Trabalho Final de APSEI

O FlexiGather do ponto de vista de APSEI

Aspetos Profissionais e Sociais da Engenharia Informática
Professor: Rui Aguiar

Realizado por:
Rafael Kauati - 105925
Roberto Castro - 107133
Maria Abrunhosa - 107658
Marta Inácio - 107826
Tiago Gomes - 108307
Sara Almeida - 108796

Introdução

No âmbito da disciplina de Aspetos Profissionais e Sociais da Engenharia informática (APSEI), foi-nos apresentado a proposta de um trabalho final onde iríamos analisar um trabalho base (TB) e apresentar as alterações necessárias para a sua comercialização, com base nos diversos aspetos lecionados na disciplina. O trabalho base do presente trabalho foi o projeto criado por alguns membros do grupo, o FlexiGather, na disciplina de Projeto de Informática (PI).

Atualmente, a indústria de gestão de eventos enfrenta alguns problemas, sendo o principal a dificuldades dos sistemas atuais não corresponderem às expectativas e aos requisitos dos clientes. Assim surgiu a ideia da criação do FlexiGather, um sistema de gestão integrada de eventos desenvolvido de modo a ser acessível e versátil, adaptando-se ao evento desejado pelos clientes.

Assim, neste relatório a partir do Flexigather vamos apresentar algumas alterações, legislações, regulamentações, medidas de cibersegurança, entre outros tópicos abordados na disciplina, que necessitam de ser correspondidos para a sua comercialização.

O trabalho base

Funcionalidades

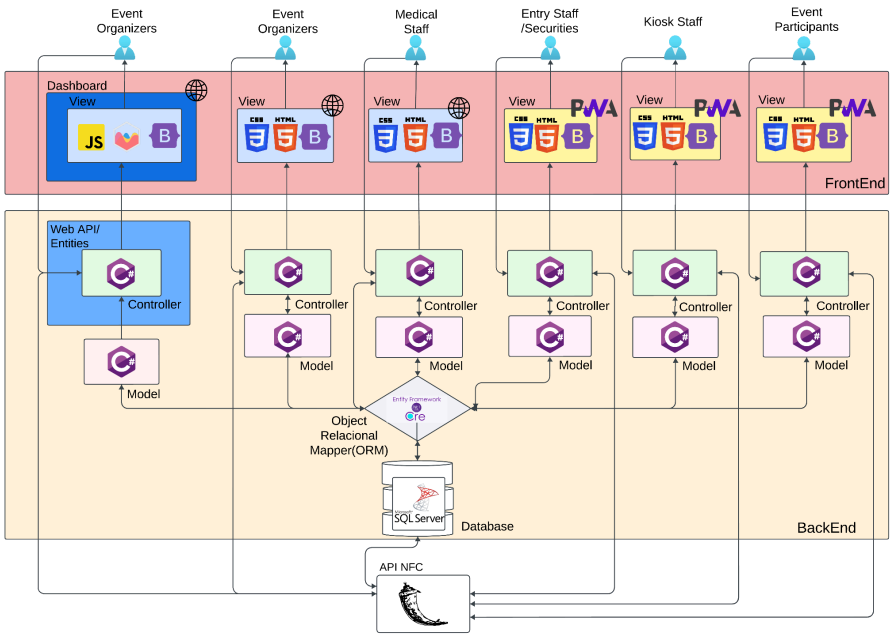
O FlexiGather, um sistema de gestão de eventos que pretende competir com plataformas de gestão de eventos, que permite realizar compras no evento associado, atualizações de saldo, monitorização de dados , controlo de acessos, com registo de entradas e saídas do evento, gestão de informações pessoais, nomeadamente médicas.

Arquitetura

Para isso o sistema possui uma base de dados centralizada, em SQL Server, dividida em domínios. Um domínio do evento, que possui tabelas correspondentes às áreas comuns entre os eventos, por exemplo o kiosk, um domínio temático que permite o cliente escolher o tipo de evento que deseja de modo a que o sistema corresponda às suas expectativas e, por fim, um domínio médico para gerir e guardar as informações e tratamentos médicos efetuados no evento.

Este último, apresenta-se como uma novidade do TB em relação a possíveis competidores de mercado como a 360 city e a cvent, proporcionando-nos alguma vantagem quando são realizados, por exemplo, eventos desportivos.

