Análise e Planeamento

DESOFS – Relatório sobre o Ciclo de Vida do Desenvolvimento de Software Seguro

1200920; Eduardo Sousa
1190974; Pedro Lemos
1191526; Pedro Moreira
1230205; Rita Pinto
1201590; Tiago Costa

Introdução

No contexto digital atual, é crucial desenvolver sistemas seguros para garantir a integridade e a confidencialidade das informações. Neste projeto, iremos criar um jornal de notícias online seguindo os princípios do Ciclo de Vida de Desenvolvimento de Software Seguro (sigla SSDLC em inglês).

O objetivo principal é implementar um sistema robusto e seguro para a publicação e distribuição de notícias online. O jornal digital terá funcionalidades específicas, como registo de utilizadores, gestão de conteúdos, comentários de leitores e administração do site, entre outros.

Durante este projeto, iremos ter a oportunidade de explorar os fundamentos da segurança de software, aplicando-os diretamente na construção de um sistema real.

Análise

Descrição do projeto

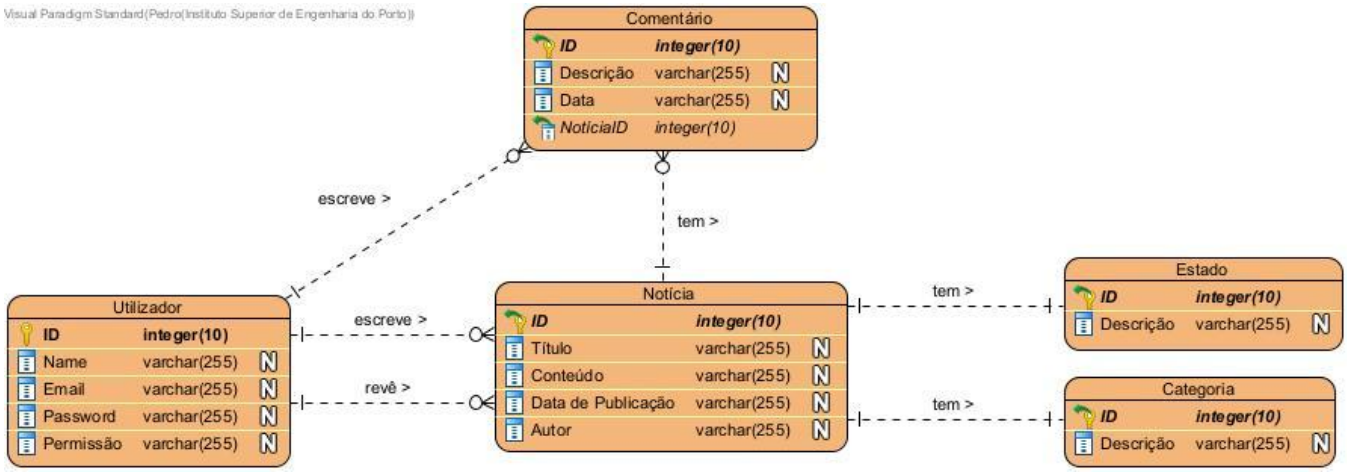
Este relatório aborda a modelação de ameaças relacionado um *website* de notícias. Neste *website*, estão presentes cinco tipos de utilizadores, enumerados por ordem crescente por nível de permissões: Leitor Não Registado, Leitor Registado, Jornalista, Editor e Administrador. Um leitor quer ele seja registado ou não, ao entrar no *website*, é deparado com a página inicial, que consiste nas notícias mais recentes, as quais podem ser selecionadas para ler a notícia em mais detalhe. É também possível um utilizador registar-se ou entrar com as suas credenciais. Um utilizador apenas se pode registar como Leitor Registado, para obter mais permissões, um perfil tem de ser criado pelo Administrador, mas um utilizador com permissões de Leitor Registado, Jornalista ou Editor, pode ser promovido em termos de permissões, também apenas pelo Administrador.

É possível também aos Leitores Registados, Jornalistas e Editores interagirem com notícias quando as mesmas estão selecionadas, sendo possível adicionar comentários. De forma às notícias serem publicadas e disponível para leitura, é necessário a escrita das mesmas, realizada pelo Jornalista. Após a escrita da mesma, é realizado um processo de revisão pelo Editor no qual a notícia pode ser aprovada, ou seja, publicada ou rejeitada. Os processos de revisão e publicação para revisão das notícias são realizados pelo Editor e Jornalista, respetivamente, que têm permissões para aceder às páginas necessárias para concluir cada processo.

Tal como o Editor e o Jornalista, o Administrador também tem acesso a páginas que outros utilizadores não têm acesso, na qual o mesmo pode gerir os utilizadores, ou seja, elevar ou rebaixar as permissões e criar ou apagar utilizadores.

Para tornar mais claro a forma como as entidades se relacionam, está representado na seguinte figura, o modelo de domínio.

Figura 1 - Modelo de Domínio



Informação do Modelo de Ameaças

O *Threat Model Information* é fundamental na segurança de software, devido às constantes ameaças e a necessidades de gerenciá-las adequadamente. Atacantes variam em habilidade, desde criminosos com pouca experiência até agentes sofisticados. Bugs revelam as fraquezas de um sistema e os atacantes exploram estas vulnerabilidades. O processo de identificar todas as ameaças e vulnerabilidades em sistemas complexos é complexo, mas o *Threat Modeling* oferece uma visão abrangente para entender e mitigar riscos. Além disso, ao examinar o software de diferentes perspetivas é possível identificar oportunidades para melhorias e novos recursos além da segurança.

Em geral, existem três abordagens básicas para o *Threat Modeling* a abordagem centrada no software, centrada no atacante e centrada no ativo. No nosso projeto, decidimos adotar a abordagem Centrada no Software. Isso significa que iremos avaliar a aplicação em questão, determinar os riscos associados e identificar maneiras para mitigá-los. Para isso, é necessário ter um bom entendimento da aplicação e do sistema em iremos executar.

Utilizadores da aplicação

Os utilizadores que vão interagir com o *website* terão diferentes permissões e funcionalidades uns dos outros. De forma a tornar a categorizar cada diferente tipo de utilizador, são atribuídos os seguintes termos a cada grupo de utilizadores:

1. Administrador
2. Editor
3. Jornalista
4. Leitor Registado
5. Leitor Não Registado

Requisitos Funcionais

Os *requisitos funcionais* são uma parte essencial da especificação do nosso sistema, descrevem as operações específicas que o sistema deve ser capaz de realizar para atender às necessidades dos utilizadores e alcançar os objetivos específicos do negócio. Eles detalham as funcionalidades do sistema, como o que ele deve fazer em termos de entradas, saídas e comportamentos esperados.

RF1 - O Leitor Não Registado deve criar conta leitor com um nome, e-mail e palavra-passe.

RF2 - O Leitor deve conseguir selecionar uma notícia para ler o conteúdo completo.

RF3 - O Leitor deve conseguir ler as notícias mais recentes na página inicial.

RF4 - As notícias devem ser organizadas por categorias para facilitar a navegação do Leitor.

RF5 - O Leitor Registado deve conseguir fazer login com as suas credenciais.

RF6 - O Leitor Registado deve poder comentar cada notícia quando esta está selecionada.

RF7- O Leitor deve poder gerir as suas configurações de conta, como a palavra e as restantes informações pessoais.

RF8 - O Leitor deve poder realizar ações comuns, como voltar à página anterior ou atualizar a página, de forma intuitiva e fácil para conseguir obter as notícias mais recentes, por exemplo.

RF9 - O Jornalista deve poder escrever noticias.

RF10 - O Editor deve poder realizar ações como adicionar, excluir, aprovar ou editar noticias.

RF11- O Administrador gere os utilizadores, sendo capaz de alterar as permissões de qualquer utilizador exceto de outro Administrador.

Requisitos Não Funcionais

Os *requisitos não funcionais* são critérios que especificam qualidades do sistema, em vez de suas funcionalidades específicas. Devem descrever as características do sistema que afetam o seu desempenho, segurança, usabilidade, confiabilidade e outros aspectos relacionados à qualidade. Esses requisitos descrevem como o sistema deve executar as suas funcionalidades, em vez de quais funcionalidades deve executar.

Funcionalidade

RNF1 - O sistema deve ser capaz de suportar a importação e adição de imagens a uma notícia.

RNF2 - Deverá ser possível pesquisar noticias por título, autor e data de publicação.

Usabilidade

RNF3 - O sistema deve ser acessível a partir de uma página web adaptada a todos os dispositivos.

RNF4 - O texto das notícias deve ser legível em todos os dispositivos.

RNF5 - O sistema deve ser fácil de usar e intuitivo.

RNF6 - O sistema deve ser capaz de suportar a adição de notícias por utilizadores sem conhecimentos técnicos.

Confiabilidade

RNF7 - O sistema não deve ter mais de 1 hora de inatividade por mês.

RNF8 - O sistema deve ser capaz de recuperar de falhas em menos de 5 minutos.

Performance

RNF9 - O sistema não deve demorar mais de 10 segundos para carregar a página inicia.

RNF10 - O sistema não deve demorar mais de 10 segundos para carregar a página de uma notícia.

Capacidade de suporte

RNF11 - A página web deve ser suportada por todos os navegadores modernos desktop e mobile.

RNF12 - O sistema deve ser capaz de suportar 1000 acessos simultâneos.

Segurança

RNF13 - O sistema deve estar em conformidade com os requisitos de segurança OWASP.

RNF14 - O sistema deve ser capaz de proteger os dados dos utilizadores (todos os roles).

