário, deixar disponível um canal de comunicação direto com a equipe para eventuais denúncias.
- **Plano de Contingência:** Acionar a justiça.

6 - Risco Técnico | Risco de DDOS.

- **Gravidade do Risco:** Grave
- **Descrição:** DDOS tem como objetivo tornar um serviço, servidor ou infraestrutura instáveis ou indisponível, através de uma sobrecarga de tráfego impedindo o real usuário acessar o site.
- **Impactos:** Site fora do ar, perda de valor monetário.
- **Indicadores**: Lentidão, site inacessível, alto tráfego de rede.
- **Estratégia de Mitigação:** Verificações de vulnerabilidade em dia, software de segurança atualizado, serviço Anti-DDOS ativos, ter uma conexão reserva.

- Plano de Contingência: verificar o Anti-DDOS que detecta o que é um tráfego legítimo do ilícito na rede.

7 - Risco de Planejamento |Risco de vulnerabilidade .

- **Gravidade do Risco:** Grave
- **Descrição:** Consiste em não adotar as medidas de segurança necessárias para manter o servidor seguro contra ataques.
- **Impactos:** Disseminação de arquivos maliciosos e queda da plataforma.
- **Indicadores:** Alto índice de infecções ocorrendo e curtos períodos de tempo.
- **Estratégia de Mitigação:** Usar sempre firewalls de qualidade, sempre adotar boas práticas de segurança ao realizar a codificação.
- **Plano de Contingência:** Contratar especialistas na área de segurança da informação para realizar consultoria.

8 - Risco de Planejamento | Risco do servidor não suportar a quantidade de acessos.

- **Gravidade do Risco:** Grave
- **Descrição:** Ocorre quando diversos usuários tentam se conectar ao mesmo tempo no mesmo site. O que geralmente acontece é que há um alto número de requisições e o site (ou aplicação) acaba não suportando. Ela não está preparada para essa grande demanda", explica. "São muitas pessoas interessadas naquele produto, naquele mesmo momento.
- **Impactos:** Umas das principais causas seria, quedas e indisponibilidade dos servidores e a redução de desempenho nos sistemas. Não basta focar apenas em ranquear bem e receber um grande número de acessos. É preciso estar pronto para isso! Não é qualquer hospedagem que suporta um volume de tráfego alto e picos de acesso. Muitas vezes isso ocasiona lentidão nos acessos e pode até deixar o site fora do ar
- **Indicadores:** Alto tráfego na rede
- **Estratégia de Mitigação:** O melhor que você tem a fazer é contratar um serviço maior, talvez um servidor dedicado, para que o seu site possa continuar a funcionar normalmente.

Contratar um servidor de nuvem também pode ajudar a resolver essa questão e também é muito importante ter uma conexão reserva.

- Plano de Contingência: Realizar o upgrade no servidor, aumentar a banda de tráfego e utilizar a conexão reserva

9 - Risco de Técnico | Risco de segurança sem ter a certificação SSL.

- **Gravidade do Risco:** leve.
- **Descrição:** A certificação SSL permite que o site trafegue os seus dados criptografados com o protocolo HTTPS, a ToolsNet não trabalha com nenhum tipo de tráfego de dados sensíveis.
- **Impactos:** Perda de credibilidade.
- **Indicadores:** Diminuição nos números de acesso.
- **Estratégia de Mitigação:** instalar o certificado
- **Plano de Contingência:** Informar os usuários que não são coletados dados.

10 - Risco de Técnico |Risco tecnológico com tecnologias obsoletas.

- **Gravidade do Risco:** Grave
- **Descrição:** O uso de tecnologias obsoletas pode causar falhas de segurança e mau funcionamento das bibliotecas usadas.
- **Impactos:** Instabilidade, feedbacks negativos.
- **Indicadores:** Warns ao subir versões.
- **Estratégia de Mitigação:** Acompanhar a documentação das tecnologias usadas no projeto.
- **Plano de Contingência:** Realizar a atualização das bibliotecas.