Como podemos ver na imagem abaixo, a partir da base de dados centralizada o sistema possui um Mapeador Objeto-Relacional (ORM), o Entity Framework Core Power Tools, que permite o uso de engenharia inversa para criar os modelos do sistema. Após a criação dos modelos, todo o sistema é baseado na arquitetura Model-View-Controller(MVC). O modelo representa os dados, o controlador processa todas as interacções com o utilizador e a vista apresenta os resultados. Por fim e de modo a permitir a leitura de pulseira NFC no nosso sistema, é utilizada uma api, desenvolvida em Flask.



Ainda na arquitetura apresentada temos a interface do utilizador, a interface dos quiosques e a interface de acesso, a utilizar pelos participantes, pelo pessoal dos pontos de venda e de venda e de carregamento e pelo pessoal da entrada, respetivamente. Estas serão implementadas como PWAs - Progressive Web Apps. Quanto às restantes, serão implementadas como WebSites e são a interface médica, a interface de administração e o painel de controlo, que se destinam ao pessoal médico e aos administradores, respetivamente.

Tecnologias

Quanto às tecnologias utilizadas no nosso projeto desenvolvido em PI, temos SQL Server, Asp.NET Core, HTML, CSS, BootStrap, JavaScript, Chart.js, Entity Framework PowerTools e Flask.

A. Ecossistema de Comercialização do FlexiGather

De um modo geral, o ecossistema em que se enquadraria o FlexiGather, ao ser comercializado, seria muito semelhante ao já projetado na construção do nosso trabalho base. No entanto, os atores no nosso ecossistema, como os participantes no evento, os organizadores do evento e alguns parceiros do evento.

O nosso sistema, para funcionar, precisa de guardar todos os seus dados, seja em servidores físicos ou na cloud. Independentemente do armazenamento destes dados, cada uma das soluções custa dinheiro. Para se fazer uma gestão de como ganhar dinheiro com o nosso sistema precisamos de avaliar quais são os gastos e trabalhar a partir daí.

Primeiramente, terá de ser feito um contrato por cada evento ao qual fornecemos os nossos serviços uma vez que diferentes dimensões requerem diferentes percentagens.
Será acordado, inicialmente, um valor rondando uma porcentagem que cubra a maioria das despesas de armazenamento e/ou de compra de pulseiras ao fornecedor. A percentagem será ajustada consoante o tipo de evento e o número de participantes. Estas despesas, de armazenamento e de pulseiras, são feitas tendo em conta o valor máximo de lotação que um evento pode ter, ou seja, se para o máximo de lotação tivemos de gastar aproximadamente 20 mil euros mas na realidade só apareceram aproximadamente 70% dos participantes inicialmente esperados, o nosso gasto diminui. Se o gasto diminuir, não temos de ganhar para cobrir uma percentagem tão grande até à despesa total, uma vez que já não é preciso suportar tantos dados armazenados.

Para além disso, de forma a cobrir a margem percentual das despesas, descartada inicialmente, e ter algum lucro, será acordada uma comissão por cada bilhete vendido, ou seja, cada participante armazenado na base de dados. Esta comissão também será ajustada ao valor dos bilhetes.

A ideia de pedir uma comissão por cabeça, dá-nos a possibilidade de crescer proporcionalmente com o crescimento do evento e da sua afluência. O risco de ter prejuízo será minimizado uma vez que o valor inicial do acordo, fora as comissões, é feito tendo em conta o número máximo de participantes, o que raramente se realiza. Caso aconteça, a comissão de venda por cada bilhete facilmente cobrirá a margem percentual das despesas, descartada inicialmente.

Todo este método de negócio será aplicado a grandes eventos com um elevado número de participantes. Para pequenos e médios eventos, o contrato de pagamento procura cobrar as despesas na totalidade mais uma pequena percentagem de forma a ajustar e tentar ter lucro.

Os clientes do FlexiGather serão todos os grupos ou empresas que pretendam gerir o seu próprio evento, procurando ajuda para uma melhor gestão e organização do mesmo. Com isto, quem paga os nossos serviços são estes organizadores de eventos.

Fornecedores

Como fornecedores de serviços, teríamos empresas de cloud como a Azure para hospedagem, armazenamento e processamento de dados. Para pulseiras com tecnologias NFC, usamos fornecedores como a *nfc.pt*.