RNF15 - O sistema deve ser capaz de proteger os assets do sistema. (Noticias, imagens, etc)

Manutenção

RNF16 - O sistema deve ser fácil de manter e atualizar.

RNF17 - O sistema deve ser capaz de ser atualizado sem afetar a base de dados.

Testes

RNF18 - O sistema deve ter uma bateria extensiva de testes unitários e de integração.

RNF19 - O sistema deve ser capaz de ser testado de forma automatizada.

RNF20 - Deve existir uma suite de testes de aceitação.

RNF21 - Deve existir uma pipeline de CI/CD.

Documentação

RNF22 - Deve existir documentação de utilizador.

RNF23 - Deve existir documentação com a arquitetura do sistema e os requisitos de segurança.

Requisitos de Segurança

Os *requisitos de segurança* são essenciais para proteger sistemas e dados contra diversas ameaças. Estes estabelecem políticas que garantem a confidencialidade, integridade e disponibilidade das informações. Ao integrar requisitos de segurança desde o início do desenvolvimento, o sistema pode ser protegido contra vulnerabilidades e ataques.

Tabela 1 - Requisitos de Segurança ASVS

Requisito de Segurança	Descrição	ASVS Level	#	CWE
Autenticação Segura	Garantir que o sistema de autenticação seja robusto e seguro, incluindo a utilização de senhas fortes, autenticação de dois fatores e políticas de bloqueio de conta.	Nível 1 Nível 2 Nível 3	Password Security- 2.1.[1-12], General authenticator Security- 2.2.[1-7], Authenticator Lifecycle - 2.3.[1-3], Credentials Storage-2.4.[1-5], Credencial Recovery - 2.5.[1-7], Look-up Secret Verifier - 2.6.[1-3], Out of Band verifier - 2.7.[1-7], One time Verifier - 2.8.[1-7], Cryptographic Verifier - 2.9.[1-3],Service Authentication - 2.10.[1-4]	CWE-620, CWE-521, CWE-308, CWE-307, CWE-304, CWE-620, CWE-303, CWE-640, CWE -287, CWE-522
Proteção contra Injeção de Código	Implementar medidas de proteção para prevenir a injeção de código, incluindo SQL injection e Cross-Site Scripting (XSS).	Nível 1 Nível 2 Nível 3	Output encoding and injection prevention – 5.3.[1-10]	CWE-89, CWE-79, CWE-116, CWE-176 ,CWE-830, CWE-78, CWE-943, CWE-643
Controlo de Acesso Adequado	Garantir que os utilizadores tenham acesso apenas às áreas e funcionalidades necessárias, com um	Nível 1 Nível 2	General Access Control Design - 4.1.[1-3], Operation Level Access Control - 4.2.[1-2], Other Access Control Considerations - 4.3.[1-2]	CWE-602, CWE-639, CWE-285, CWE-352, CWE-419, CEW-548

	sistema de controlo de acesso robusto.			
Criptografia de Dados	Proteger dados sensíveis em repouso e em trânsito por meio da implementação de técnicas de criptografia adequadas.	Nível 1 Nível 2	Data Classification - 6.1.[1-3] Algorithms - 6.2.[1-2] Random Values - 6.3.1	CWE-311, CWE-310, CWE-327, CWE-338
Gestão de Sessão Segura	Gerir sessões de utilizador de forma segura, com a utilização de cookies seguros, tokens CSRF e expiração de sessão adequada.	Nível 1	Fundamental Session Management Security - 3.1.1 Session Binding - 3.2.[1-3] Session Termination - 3.3.[1-2] Cookie-based Session Management - 3.4.[1-5] Defenses Against Session Management Exploits - 3.7.1	CWE-598, CWE-384, CWE-331, CWE-539, CWE-613 CWE-614 CWE-1004 CWE-16, CWE-778
Tratamento de Error e Logging	Implementação de um sistema de tratamento de erros e logging adequado, de forma a não expor informação que o utilizador não deva ter acesso	Nível 1 Nível 2	Log Content - 7.1.[1-4], Log Processing - 7.2.[1-2], Log Protection - 7.3.[1,3], Error Handling - 7.4.[1-3]	CWE-532, CWE-778, CWE-285, CWE-117, CWE-200, CWE-210, CWE-544, CWE-431

Casos de Uso

Os *casos de uso* são uma técnica na engenharia de requisitos que descreve como os utilizadores interagem com um sistema para alcançar objetivos específicos. Os casos de uso ajudam a estabelecer requisitos de forma clara e compreensível, que fornecem uma representação visual das interações entre os utilizadores e o sistema.

UC1 – Como Leitor Não Registado, quero registar me no *website.*

UC2 – Como Leitor Registado, quero ler notícias no *website.*

UC3 – Como Leitor, quero ver as notícias na página inicial.

UC4 – Como Leitor Registado, quero comentar uma notícia enquanto a estou a ler.

UC5 – Como Jornalista, quero enviar notícias para serem revistas.

UC6 – Como Jornalista, quero importar imagens ao enviar notícia para revisão.

UC7 – Como Editor, quero rever com a possibilidade de aprovar ou rejeitar notícias que estão para revisão.

UC8 – Como Editor, quero editar notícias que estão publicadas.

UC9 – Como Administrador, quero alterar as permissões de um utilizador exceto de outro Administrador.

UC10 – Como Administrador, quero criar utilizadores com permissões de Jornalista, Editor e Administrador.

Dependências Externas

As *dependências externas* são fatores externos ao código que se podem tornar numa ameaça para a aplicação. São fatores normalmente dentro do controlo da organização, mas não dentro da equipa de desenvolvimento.

Os seguintes fatores foram identificados:

Tabela 2 - Dependências externas

ID	Descrição
1	O website vai ser desenvolvido com um front-end em Angular, hosted na plataforma Azure e regularmente atualizado com as últimas patches de segurança.
2	O website vai ser desenvolvido com um back-end em Java, hosted na plataforma

	Azure e regularmente atualizado com as últimas patches de segurança.
3	O website vai ser desenvolvido com uma base de dados em MySQL, hosted na plataforma Azure e regularmente atualizado com as últimas patches de segurança.
4	Toda a comunicação entre front-end e back-end, e entre back-end e a base de dados é realizada através de uma private network.
5	A aplicação deve providenciar HTTPS a partir de um certificado CA.
6	A aplicação utiliza Auth0 para realizar autenticação e autorização.

Entry Points

Os *entry points* demonstram onde a informação entra no sistema, locais onde o utilizador pode interagir com a aplicação a inserir informação, por exemplo, preencher campos de *input.*

Seguindo o guia [1], os *entry points* devem ser documentados da seguinte forma:

- **ID**: ID único atribuído a cada *entry point.*
- **Nome**: Nome descritivo que identifica o *entry point.*
- **Descrição**: Descrição detalhada do que acontece no *entry point.*
- **Trust Level**: Permissões necessárias para aceder ao *entry point.*

Na Tabela 3 foram identificados os seguintes *entry points*:

Tabela 3 - Entry Points

ID	Nome	Descrição	Trust Level
1	Porta HTTPS	Qualquer página do website apenas pode ser acedida através do protocolo TLS.	Leitor não autenticado (1); Leitor autenticado (2); Jornalista (3); Editor (4); Administrador (5).
2	Página de login	Local no website onde cada utilizador realiza log in para conseguir utilizar o website.	Leitor não autenticado (1); Leitor autenticado (2); Jornalista (3); Editor (4); Administrador (5).
3	Página de registo	Local onde é se permite o registo no sistema.	Leitor não autenticado (1).
4	Página publicação de notícias	Local onde é possível publicar notícias.	Jornalista (3); Editor (4).
5	Página para rever	Local para rever notícias.	Editor (4).

	notícias		
6	Página do Perfil	Cada utilizador pode alterar as suas próprias configurações (como password entre outros)	Leitor autenticado (2); Jornalista (3); Editor (4); Administrador (5).
7	Página para visualizar uma notícia	Local para ler e adicionar comentários na notícia.	Leitor autenticado (2); Jornalista (3); Editor (4).
8	Gerir utilizadores	Local para criar, apagar e/ou alterar o papel de cada utilizador	Administrador (5).
9	Página Principal	Página que contém várias notícias	Leitor não autenticado (1); Leitor autenticado (2); Jornalista (3); Editor (4).

Exit Points

Os *exit points* são pontos de interação ou saída de uma aplicação web onde ocorrem interações críticas com os utilizadores. Cada página ou funcionalidade do sistema possui diferentes pontos de saída que representam ações específicas realizadas pelos utilizadores. Desta forma, é fundamental identificar e compreender os pontos de saída para avaliar possíveis vulnerabilidades de segurança e implementar as medidas adequadas de proteção [1].

Os pontos de saída que foram identificados foram os seguintes:

1. Página de Login
    a. O *exit point* presente é a exibição de mensagens de erro para as credenciais incorretas. As mensagens detalhadas podem expor informações sobre a validade de emails ou senhas, facilitando ataques de enumeração de utilizadores ou de força bruta.
2. Página de Registo
    a. Ao exibir mensagens de erro durante o registo (por exemplo, "Email já em uso"), a aplicação pode inadvertidamente divulgar informações sensíveis, como a existência de contas de utilizadores. Isso pode ser explorado pelos atacantes para enumerar utilizadores válidos.
3. Página de Revisão de Notícias
    a. A falta de controlos de acesso adequados nesta página pode permitir que utilizadores não autorizados visualizem ou manipulem artigos em revisão, comprometendo a integridade e confidencialidade do conteúdo.
4. Página de Perfil

   a. Permitir aos utilizadores alterar informações pessoais e senhas exige uma gestão cuidadosa da segurança. Vulnerabilidades na gestão de senhas, como políticas fracas ou falta de encriptação, podem expor as credenciais dos utilizadores a potenciais ataques.
5. Comentários nas notícias
   a. A falta de validação adequada e sanitização nos comentários dos utilizadores pode resultar em vulnerabilidades de cross-site *scripting* (XSS), permitindo que os atacantes injetem e executem scripts maliciosos no contexto da aplicação.

