

# Análise de Riscos



Engenharia de Software 2023/2024
Especificação do Sistema – Análise de Riscos

Turma : 3

Grupo nº1

nº202100299 - Rui Barroso

nº202100296 - Gonçalo Vieira

nº202100984 - Francisco Silva

nº201901953 - André Pauli

- Índice
- Análise de Riscos
- Risco de planeamento
- Risco de desenvolvimento
- Risco de manutenção
- Risco de servidor
- Risco de financiamento

Risco de planeamento

Riscos

Id	Risco	Rating	Prioridade
RP1	A falta de um objetivo claro no planeamento do projeto pode causar ideias repetitivas e má gestão do processo desenvolvimento.	Alto	Baixa
RP2	A troca de ideias entre o Gestor de Projeto e o Cliente em falta resulta em conflitos e na perda do direção no planeamento.	Médio	Alta
RP3	A inclusão de quantidades exorbitantes de tarefas pode resultar em sobrecarga de trabalho para a Equipa e na dificuldade de concluir Sprint's a tempo.	Baixa	Média
RP4	Um <i>Backlog</i> que possui tarefas mal definidas, planeadas, priorizadas ou estimadas, resulta em atrasos e desorganização durante o Sprint.	Baixo	Média
RP5	A Equipa pode não estar adequadamente capacitada em termos de conhecimento técnico, habilidades ou experiência, o que pode resultar em subestimação do esforço necessário para completar as tarefas do Sprint.	Baixo	Baixa
RP6	Se as estimativas de Story Points do Sprint estiverem imprecisas, a cumprimento dos objetivos do Sprint poderá ser comprometida.	Médio	Alta
RP7	Se houver dependências de tarefas entre diferentes Sprints, a má gestão, planemaneto e desenho das tarefas pode resultar em atrasos no Sprint.	Alto	Alta
RP8	A alteração nos Requisitos do Projeto pode afetar o planeamento e o funcionamento de Sprints futuros.	Baixa	Baixa

Mitigação

<b>Id</b>	<b>Mitigação</b>
RP1	Garantir que a Equipa colabore na confecção de um único objetivo alcançável.
RP2	Estabelecer uma forte componente de comunicação com o Cliente garante um planeamento concreto.
RP3	Escolher de forma eficiente as tarefas a concluir na reunião de Sprint Planning.
RP4	Delegar corretamente as tarefas entre os membros da Equipa consoante as suas capacidades.
RP5	Delegar corretamente as tarefas entre os membros da Equipa consoante as suas capacidades.
RP6	Projetar e prever melhor os Story Points de cada membro.
RP7	Identificar e gerir as tarefas nos pontos de contacto entre os Sprints.
RP8	Possuir uma boa Análise e Especificação de Requisitos

Risco de desenvolvimento

Riscos

<b>Id</b>	<b>Risco</b>	<b>Rating</b>	<b>Prioridade</b>
RD1	Risco de implementação inadequada do sistema de pagamentos integrado	Baixo	Alta
RD2	Risco de dificuldades na personalização dos treinos na funcionalidade de recomendação de treinos personalizados	Médio	Média
RD3	Dificuldades na integração de novas funcionalidades com as existentes, resultando em inconsistências ou conflitos no produto final	Alto	Alta
RD4	Problemas de layout ou usabilidade na interface do utilizador, dificultando a navegação ou compreensão das funcionalidades da aplicação	Médio	Alta

Mitigação

<b>Id</b>	<b>Mitigação</b>
RD1	Erro na lógica de recomendação de treinos personalizados, resultando em recomendações inadequadas ou pouco úteis
RD2	Falha na autenticação ou sincronização de dados durante o processo de inscrição de utilizadores
RD3	Realizar testes de integração extensivos para identificar e resolver conflitos potenciais entre as funcionalidades existentes e as novas. Estabelecer uma estratégia de gestão de mudanças para garantir uma implementação suave de novas funcionalidades.

RD4	Conduzir testes de usabilidade regulares com utilizadores reais para identificar e corrigir problemas de layout e usabilidade. Realizar iterações de design com base no feedback dos utilizadores para melhorar continuamente a experiência do utilizador.
-----	--

Risco de manutenção

Riscos

Id	Risco	Rating	Prioridade
RM1	Descontinuação do serviço Stripe	Alta	Alta
RM2	Vulnerabilidades de segurança na API Stripe	Média	Média
RM3	Dependência de terceiros (Firebase Storage)	Média	Média
RM4	Possíveis mudanças nas APIs (Stripe e Firebase Storage)	Baixa	Baixa