Clientes

Os clientes da FlexiGather seriam entidades que organizam eventos e estão interessadas em auxiliar-se de meios tecnológicos para facilitar a gestão dos mesmos. Exemplos incluem o Corpo Nacional de Escutas, Associações Académicas, e Organizações de Festivais ou até Maratonas. Estas entidades necessitam de soluções para gestão de acessos, facilitação de compras dentro do evento e suporte médico. Os clientes podem ser segmentados em pequenas e médias empresas (PMEs) que realizam eventos corporativos, grandes corporações que organizam grandes conferências e entidades governamentais que realizam eventos públicos e comunitários.

Compensação e Diferenciais

A compensação do Flexigather poderia ser através de um modelo de subscrição, com taxas mensais ou anuais baseadas no número de eventos ou participantes, comissões sobre vendas feitas dentro do evento e venda de hardware, como pulseiras NFC e scanners. Os fatores diferenciadores do Flexigather incluem a capacidade do sistema de se adaptar a vários tipos de eventos, utilizando uma base de dados baseada em domínios, e a possibilidade de interface de suporte médico para gestão de tendas de apoio médico em eventos.

Enquadramento Regulatório

O nosso sistema pode enquadrar-se no Regulamento Geral sobre a Proteção de Dados (RGPD), que garante a legalidade na aquisição, armazenamento e gestão de dados pessoais e dados de saúde. No entanto, é importante analisar que poderemos estar fora do âmbito de violação deste regulamento, por exemplo no que toca aos dados médicos, já que estes, que são fornecidos no momento da inscrição, são necessários ao funcionamento da interface médica e é do interesse legítimo do utilizador que sejam recolhidos.

Para que se desse a comercialização do nosso trabalho base, para uma melhor gestão de recursos e maior agilidade no que toca a carregamentos, seria implementada a possibilidade de carregamento digital, por exemplo com o uso de “MBWay” a partir do nosso sistema, na interface do participante. Assim seria necessário o cumprimento do Regulamento de Serviços de Pagamento 2 (PSD2). Regulamento que estabelece requisitos para a Autenticação Forte do Cliente (SCA), promovendo integração e eficiência do mercado de pagamentos tornando-os mais seguros e protegendo os consumidores e empresas europeias.

É de notar que, dado que o nosso sistema, tal como dito anteriormente, é adaptável para vários tipos de eventos, poderemos enquadrar-nos em diferentes planos regulatórios adicionais. Por exemplo, num evento onde houvessem participantes menores de idade, nova regulamentação teria de ser tida em conta, como, por exemplo, o limite etário para consentimento parental tido em conta pela autoridade nacional de proteção de dados.

Efeitos de escala

O nosso projeto seria escalável a nível de dimensão dos eventos bem como de diferenciação do tipo de eventos. O nosso TB, dado que foi inicialmente projetado para um cenário de utilização com número expectável de participantes reduzido, não é totalmente escalável horizontalmente, isto é, para aumentar a dimensão de utilizadores do nosso sistema teríamos de futuramente implementar um *message broker*, por exemplo, utilizando *Kafka*.

Atualmente, o TB suporta apenas pedidos síncronos. Em caso de elevada latência da rede, alguns pedidos podem ficar perdidos. Para controlar estes problemas, a solução seria implementar um *message broker*, utilizando tecnologias similares ao Apache *Kafka*, de forma a sistemas que incluem uma fila de pedidos assíncronos. Esta implementação, em caso de falhas de rede ou no sistema em si, guarda os pedidos e estes serão executados à medida que a rede/sistema seja restabelecido, assegurando fault tolerance para o sistema.

Uma das alternativas, seria criar algumas interfaces em modo offline, isto é, sem obrigatoriedade de receberem informação em tempo real e, depois de se criar um grupo de pedidos, os mesmos seriam encaminhados para a base de dados ao mesmo tempo, dando um ideia de assincronicidade. Neste caso, uma das interfaces que não poderia ser desenvolvida desta forma, perdendo todo o seu caráter e impacto, seria a interface médica e, com menos importância, a *dashboard*.

B. Propriedade Intelectual e Marcas Registradas

A “FlexiGather”, enquanto uma empresa que fornece um serviço, não exige o registo de patente ou modelo de utilidade, já que não existe nenhuma atividade inventiva valorizável ou vantagem técnica ou prática obviamente evidente com necessidade de ser protegida. Por outro lado, quanto aos direitos de incidência comercial, para proteger a propriedade industrial teríamos uma marca registrada nacionalmente, bem como um logotipo através do INPI (Instituto Nacional da Propriedade Industrial).