Ativos

Os ativos, ou *assets* na sua forma mais utilizada em inglês, são os elementos visados pelos potenciais atacantes e são a motivação por trás da existência de ameaças. Podem ser físicos, como os dados de clientes numa aplicação, ou abstratos, como a reputação de uma organização.

Ao documentar os ativos no modelo de ameaças, cada ativo é descrito da seguinte forma [1]:

- **ID**: Um identificador único atribuído a cada ativo para referência futura.
- **Nome**: Uma designação descritiva que identifica claramente o ativo.
- **Descrição**: Uma explicação detalhada do que é o ativo e por que é importante protegê-lo.
- **Nível de Confiança**: Os diferentes níveis de acesso ou importância atribuídos ao ativo.

Na Tabela 4 é possível ver os potenciais ativos que foram identificados na análise inicial feita ao jornal online.

Tabela 4 - Ativos identificados

ID	Nome	Descrição	Nível de Confiança
1	Credenciais do leitor	As credenciais que o leitor usa para aceder ao jornal.	Leitor autenticado (2); Administrador (5)
2	Infraestrutura	Servidores que hospedam o site e os sistemas que estão ligados entre si.	Administrador (5)
3	Reputação do Jornal	Credibilidade e confiança do jornal.	Leitor não autenticado (1); Leitor autenticado (2); Jornalista (3); Editor (4); Administrador (5)
4	Acesso a informação confidencial	Noticias que ainda não foram publicadas ou que ainda estão em fase de avaliação	Jornalista (3); Editor (4); Administrador (5)
5	Acesso privilegiado ao website	As contas de administrador e editor visto possuírem acesso privilegiado ao jornal	Editor (4); Administrador (5)
6	Funcionamento da plataforma	Disponibilidade do site e a integridade dos dados e backup.	Administrador (5)

Níveis de Confiança

Os níveis de confiança, ou *trusts levels*, representam os direitos de acesso que a aplicação concede a entidades externas. Estes níveis são cruzados com os pontos de entrada (*entry points*) e ativos (*assets*), permitindo definir os privilégios de acesso necessários em cada ponto de entrada e para interagir com cada ativo [1].

Os níveis de confiança são documentados no modelo de ameaças da seguinte forma:

- **ID:** Um número único é atribuído a cada nível de confiança para referência futura e cruzamento com pontos de entrada e ativos.
- **Nome:** Um nome descritivo que identifica as entidades externas que foram concedidas este nível de confiança.
- **Descrição:** Uma descrição textual do nível de confiança, detalhando a entidade externa que recebeu este nível de confiança e os privilégios ou direitos associados.

Os níveis de confiança que foram identificados na aplicação foram os seguintes:

Tabela 5 - Níveis de confiança presentes no jornal

ID	Nome	Descrição
1	Leitor Não Registado	Um utilizador que está conectado ao jornal, mas que não está autenticado.
2	Leitor Registado	Um utilizador que está conectado ao jornal utilizando a sua conta.
3	Jornalista	Um utilizador com permissões para criar notícias.
4	Editor	Aprova ou rejeita as notícias que são propostas pela jornalista.
5	Administrador	Administrador que tem acesso às permissões dos utilizadores dentro do jornal, podendo promover ou despromover os utilizadores.

Diagramas de Fluxo de Dados

Nível 0

O nível 0, também denominado como *diagramas de contexto*, são uma representação geral da interação que os componentes têm entre si e entre entidades externas.

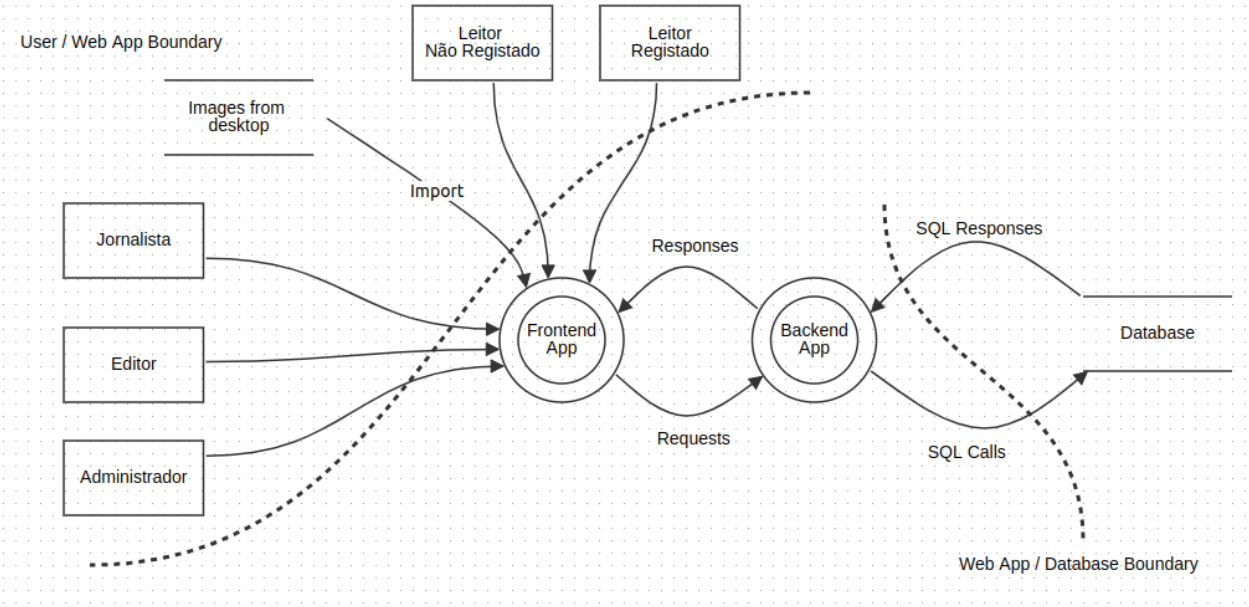


Figura 2 - DFD Level 0: Overview

Nivel 1

O nível 1 apresentam uma visão mais detalhada do sistema do que o anterior, mostrando os principais processos que, em conjunto, formam o sistema.