Mitigação

Id	Mitigação
RM1	Diversificação de fornecedores de serviços de pagamento: Manter a opção de integração com outros provedores de serviços de pagamento, além do Stripe, para mitigar os impactos caso o serviço seja descontinuado. Realizar avaliações regulares do mercado para identificar alternativas viáveis.
RM2	Implementação de práticas de segurança robustas: Realizar auditorias regulares de segurança na integração com o Stripe, implementar medidas de segurança recomendadas pelo próprio Stripe e garantir a conformidade com padrões de segurança, como PCI DSS (Payment Card Industry Data Security Standard). Utilizar bibliotecas e frameworks seguros e manter todas as dependências atualizadas para mitigar o risco de vulnerabilidades.
RM3	Backup de dados: Implementar políticas de backup adequadas para os dados armazenados no Firebase Storage, garantindo a redundância e a disponibilidade dos arquivos essenciais para o funcionamento do sistema. Considerar a replicação dos dados em outros provedores de armazenamento em nuvem como medida adicional de mitigação.
RM4	Monitoramento contínuo das APIs: Manter-se atualizado com as atualizações e mudanças nas APIs do Stripe e do Firebase Storage, acompanhando os comunicados de alterações e mantendo um plano de contingência para lidar com possíveis mudanças que possam impactar a integração. Testar regularmente a integração para garantir sua funcionalidade adequada após atualizações ou mudanças nas APIs.

Risco de servidor

Riscos

Id	Risco	Rating	Prioridade
----	-------	--------	------------

RServ1	Vulnerabilidades de Segurança na Aplicação ASP.NET Core MVC	Médio	Alta
RServ2	Interrupções de Serviço devido a Problemas na Configuração da Infraestrutura na Azure	Alto	Crítica
RServ3	Exposição de Dados Sensíveis devido a Configurações Inadequadas de Segurança	Alto	Alto
RServ4	Vulnerabilidades de Segurança na Base de Dados Azure	Médio	Médio
RServ5	Problemas de Desempenho devido a Falta de Otimização da Base de Dados da Azure	Baixo	Baixo
RServ6	Interrupções no Serviço devido a Falta de Escalabilidade da Aplicação	Médio	Alta

#### Mitigação

Id	Mitigação
RServ1	<ul style="list-style-type: none"> <li>Realizar auditorias de segurança regulares na aplicação para identificar e corrigir vulnerabilidades conhecidas.</li> <li>Implementar práticas de desenvolvimento seguro, como validação de entrada de dados, prevenção de injeção de SQL e uso de frameworks de segurança.</li> <li>Manter a aplicação e todas as bibliotecas/frameworks utilizadas atualizadas para corrigir falhas de segurança conhecidas.</li> </ul>
RServ2	<ul style="list-style-type: none"> <li>Implementar monitoramento proativo da infraestrutura Azure para identificar e resolver rapidamente problemas de configuração ou falhas nos serviços.</li> <li>Utilizar práticas de DevOps e automação para garantir a consistência e confiabilidade da configuração da infraestrutura.</li> <li>Implementar políticas de backup e recuperação de desastres para minimizar o impacto de interrupções de serviço.</li> </ul>
RServ3	<ul style="list-style-type: none"> <li>Implementar controle de acesso baseado em função (RBAC) para restringir o acesso aos dados apenas às pessoas autorizadas.</li> <li>Criptografar dados sensíveis em repouso e em trânsito para protegê-los contra acesso não autorizado.</li> <li>Realizar auditorias de segurança regulares para identificar e corrigir configurações inadequadas de segurança.</li> </ul>
RServ4	<ul style="list-style-type: none"> <li>Implementar práticas recomendadas de segurança da base de dados, como autenticação forte, criptografia de dados e auditoria de acesso.</li> <li>Manter o banco de dados Azure atualizado com as últimas atualizações de segurança e patches de correção.</li> <li>Utilizar firewalls de rede e grupos de segurança para restringir o acesso a base de dados apenas a IPs e serviços confiáveis.</li> </ul>
RServ5	<ul style="list-style-type: none"> <li>Realizar análises de desempenho regulares na base de dados Azure para identificar e otimizar consultas lentas e problemas de índice.</li> <li>Utilizar cache de consultas e estratégias de armazenamento em cache para reduzir a carga no banco de dados e melhorar o desempenho da aplicação.</li> </ul>

	<ul style="list-style-type: none"><li>• Implementar monitoramento de desempenho contínuo para identificar e resolver problemas de desempenho em tempo real.</li></ul>
RServ6	<ul style="list-style-type: none"><li>• Implementar escalabilidade automática na aplicação Azure para lidar com picos de tráfego e aumento da carga de trabalho.</li><li>• Utilizar serviços gerenciados e escaláveis da Azure, como Azure App Service e Azure SQL Database, que oferecem escalabilidade horizontal e vertical.</li><li>• Realizar testes de carga e dimensionamento para identificar os limites de capacidade da aplicação e planejar a escalabilidade conforme necessário.</li></ul>

Risco de financiamento

Riscos

Id	Risco	Rating	Prioridade
RF1	Orçamento Insuficiente devido a Custos Inesperados	Alto	Alto

Mitigação

Id	Mitigação
RF1	<ul style="list-style-type: none"><li>• Realizar uma análise de custos detalhada para identificar e estimar todos os custos potenciais do projeto.</li><li>• Criar uma reserva de contingência no orçamento para cobrir custos inesperados ou emergências.</li><li>• Implementar práticas de gerenciamento financeiro eficazes, como monitoramento regular do fluxo de caixa e revisões financeiras periódicas.</li><li>• Procurar otimizar os custos onde possível, buscando alternativas mais econômicas ou eliminando gastos desnecessários.</li></ul>