C. Licenciamento Open Source

Analisando as livrarias, frameworks e dependências de software utilizadas ao longo do projeto, podemos enumerá-las juntamente com suas respectivas licenças open-source.

Open Source Software utilizados (e suas respectivas licenças):

- Flask: BSD-3
- ChartJs: MIT license
- Azure Identity: MIT license
- NuGet: Apache 2.0
- Rotativa: MIT license
- ZXing.Net.Bindings.Windows.Compatibility: Apache-2.0
- X.PagedList: MIT license
- System.Text.Json: MIT license
- Microsoft.AspNetCore.Identity.EntityFrameworkCore: MIT license
- Microsoft.EntityFrameworkCore.SqlServer: Apache 2.0
- Microsoft.VisualStudio.Web.CodeGeneration.Design: MIT license
- MailKit: MIT license
- Microsoft.Extensions.DependencyInjection: MIT license
- Microsoft.EntityFrameworkCore.Tools: MIT license

Tendo em conta a lista de dependências open source utilizadas, é possível sinalizar algumas considerações no que a presença de tais licenças e utilização de seus OSS implica no projeto:

- **Modificação e distribuição:** Permite-se modificar e distribuir o software, inclusive em projetos proprietários e de código fechado.
- **Uso Comercial:** Permitido o uso comercializado, sem obrigatoriedade em disponibilizar publicamente o código derivativo.
- **Atribuição:** Obrigatoriedade na reconhecimento autoral e inclusão da licença original no uso do OSS ou em casos de alterações feitas no código fonte original.

Tais medidas, seguidas adequadamente, asseguram a FlexiGather a legitimidade na autônoma decisão na utilização, compartilhamento e tratamento do source code do TB, em função do uso de licenças **MIT, Apache 2.0 e BSD-3**. É de frisar que o nosso código não seria open-source.

D. Cibersegurança

Maiores ataques

O nosso sistema pode ser alvo de ataques de cibersegurança consideráveis, de entre eles destacando:

- **Phishing**: Tentativas de obter informações sensíveis disfarçando-se como comunicações confiáveis.
- **DDoS** (Distributed Denial of Service): Ataques que sobrecarregam os servidores, tornando o serviço indisponível.
- **Injeção de SQL**: Exploração de vulnerabilidades em bases de dados para roubo ou alteração de dados.
- **Malware e Ransomware**: Software malicioso que compromete o sistema ou exige resgate para restaurar o acesso.
- **Engenharia Social:** Manipulação psicológica para obter informações confidenciais.
- **Exfiltração de Dados**: Acesso não autorizado a dados sensíveis.
- **Man-in-the-Middle** (MitM): Interceptação de comunicações entre sistemas para acessar informações confidenciais.
- **Exploits de Zero-Day**: Exploração de vulnerabilidades desconhecidas antes que possam ser corrigidas.

Legislação de cibersegurança

O Flexigather tem de cumprir várias legislações de cibersegurança para poder ser usado legalmente e garantir a proteção dos dados dos participantes dos diferentes eventos. A legislação mais relevante será o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, que estabelece regras e protocolos a seguir para a proteção de dados pessoais e sensíveis. Além disso, pode vir a ser necessário estarmos de acordo com a Diretiva NIS (Network and Information Systems Directive), cujo objetivo é alcançar um alto nível de segurança das redes e sistemas de informação na União Europeia. Dependendo da localização dos eventos e dos participantes, o Flexigather pode vir a ter de cumprir com a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) dos Estados Unidos, se estivermos a lidar com dados médicos de cidadãos americanos. Além disso, seguir as melhores práticas e padrões da indústria, como o ISO/IEC 27001 para sistemas de gestão de segurança da informação, ajudará a garantir que o FlexiGather esteja em conformidade com as normas internacionais de segurança.

Implementação de soluções de cibersegurança

Res: Para implementar soluções de cibersegurança no Flexigather, tanto em termos de tecnologias como de processos, devemos considerar os seguintes passos:

Tecnologias:

- Criptografia: Utilizar criptografia forte, como o AES-256, para proteger dados em trânsito e em repouso.