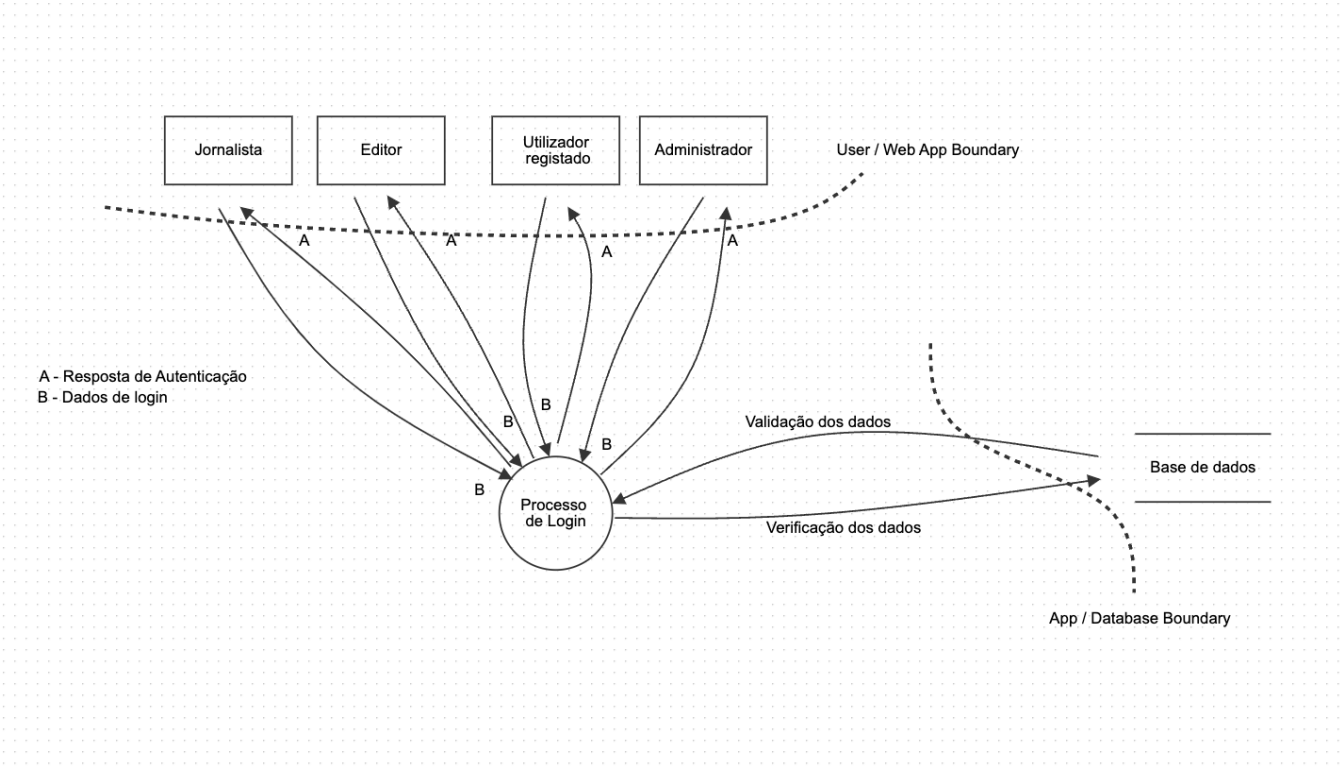


Figura 3 - DFD Nivel 1: Login

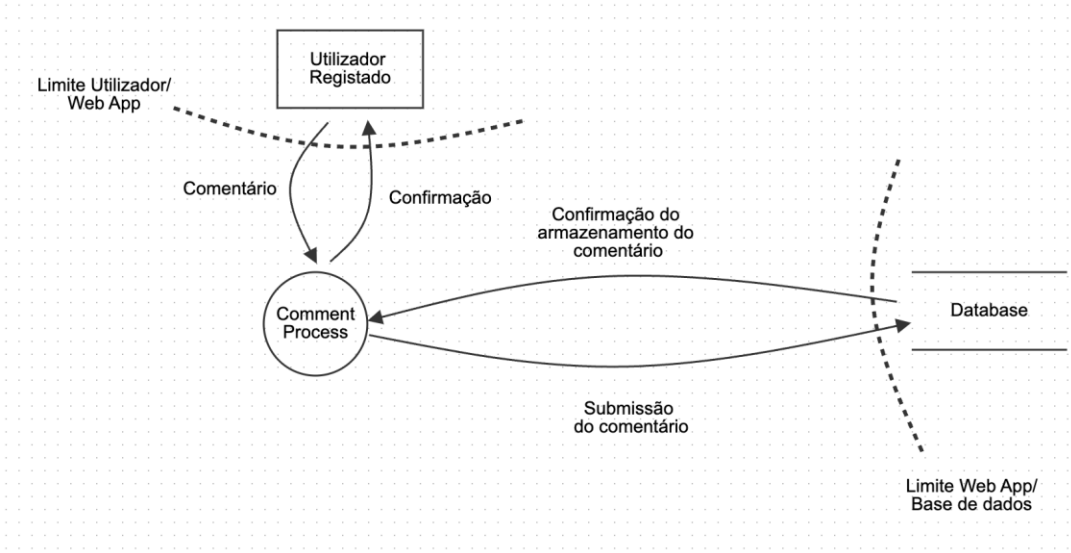


Figura 4 - DFD Nível 1: Comentários

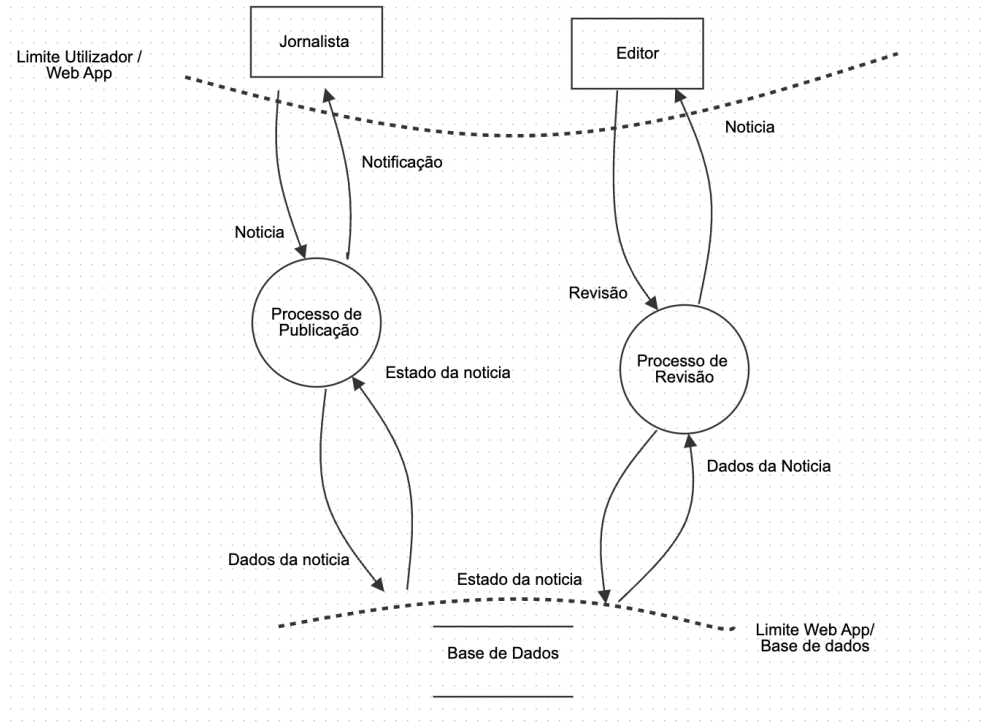


Figura 5 - DFD Nível 1: Publicação de notícias

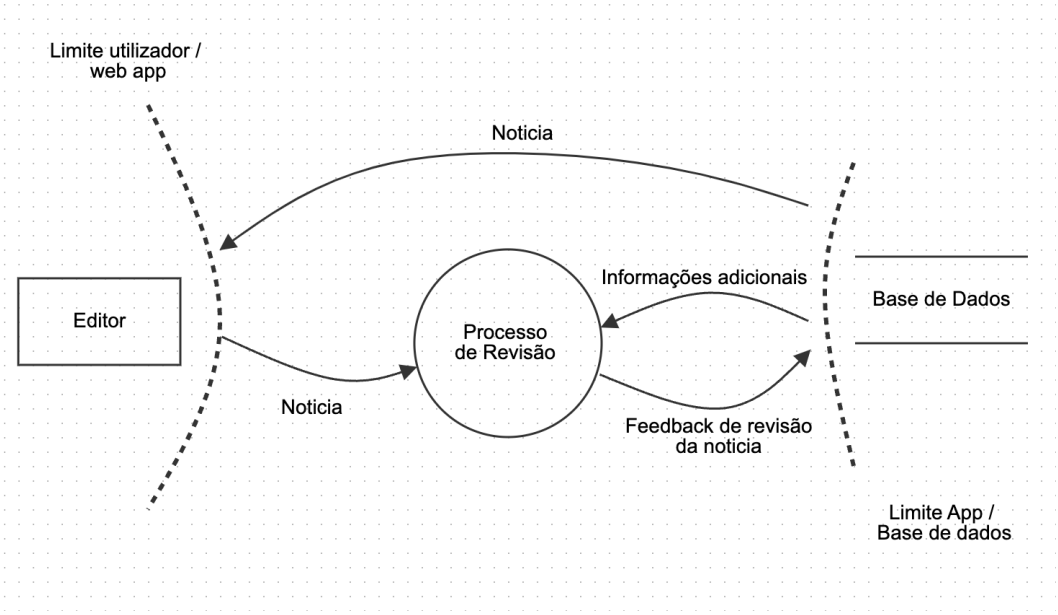


Figura 6 - DFD Nível 1: Revisão de notícias

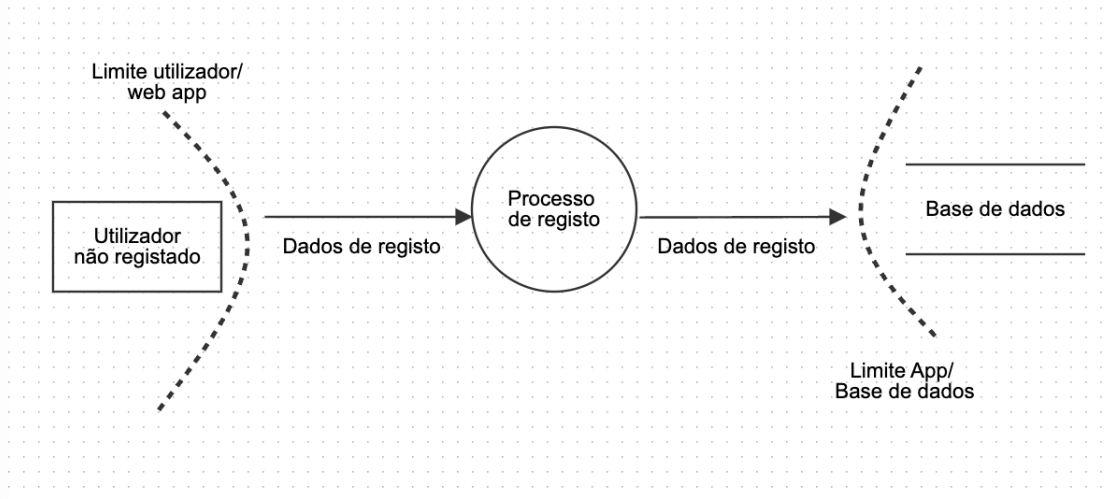


Figura 7 - DFD Nível 1: Registo

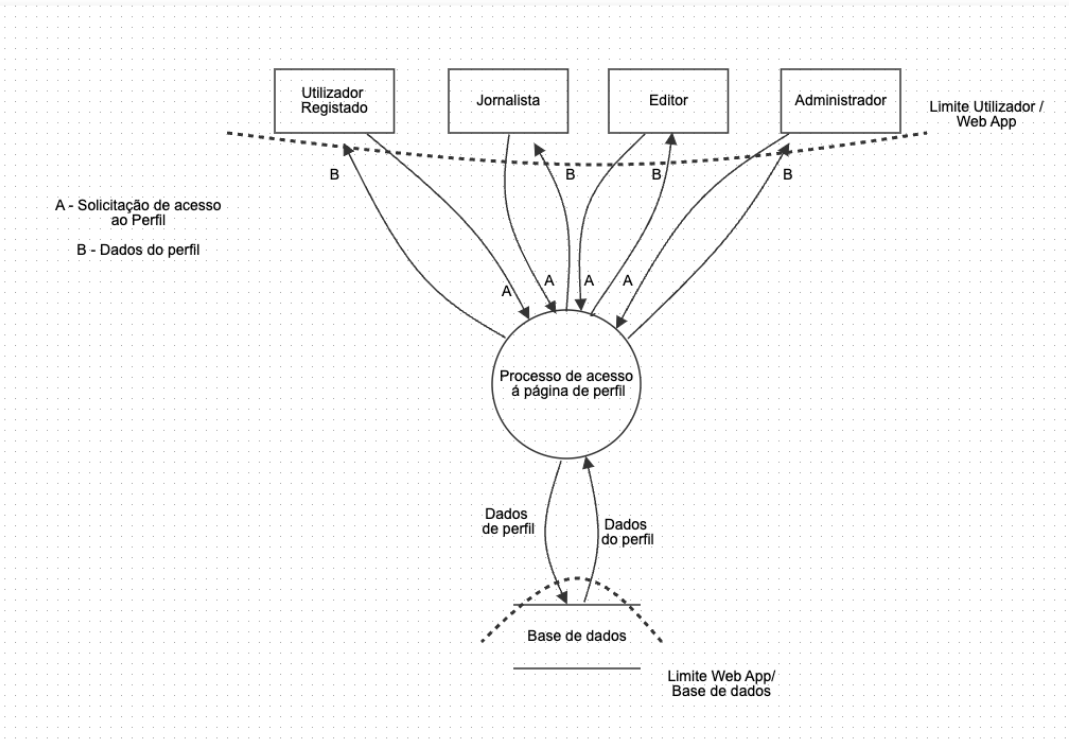


Figura 8 - DFD Nível 1: Perfil

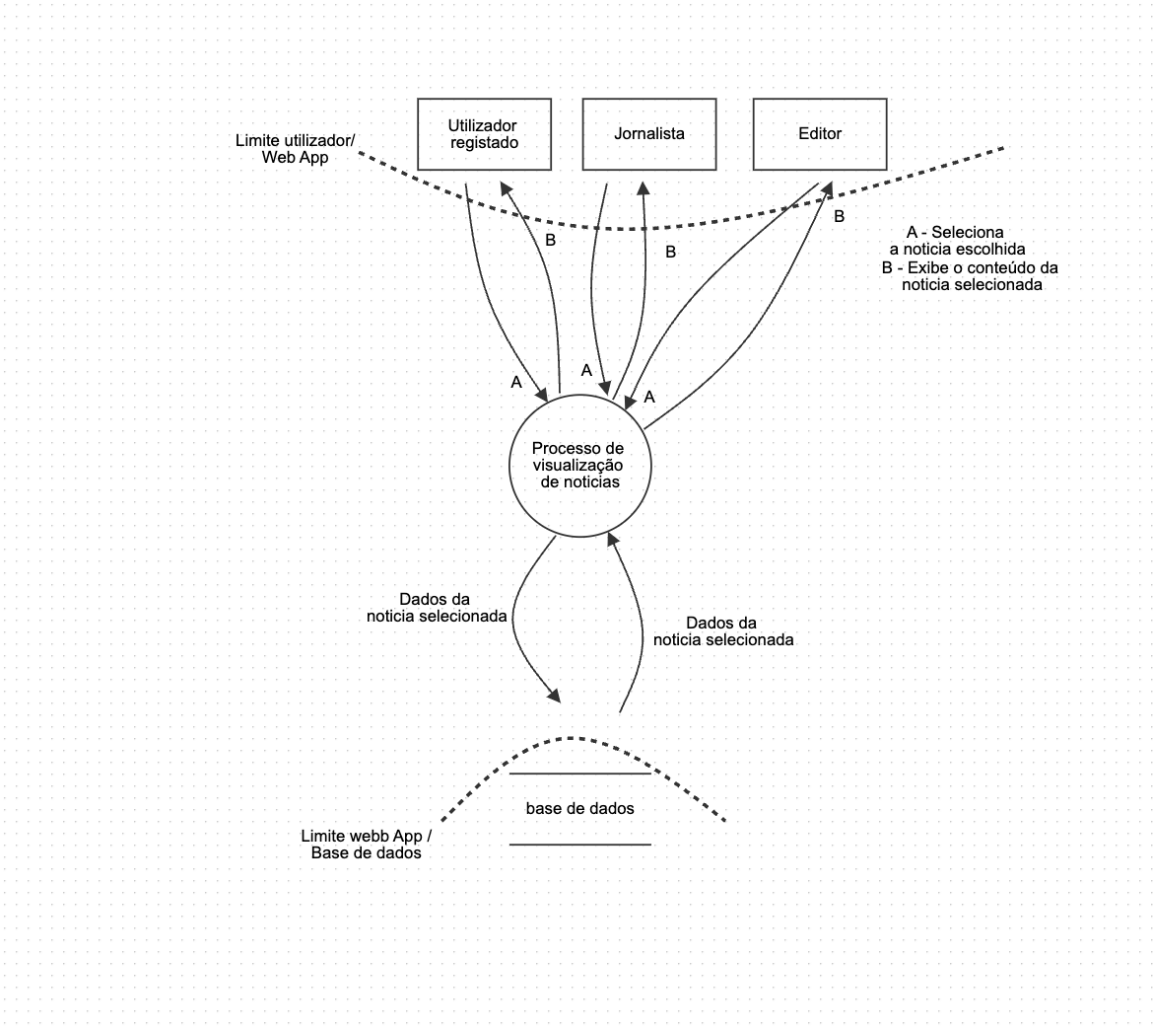


Figura 9 - DFD Nível 1: Visualizar noticias

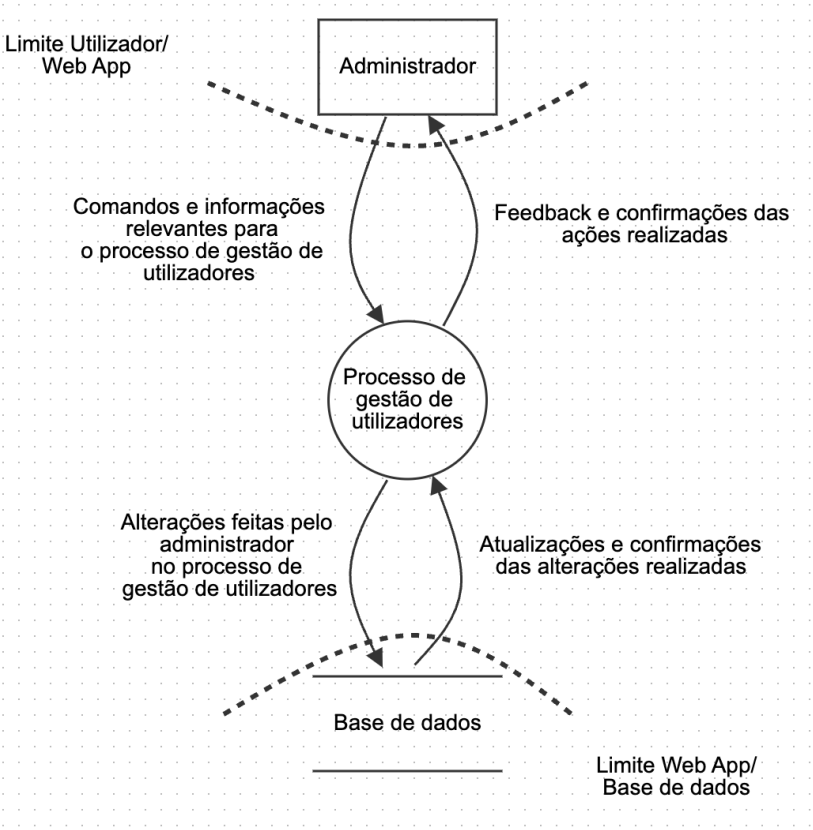


Figura 10 - DFD Nível 1: Gestão de utilizadores

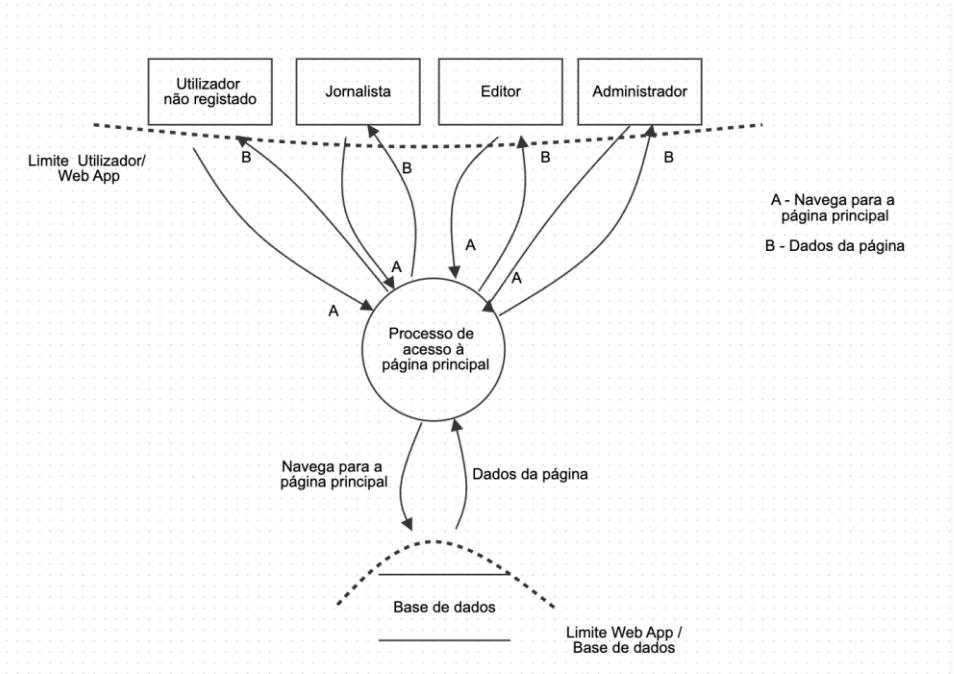


Figura 11- DFD Nível 1: Página principal

STRIDE

A tabela STRIDE é um modelo de segurança estruturado que serve para identificar e categorizar as ameaças à segurança de sistemas informáticos. O acrónimo STRIDE representa seis diferentes tipos de ameaças: *Spoofing* (falsificação de identidade), *Tampering* (adulteração de dados), *Repudiation* (negação de ações realizadas), *Information Disclosure* (divulgação de informações), *Denial of Service* (negação de serviço) e *Elevation of Privilege* (elevação de privilégios). Este modelo é particularmente útil durante o desenho e a análise de sistemas, fornecendo uma abordagem metódica para a identificação de possíveis vulnerabilidades e para o desenvolvimento de estratégias de mitigação adequadas.

A pertinência de aplicar a tabela STRIDE deriva da sua capacidade para sistematizar a análise de segurança, permitindo uma visão abrangente e detalhada das potenciais falhas de segurança em diferentes componentes de um sistema. Para cada Diagrama de Fluxo de Dados (DFD) criado, uma tabela STRIDE correspondente será elaborada.

Nível 0 – Componente da Aplicação

Na Tabela , está a representar a análise STRIDE para o *Data Flow Diagram* de nível 0.Tabela 2

Tabela 5 - STRIDE - Nível 0: Componente da Aplicação

Categoria	**Propriedade violada**	**Descrição**
Spoofing	Autenticação	1. A aplicação precisa de ser facilmente acedida pelos seus utilizadores. Apesar desta necessidade, os processos de autenticação como login não se podem tornar vulneráveis a ameaças.
Tampering	Integridade	2. Os utilizadores podem alterar as suas credenciais. Estes dados apenas podem ser alterados pelo próprio utilizador. 3. Os jornalistas podem publicar notícias (após estas serem aprovadas). Existe a ameaça de as notícias serem alteradas por um atacante.
Repudiation	Não-repudiação	Nenhuma ameaça identificada
Information Disclosure	Confidencialidade	4. Existe a ameaça de um atacante tentar obter as credenciais do utilizador para obter informação pessoal ou tentar obter informação à qual não deveria ter acesso.
Denial of Service	Disponibilidade	5. Existe a possibilidade de ataques de DDoS.
Elevation of Privilege	Autorização	Nenhuma ameaça identificada

Para Tabela 6 teve-se como base a Figura 3.

Tabela 6 - STRIDE - Nível 1: Login

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	6. O ato de autenticação é feito por uma por uma página de login. Existe a possibilidade de ataques de bruteforce às credenciais dos utilizadores. 7. Um atacante pode replicar a página web de log in, fazendo parecer a página legitima, na tentativa de obter as credenciais dos utilizadores que são enganados. 8. Interceção de palavra-passe durante a comunicação entre cliente e servidor
Tampering	Integridade	9. A aplicação persiste os seus dados numa base de dados, esta pode ser acedida diretamente caso o atacante tenha as credenciais de administrador
Repudiation	Não-repudiação	10. Nenhuma ameaça identificada
Information Disclosure	Confidencialidade	11. Exposição de detalhes sensíveis dos utilizadores ou informações confidenciais devido a falhas na segurança da autenticação.
Denial of Service	Disponibilidade	12. Sobrecarga intencional do sistema de login através de ataques de força bruta ou distribuídos (DDoS), comprometendo a disponibilidade do serviço para utilizadores legítimos.
Elevation of Privilege	Autorização	13. Exploração de vulnerabilidades no sistema de login para obter privilégios não autorizados, potencialmente dando a um atacante acesso a funcionalidades restritas a administradores ou editores

Na Tabela 7 compreende-se a Figura 4.

Tabela 7 - STRIDE - Nível 1: Comentários

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	14. Utilização indevida de uma conta de utilizador registado para postar comentários maliciosos ou difamatórios.
Tampering	Integridade	15. Alteração de comentários enviados por utilizadores após a submissão, antes de serem

		armazenados na base de dados.
Repudiation	Não-repudiação	16. Inexistência de registos de auditoria para ações de comentários, impossibilitando a prova da origem de um comentário específico.
Information Disclosure	Confidencialidade	Nenhuma ameaça identificada.
Denial of Service	Disponibilidade	17. Ataques que inundem o processo de comentários com tráfego excessivo, impedindo o funcionamento normal e a postagem de comentários legítimos.
Elevation of Privilege	Autorização	Nenhuma ameaça identificada

No caso da Tabela 8, associa-se à Figura 5.

Tabela 8 - STRIDE - Nível 1: Publicação de Notícias

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	18. Acesso não autorizado ao sistema com a utilização de credenciais de jornalista ou editor para postar notícias falsas ou manipuladas.
Tampering	Integridade	19. Alteração não autorizada no conteúdo ou no estado de notícias durante o processo de publicação ou revisão, comprometendo a veracidade da informação.
Repudiation	Não-repudiação	20. Ausência de registo detalhado das alterações feitas nos dados da notícia, permitindo a jornalistas ou editores negar alterações realizadas.
Information Disclosure	Confidencialidade	21. Vazamento de informações confidenciais de rascunhos ou notícias pendentes de revisão, devido a falhas na segurança da base de dados.
Denial of Service	Disponibilidade	22. Sobrecarga dos processos de publicação ou revisão de notícias, seja intencional ou acidental, que possa impedir a operação normal da aplicação.
Elevation of Privilege	Autorização	23. Explotação de vulnerabilidades no processo de revisão para permitir que um jornalista publique notícias sem a aprovação necessária do editor.

No caso da Tabela 9, representa o STRIDE associado à Figura 6

Tabela 9 - STRIDE - Nível 1: Revisão de Notícias

Categoria	Propriedade violada	Descrição

Spoofing	Autenticação	24. Acesso indevido ao sistema de revisão através da usurpação da identidade de um editor legítimo para alterar ou publicar notícias.