- Firewalls e Sistemas de Detecção de Intrusões (IDS): Implementar firewalls e IDS para monitorar e bloquear tráfego suspeito.
- Autenticação Multifator (MFA): Exigir MFA para todos os acessos ao sistema para aumentar a segurança.
- Certificados SSL/TLS: Utilizar certificados SSL/TLS para proteger as comunicações web.
- Backup e Recuperação de Dados: Implementar sistemas de backup regulares e planos de recuperação de desastres para garantir a integridade dos dados.

Processos:

- Políticas de Segurança: Desenvolver e implementar políticas de segurança abrangentes que definam procedimentos de segurança e responsabilidades.
- Formação e Conscientização: Oferecer formação regular em cibersegurança para todos os funcionários para aumentar a conscientização sobre ameaças e práticas de segurança.
- Gestão de Permissões: Implementar um rigoroso controle de acesso baseado no princípio do menor privilégio, garantindo que os utilizadores tenham apenas as permissões necessárias.
- Monitorização e Auditoria: Realizar monitorização contínua e auditorias regulares dos sistemas de segurança para identificar e mitigar ameaças.
- Resposta a Incidentes: Estabelecer um plano de resposta a incidentes que detalhe os passos a serem tomados em caso de violação de segurança, incluindo a notificação às autoridades competentes e aos afetados.

E. Recuperação de um Ataque Publicitado na Internet

Em cenários de violação de dados, medidas de contenção de danos iriam ser tomadas as seguintes medidas:

1. **Comunicação e Transparência:**
    - Notificar o mais cedo possível e com a maior transparência tanto os clientes quanto parte envolvidas sobre o ataque e as medidas imediatas que estão a ser tomadas.
    - Fornecer orientações sobre medidas que os clientes podem tomar para se protegerem.
    - Manter a transparência sobre o ocorrido, o impacto e o que está sendo feito para remediar a situação.
2. **Controlo dos possíveis danos:**
    - Contratar especialistas de segurança para avaliar e melhorar a infraestrutura de segurança.
    - Reportar o incidente às autoridades competentes.
3. **Melhoria da Segurança com ajuda de uma equipa especializada:**
    - Atualizar todos os sistemas e garantir que desenvolvedores e funcionários sigam as melhores práticas de segurança.
    - Correção de vulnerabilidades identificadas.
    - Recuperação de dados através dos backups.
4. **Auditoria e Planeamento:**
    - Realizar periódicas auditorias completas dos sistemas de segurança.
    - Desenvolver, rever e testar regularmente um plano de recuperação de ataques.
5. **Parcerias estratégicas:**
    - Realizar parcerias com empresas estratégicas, como empresas de segurança, de modo a recuperar a confiança dos nossos clientes pela existência de uma nova garantia de segurança externa ao nosso sistema.
6. **Rebranding:**
    - No caso de perdemos a total confiança dos nossos clientes, podemos optar pelo recomeço do nosso sistema com uma nova imagem.

F. Proteção de Privacidade

A proteção de privacidade é essencial para o Flexigather, que recolhe dados pessoais dos participantes dos eventos. Para garantir segurança e conformidade com o RGPD, serão implementadas várias medidas:

1. **Medidas de Segurança:**
    - **Criptografia:** Utilizar criptografia para dados em trânsito e em repouso (AES e TLS).
    - **Autenticação Multifator (MFA):** Assegurar um acesso seguro e restrito a pessoal autorizado.
    - **Privacidade por Design:** Minimizar a coleta de dados, anonimizar informações pessoais e obter consentimento informado dos utilizadores.
2. **Monitorização e Auditoria:**
    - Realizar monitorização contínua e auditorias regulares para identificar e corrigir vulnerabilidades.
3. **Soluções Técnicas:**
    - **Firewalls e IDS:** Implementar firewalls e sistemas de detecção de intrusão.
    - **Gestão de Acessos:** Reforçar a gestão de acessos com MFA e políticas de senhas fortes.
    - **Desenvolvimento Seguro:** Garantir um ciclo de vida de desenvolvimento seguro (SDLC) e realizar testes de penetração regulares.
4. **Resposta a Pedidos Legais:**
    - Estabelecer uma equipa dedicada e ferramentas automatizadas para coleta e entrega de dados.
    - Manter registos detalhados de todas as solicitações e respostas.
    - Integrar com sistemas de gestão de dados existentes e fornecer formação contínua sobre regulamentações de privacidade e procedimentos.