Tampering	Integridade	25. Modificação das notícias ou do feedback de revisão na base de dados ou durante a transmissão da informação para o editor, resultando em conteúdo inautêntico ou incorreto.
Repudiation	Não-repudiação	26. Falta de mecanismos de rastreio e registo das alterações efetuadas no conteúdo das notícias, o que permite aos editores negar modificações feitas por eles.
Information Disclosure	Confidencialidade	Nenhuma ameaça identificada.
Denial of Service	Disponibilidade	27. Ataques que miram sobrecarregar o processo de revisão, como a inundação do sistema com múltiplas submissões simultâneas, impactando a capacidade de processar revisões de forma eficiente.
Elevation of Privilege	Autorização	28. Abuso de permissões no sistema de revisão que permite a um utilizador com privilégios menores editar ou aprovar notícias sem as devidas permissões.

Para Tabela 10, teve-se como base o DFD presente na Figura 7.

Tabela 10 - STRIDE - Nível 1: Registo

Categoria	**Propriedade violada**	**Descrição**
Spoofing	Autenticação	29. Criação de contas utilizando identidades falsas ou dados roubados. 30. Registo de utilizadores não autorizados que pretendem mascarar a sua verdadeira identidade.
Tampering	Integridade	31. Alteração dos dados de registo submetidos por um utilizador ou já armazenados na base de dados. 32. Injeção de SQL através dos campos de registo para modificar ou corromper a base de dados.
Repudiation	Não-repudiação	33. 5. Inexistência de registos de auditoria para as ações de registo, o que permite aos utilizadores negar a criação de contas ou alterações feitas.
Information Disclosure	Confidencialidade	34. Divulgação dos dados de registo dos utilizadores durante o processo de registo ou devido a acessos indevidos à base de dados.

Denial of Service	Disponibilidade	35. Sobrecarga do processo de registo com solicitações em massa, o que pode tornar o serviço indisponível para utilizadores legítimos.
Elevation of Privilege	Autorização	36. Ganho de acesso não autorizado a funcionalidades da aplicação durante ou após o processo de registo devido a falhas no sistema de controlo de acesso.

Na Tabela 11, corresponde o DFD ilustrado na Figura 8.

Tabela 11 - STRIDE - Nível 1: Perfil

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	37. Acesso não autorizado ao perfil de outro utilizador mediante o uso de credenciais roubadas ou falsificação de sessão.
Tampering	Integridade	38. Modificação não autorizada dos dados do perfil, como email ou password, na base de dados ou durante a sua transmissão.
Repudiation	Não-repudiação	39. Ausência de registo de operações efetuadas no perfil que possibilite a um utilizador negar alterações indevidas.
Information Disclosure	Confidencialidade	40. Exposição de dados pessoais dos perfis dos utilizadores, incluindo informações sensíveis, através de falhas de segurança na base de dados ou na aplicação.
Denial of Service	Disponibilidade	41. Ataques direcionados ao processo de acesso ao perfil que podem sobrecarregar o sistema, tornando-o inacessível para utilizadores legítimos.
Elevation of Privilege	Autorização	42. Exploração de vulnerabilidades no controle de acesso que permite a um utilizador obter permissões de outro tipo de utilizador, como editor ou administrador.

Tendo em conta o DFD presente na Figura 9, elaborou-se a Tabela 12.

Tabela 12 - STRIDE - Nível 1: Visualizar notícias

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	43. Utilização de credenciais falsas para aceder como jornalista ou editor e visualizar notícias restritas ou em fase de edição.
Tampering	Integridade	44. Alteração maliciosa dos dados da notícia na

		base de dados ou durante a sua visualização, o que pode resultar na difusão de informação incorreta.
Repudiation	Não-repudiação	45. Falta de mecanismos de log que registem o acesso a notícias e ações realizadas por utilizadores, jornalistas ou editores, permitindo negar visualizações ou alterações.
Information Disclosure	Confidencialidade	46. Acesso não autorizado a notícias ainda não publicadas, devido a falhas na restrição de acesso ou na encriptação dos dados.
Denial of Service	Disponibilidade	47. Ataques que sobrecarreguem o sistema, como um flood de pedidos de visualização, impedindo o acesso legítimo às notícias.
Elevation of Privilege	Autorização	48. Manipulação do sistema para obter permissões de visualização não concedidas, como um utilizador não registado a aceder conteúdo exclusivo para utilizadores registados.

Com a Tabela 13, encontra-se representado o STRIDE associado ao DFD da Figura 10.

Tabela 13 - STRIDE - Nível 1: Gestão de utilizadores

Categoria	**Propriedade violada**	**Descrição**
Spoofing	Autenticação	49. Imitação de um administrador por um atacante para obter controle sobre as contas dos utilizadores.
Tampering	Integridade	50. Modificação não autorizada nas informações dos utilizadores, incluindo permissões, por um atacante com acesso à base de dados.
Repudiation	Não-repudiação	51. Falta de registos adequados das ações de gestão, impedindo a rastreabilidade das alterações feitas pelos administradores.
Information Disclosure	Confidencialidade	52. Acesso indevido a informações pessoais e confidenciais dos utilizadores durante o processo de gestão.
Denial of Service	Disponibilidade	53. Ataques que visam sobrecarregar o processo de gestão de utilizadores, impedindo os administradores de realizar as suas funções.
Elevation of Privilege	Autorização	54. Exploração de falhas no processo de gestão para elevar privilégios de um utilizador comum a níveis administrativos.

Com a Figura 11, procedeu-se à elaboração da Tabela 14.

Tabela 14 - STRIDE - Nível 1: Página Principal

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	55. Acesso à página principal com credenciais de utilizador não autorizadas, podendo levar à visualização de informações restritas.
Tampering	Integridade	56. Modificação dos dados que aparecem na página principal, alterando notícias ou conteúdo apresentado aos utilizadores.
Repudiation	Não-repudiação	57. Ausência de registos de atividade que possibilite confirmar se um utilizador visualizou ou modificou o conteúdo da página principal.
Information Disclosure	Confidencialidade	Nenhuma ameaça identificada.
Denial of Service	Disponibilidade	58. Ataques que impeçam o carregamento da página principal ou sobrecarreguem o sistema, negando acesso aos utilizadores.
Elevation of Privilege	Autorização	59. Aproveitamento de vulnerabilidades na aplicação que permita a um utilizador não registado ou a um jornalista aceder a funcionalidades administrativas na página principal.

Nas tabelas 15 está registada a analise STRIDE á dependência do sistema ao sistema de autenticação

Tabela 15 - STRIDE - Auth0

Categoria	Propriedade violada	Descrição
Spoofing	Autenticação	60. Tentativa de obtenção de dados de um utilizador na comunicação entre o sistema e o sistema externo de autenticação
Tampering	Integridade	61. Alteração aos dados de login do utilizador com vista em impedir este de se autenticar no sistema
Repudiation	Não-repudiação	62. A inexistência de forma de identificar as alterações efetuadas a dados de login de utilizador.
Information Disclosure	Confidencialidade	63. Inexistência ou insuficiência de encriptação dos dados trocados entre o sistema e o sistema Auth0
Denial of Service	Disponibilidade	64. Sobrecarga intencional do sistema externo de login para negar a o acesso a este sistema
Elevation of Privilege	Autorização	Nenhuma ameaça identificada

Casos de Uso e Abuso

Os casos de uso descrevem como os utilizadores interagem com um sistema para alcançar objetivos específicos de maneira legítima e esperada. Eles fornecem uma representação clara e visual das interações entre os usuários e o sistema, ajudando a capturar requisitos de forma compreensível.

Por outro lado, os casos de abuso representam interações maliciosas ou não autorizadas que utilizadores ou agentes externos podem tentar realizar com o sistema. Eles descrevem cenários nos quais o sistema pode ser explorado de maneira prejudicial, seja através de violações de segurança, manipulação de dados ou uso indevido de funcionalidades.

Ao identificar tanto os casos de uso quanto os casos de abuso durante o processo de engenharia de requisitos, podemos projetar sistemas mais seguros e robustos, para mitigar potenciais vulnerabilidades e protegendo contra ameaças.

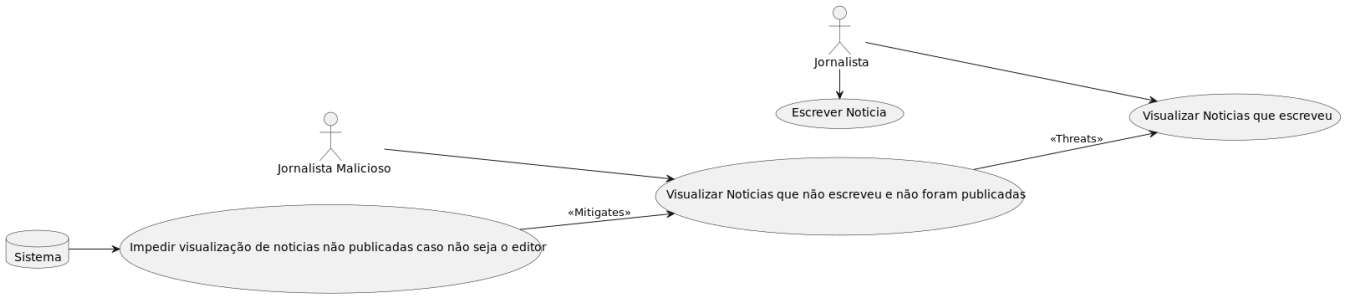


Figura 9 Jornalista Malicioso visualizar notícias que não foram publicadas de outros jornalistas