G. Aspectos Éticos e Regulamentação

O Flexigather envolve a recolha e armazenamento de dados pessoais e sensíveis, incluindo fotos e informações médicas dos participantes. Por isso, é essencial abordar os aspectos éticos e regulamentares de forma adequada:

1. **Aspectos Éticos:**
    - **Privacidade dos Dados:** Garantir que os dados pessoais e médicos dos participantes estejam protegidos contra acessos não autorizados.
    - **Transparência:** Informar claramente os participantes sobre quais dados estão a ser recolhidos e obter seu consentimento explícito.
    - **Segurança:** Implementar medidas rigorosas para prevenir a fuga dos dados e garantir a segurança das informações pessoais e médicas.
    - **Recolha de dados médicos**: Quanto à recolha, dado que temos dados médicos, é importante referir que estes não são recolhidos por nós, apenas armazenados, já que são fornecidos pelos participantes no momento da inscrição no evento.
2. **Uso de Fotos:**
    - As fotos tiradas no check-in serão usadas exclusivamente para confirmar a identidade dos participantes, garantindo a segurança em casos, por exemplo, de roubo de pulseiras. Estas fotos estariam apenas disponíveis nas interfaces de acesso e kiosks, bem como na enfermaria, confirmando o uso seguro e a necessidade das fotografias referidas anteriormente.
3. **Regulamentação a Cumprir:**
    - **RGPD:** Garantir os direitos de acesso, correção e eliminação dos dados dos participantes, processando esses dados de forma justa e transparente.
    - **Legislação de Proteção de Dados:** Cumprir com a Lei de Proteção de Dados Pessoais de cada país onde o projeto opera.
    - **Regulamentações de Saúde:** Seguir regulamentações específicas do setor de saúde, caso se revele necessário no tratamento dos dados médicos.

H. Inteligência Artificial

Visto que não foi utilizado, diretamente ou indiretamente, nenhuma ferramenta de inteligência artificial no TB, não há considerações relevantes a expressar neste tópico.

I. Relações com Hyperscalers

À medida que a demanda do serviço se eleve para proporções de milhares, ou até milhões, de utilizadores (participantes de eventos), torna-se vital a adoção de serviços hyperscalers, para assegurar que o sistema consiga operar sem problemas notáveis de latência de transmissão de dados (em rede) ou processamento. No nosso caso, uma relação com a Azure, onde estariam deployed os nossos serviços, era essencial.

1. **Adoção:**
    - Estabelecer as necessidades de capacidade e de rede ao serviço escalado para os contratados hyperscalers.
    - Desenvolver métodos e ferramentas para monitorar e gerir os dados no serviço de nuvem.
2. **Formato de Relação:**
    - Contratos que explicitam as necessidades de armazenamento, processamento e rede iniciais, com datas estipuladas para possíveis crescimentos.
    - Cláusulas legais e regulamentações a serem cumpridas.
3. **Legislação Europeia:**
    - **RGPD:** Assegurar os princípios de Proteção de dados por design e por padrão.
    - **Consentimento e Direitos:** Garantir os direitos dos titulares de dados.
    - **Confidencialidade e Privacidade:** Proteger a comunicação de dados.
    - **Transparência:** Manter práticas transparentes de gestão de dados.
    - **Notificação de Incidentes:** Estabelecer procedimentos claros para a notificação de incidentes.

J. Efeitos de Rede

1. **Efeitos de Rede Positivos:**
    - **Utilizador Crescente:** Mais organizadores de eventos aumentam o valor da plataforma para todos.
    - **Efeito de Dados:** Mais dados melhoram a personalização e recomendações.
    - **Integrações e Parcerias:** Integração com plataformas populares (pagamentos, redes sociais) aumenta o valor.
    - **Comunidade e Feedback:** Comunidade de utilizadores fornece feedback valioso para melhorias contínuas.
2. **Efeitos de Rede Negativos:**

    Quanto aos efeitos de rede negativos, estes não são de maior relevância na comercialização dos nossos serviços dado que os teríamos deployed na Azure, ou seja, eles assegurariam segurança, suporte e confiabilidade na rede para suportar o armazenamento dos dados necessários aos eventos com quem estaríamos a trabalhar.