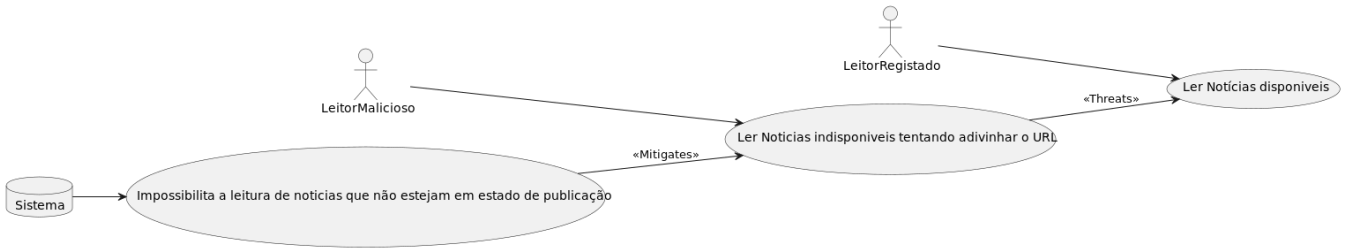


Figura 10 Leitor Malicioso lê notícias que não tem acesso

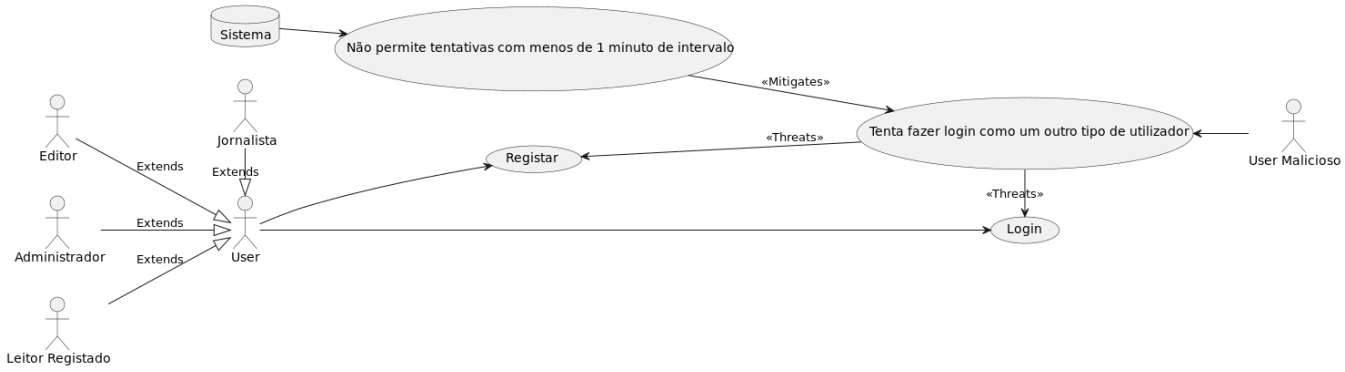


Figura 11 Obter acessos indevidos

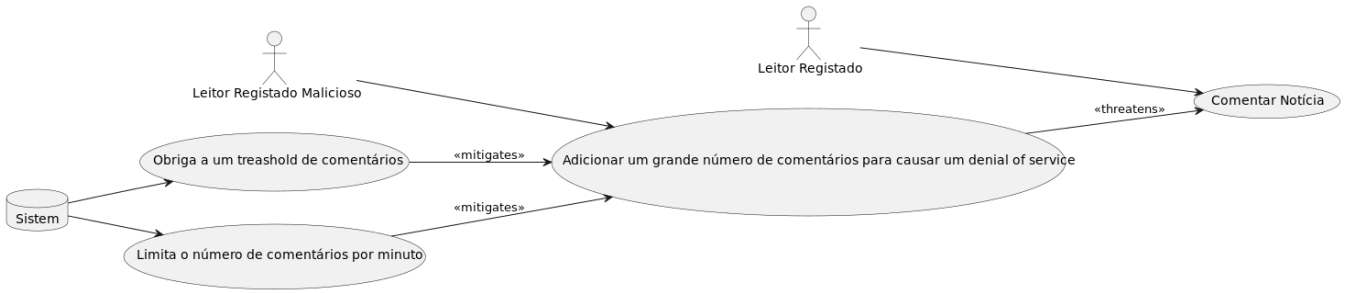


Figura 12 DOS através de comentários

Classificação de Ameaças

A classificação de ameaças desempenha um papel fundamental na compreensão dos riscos e na implementação de medidas adequadas de proteção. Ao identificarmos e classificarmos as ameaças potenciais, podemos priorizar os esforços de segurança e adotar estratégias eficazes para mitigar esses riscos. Destacamos algumas categorias comuns de ameaças e suas implicações:

1 º - Ameaças que visam o acesso ao servidor/sistema, pois com total acesso do mesmo consegue-se ter total controlo de toda aplicação e dados. Na tabela STRIDE isto é tipicamente aplicado às ameaças de acesso privilegiado.

2º - Ameaças que coletam dados pessoais, pois compreende-se que as informações pessoais são as mais importantes. Predominantemente *Spoofing* e confidencialidade destes mesmos.

3º - *Denial of Service* pois sem os serviços UP não existe continuidade de negócio.

4º - Integridade garantir que as informações exibidas são fidedignas, pois a sua falha, leva a graves impactos de reputação.

5º - Confidencialidade pois as notícias só devem ser demonstradas a utilizadores.

Mitigações e Contramedidas

A identificação de contramedidas visa verificar se existem medidas de proteção, como controles de segurança ou políticas, que possam impedir a materialização de uma ameaça. As vulnerabilidades representam ameaças sem contramedidas adequadas. Após categorizar as ameaças utilizando modelos como o STRIDE, é possível buscar contramedidas apropriadas para cada categoria identificada. Catálogos especializados oferecem abordagens para mitigar vulnerabilidades, apresentando uma variedade de opções para fortalecer a segurança dos sistemas informáticos e salvaguardar contra riscos potenciais.

Considerando os requisitos de segurança delineados anteriormente, é possível atenuar e prevenir ameaças em cada camada do sistema. Essas medidas garantem defesa contra *Spoofing*, incluindo ataques que visam a obtenção de credenciais por meio de ataques de força bruta ou explorando falhas em protocolos inseguros para acesso indevido a credenciais de terceiros. Tais medidas fortalecem a integridade dos dados, assegurando que os acessos às contas sejam realizados apenas por usuários legítimos, reduzindo as vulnerabilidades que poderiam permitir a um atacante a alteração não autorizada de informações. Através do tratamento de erros e do registo detalhado de eventos (*logging*), enfrentam-se os desafios relacionados ao repúdio, registando de forma confiável as ações realizadas, proporcionando prova incontestável das atividades dos usuários no sistema. Além disso, são delineados mecanismos que reduzem a probabilidade de interrupção do serviço e o acesso não autorizado a privilégios.

Ameaças que visam o acesso ao servidor/sistema (1º) :

- **Mitigações:**
  - Implementar uma política de controlo de acesso baseada no princípio do menor privilégio.
  - Utilizar autenticação multifatorial para reforçar a autenticação.
  - Criptografar dados sensíveis para proteger contra acessos não autorizados.
- **Contramedidas:**
  - Utilizar firewalls e sistemas de detecção de intrusões para monitorizar e controlar o tráfego de rede.
  - Implementar sistemas de gerenciamento de identidade e acesso (IAM) para garantir que apenas utilizadores autorizados tenham acesso aos recursos.
  - Implementar monitoramento contínuo de eventos de segurança para detetar e responder a atividades suspeitas.

Ameaças que coletam dados pessoais (2º) :

- **Mitigações:**
  - Criptografar dados pessoais armazenados para proteger contra acesso não autorizado.
  - Implementar controlos de acesso rigorosos para limitar o acesso a dados pessoais apenas a usuários autorizados.
  - Educar os funcionários do jornal sobre práticas seguras de manipulação de dados pessoais.
- **Contramedidas:**
  - Implementar técnicas de deteção de *spoofing* para identificar e mitigar tentativas de falsificação de identidade.
  - Implementar políticas de privacidade claras e transparentes para garantir o tratamento adequado de dados pessoais.
  - Utilizar sistemas de prevenção de perda de dados (DLP) para monitorizar e proteger dados pessoais contra *leaks* de dados não autorizados.

Denial of Service (Negacão de Serviço) (3º) :

- Mitigações:
  - Utilizar serviços de mitigação de DDoS (Distributed Denial of Service) para filtrar tráfego prejudicial antes que ele atinja a infraestrutura principal.
  - Implementar sistemas de redundância e balanceamento de carga para mitigar o impacto de ataques de negação de serviço.
  - Monitorização proativa da disponibilidade de serviços para identificar e responder rapidamente a anomalias no sistema.
- Contramedidas:
  - Implementar sistemas de detecção de intrusões (IDS) para identificar e bloquear ataques de negação de serviço.
  - Utilizar serviços de proteção DDoS fornecidos por provedores de nuvem ou terceiros especializados.
  - Configurar firewalls para limitar o tráfego prejudicial e proteger contra ataques de negação de serviço.

Integridade dos dados (4º) :

- Mitigações:
  - Implementar sistemas que controlem a integridade para detectar e responder a alterações não autorizadas nos dados.
  - Utilizar assinaturas digitais para verificar a autenticidade e integridade dos dados transmitidos.

- Criptografar dados sensíveis para proteger contra alterações não autorizadas.

- Contramedidas:
  - Implementar controlos de acesso rigorosos para garantir que apenas utilizadores autorizados possam modificar os dados.
  - Utilizar sistemas de detecção de intrusões para identificar e responder a tentativas de alteração não autorizada de dados.
  - Realizar backups regulares dos dados para restauração em caso de comprometimento da integridade dos dados.

Confidencialidade das informações (5º) :

- Mitigações:
  - Utilizar técnicas de criptografia para proteger dados confidenciais.
  - Implementar políticas de controle de acesso baseadas em função para restringir o acesso a informações confidenciais.
  - Educar os funcionários sobre a importância da segurança da informação e práticas adequadas de compartilhamento de informações.
- Contramedidas:
  - Implementar sistemas de prevenção de perda de dados (DLP) para monitorar e proteger dados confidenciais contra vazamentos não autorizados.
  - Utilizar sistemas de criptografia de ponta a ponta para proteger a confidencialidade das comunicações.
  - Implementar mecanismos de controle de acesso granular para garantir que apenas usuários autorizados tenham acesso a informações confidenciais.

Perfil de Ameaças

Após a análise das ameaças e as suas respetivas mitigações ser realizada, é possível identificar que o perfil de ameaças é: Ameaças parcialmente mitigadas.

Todas as ameaças possuem uma ou mais medidas de mitigação, mas existe sempre a possibilidade, independente do quão mínimo seja o impacto, as ameaças podem ainda assim ser exploradas. Tendo em conta que a aplicação é dependente de tecnologias desenvolvidas por terceiros, existe sempre a possibilidade de uma ameaça ser exposta pela tecnologia e ser explorada na aplicação.

Conclusão

Em suma, este relatório abordou detalhadamente o ciclo de vida de desenvolvimento de software seguro, com máxima atenção na importância de implementar medidas de segurança robustas em todas as fases do processo. Desde a análise das ameaças até a definição de requisitos funcionais e não funcionais, cada etapa foi cuidadosamente planejada para garantir a integridade e a confidencialidade do sistema.

Os principais pontos enfatizados incluem a necessidade de uma autenticação segura, controle de acesso adequado, criptografia de dados e gerenciamento de sessões seguras. Além disso, a abordagem de ameaças como *spoofing*, *tampering*, *repudiation*, *information disclosure*, *denial of service* e *elevation of privilege* foi discutida em detalhes, juntamente com as contramedidas correspondentes para mitigar esses riscos.

Estas conclusões são essenciais porque destacam a importância de priorizar a segurança cibernética em todos os projetos de desenvolvimento de software. Investir em medidas de segurança desde o início do processo de desenvolvimento não apenas protege os sistemas contra ameaças potenciais, mas também fortalece a confiança dos usuários e a reputação da organização.

Em última análise, ao adotar uma abordagem proativa para a segurança de software, podemos minimizar os riscos de violações de dados e garantir que os sistemas permaneçam seguros e resilientes face de ameaças em constante evolução.

Referências

[1] OWASP, “Threat Modeling Process,” OWASP, [Online]. Available: https://owasp.org/www-community/Threat_Modeling_Process.