|  |  |  |  |
| --- | --- | --- | --- |
| A picture containing icon  Description automatically generated | | Curso de TeSP em  Programação de Sistemas de Informação  Tópicos de Segurança | |
|  |  | |  |
| **Ano Letivo 2024/2025** | **Av. Periódica** | | **1º Ano, 2º Semestre** |

|  |
| --- |
| **PROJETO DE TÓPICOS DE SEGURANÇA** |

**Relatório de Especificação de Requisitos do projeto de Tópicos de Segurança**

|  |  |  |
| --- | --- | --- |
| **Turno**: PL3 | **Grupo**: A (se aplicável) | **Docente**: Nuno Simões |
| **Nº 2241567** | Alexandre Conrado | |
| **Nº 2241572** | Diogo Soares | |
| **Nº 2241570** | Guilherme Silva | |

**Índice**

[1 Introdução 5](#_Toc67476478)

[2 Especificação do Sistema 6](#_Toc67476479)

[2.1 Especificação de Requisitos 6](#_Toc67476480)

[2.1.1 Requisitos Funcionais (RF) 6](#_Toc67476481)

[2.1.2 Requisitos Não Funcionais (RNF) 7](#_Toc67476482)

[2.1.3 Wireframes UI 14](#_Toc67476483)

[3 Conclusão 15](#_Toc67476484)

**Índice de tabelas**

[Tabela 1 Requisitos Funcionais 5](#_Toc67471061)

[Tabela 2 Requisitos Não Funcionais de Usabilidade 6](#_Toc67471062)

[Tabela 3 Requisitos Não Funcionais de Fiabilidade 7](#_Toc67471063)

[Tabela 4 Requisitos Não Funcionais de Segurança 8](#_Toc67471064)

[Tabela 5 Requisitos Não Funcionais de Eficiência 9](#_Toc67471065)

[Tabela 6 Requisitos Não Funcionais de Disponibilidade 10](#_Toc67471066)

[Tabela 7 Requisitos Não Funcionais de Ambiente 11](#_Toc67471067)

[Tabela 8 Requisitos Não Funcionais de Desenvolvimento 12](#_Toc67471068)

# Introdução

<Contextualizar o projeto>

# Especificação do Sistema

O problema abordado neste projeto é a necessidade de um chat seguro, que permita a comunicação entre clientes e servidor com proteção avançada contra interceções e alterações de dados. Atualmente, muitas soluções não garantem uma camada forte de segurança na transmissão de mensagens, deixando os utilizadores vulneráveis a possíveis ataques, como roubo de credenciais, falsificação de identidade e manipulação de mensagens e dados.

Para resolver este problema, o sistema proposto deve implementar técnicas avançadas de criptografia simétrica e assimétrica, garantindo que as mensagens que forem trocadas estejam protegidas contra acessos não autorizados. Além disso, a autenticação dos utilizadores e a validação de mensagens com assinaturas digitais são fundamentais para garantir a integridade das comunicações.

## Especificação de Requisitos

### Requisitos Funcionais (RF)

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RF-01 | O sistema deve permitir uma autenticação para o utilizador no servidor, garantindo a segurança das credenciais do utilizador. | Alta |  |
| RF-02 | Os clientes devem ser capazes de enviar e receber mensagens com segurança através de um sistema de criptografia. | Alta |  |
| RF-03 | O sistema deve conseguir validar a autenticidade das mensagens utilizando as assinaturas digitais. | Alta |  |
| RF-04 | O servidor deve conseguir aceitar várias ligações simultâneas de diversos clientes. | Alta |  |
| RF-05 | O cliente deve criar e enviar a chave pública para o servidor enquanto faz a conexão inicial. | Média |  |
| RF-06 | O cliente deve disponibilizar uma interface gráfica intuitiva e funcional para o fácil manuseio. | Média |  |
| RF-07 | O servidor deve ser capaz de armazenar com segurança a chave pública dos clientes para as suas futuras coneções. | Média |  |
| RF-08 | O servidor deve criar um ficheiro de logs incluindo todas as interações relevantes entre servidor e cliente. | Média |  |

Tabela 1 Requisitos Funcionais

### Requisitos Não Funcionais (RNF)

#### Requisitos Não Funcionais de Usabilidade

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-USA-01 | A interface gráfica do cliente deve ser uma interface intuitiva, para facilitar a interação do utilizador. | Alta |  |
| RNF-USA-02 | O sistema deve mostrar mensagens de erro e feedback ao utilizador assim que o mesmo faça uma ação. | Alta |  |
| RNF-USA-03 | A navegação dentro da aplicação deve ser uma navegação de fácil compreensão. | Média |  |

Tabela 2 Requisitos Não Funcionais de Usabilidade

#### Requisitos Não Funcionais de Fiabilidade

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-FIA-01 | O sistema deve conseguir se recuperar rapidamente após algum tipo de falha inesperada. | Alta |  |
| RNF-FIA-02 | O servidor deve manter uma estabilidade entre as conexões mesmo em situações de uma carga elevada | Média |  |

Tabela 3 Requisitos Não Funcionais de Fiabilidade

#### Requisitos Não Funcionais de Segurança

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-SEG-01 | O sistema deve conter uma criptografia assimétrica para a troca de chaves públicas. | Alta |  |
| RNF-SEG-02 | O sistema deve utilizar uma criptografia simétrica para proteger a confidencialidade das mensagens enviadas. | Alta |  |

Tabela 4 Requisitos Não Funcionais de Segurança

#### Requisitos Não Funcionais de Eficiência

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-EFI-01 | O sistema deve garantir um alto desempenho e um tempo de resposta rápido. | Alta |  |
| RNF-EFI-02 | A aplicação deve leve em nível de requisitos computacionais. | Média |  |

Tabela 5 Requisitos Não Funcionais de Eficiência

#### Requisitos Não Funcionais de Disponibilidade

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-DIS-01 | O servidor deve manter um tempo de atividade duradouro, assim evitará um período de inatividade. |  |  |
| RNF-DIS-02 | O sistema deve ser capaz de lidar com acessos simultâneos sem alterar e prejudicar a experiência do utilizador. |  |  |

Tabela 6 Requisitos Não Funcionais de Disponibilidade

#### Requisitos Não Funcionais de Ambiente

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-AMB-01 | O software deve ser compatível com os sistemas operativos do Windows. | Alta |  |
| RNF-AMB-02 | O código deve ser modular para permitir futuras expansões e alterações no mesmo. | Média |  |

Tabela 7 Requisitos Não Funcionais de Ambiente

#### Requisitos Não Funcionais de Desenvolvimento

<etapa II – marcar com um X na coluna “Implementado”>

|  |  |  |  |
| --- | --- | --- | --- |
| # ID | Descrição | Prioridade | Implementado |
| RNF-DES-01 | O código deve ser bem estruturado e bem documentado para providencial alguma futura manutenção. | Alta |  |
| RNF-DES-02 | A arquitetura do software deve permitir uma escalabilidade e uma adição de novas funcionalidades. | Alta |  |

Tabela 8 Requisitos Não Funcionais de Desenvolvimento

### Wireframes UI

Uma imagem com texto, captura de ecrã, diagrama, file

Os conteúdos gerados por IA poderão estar incorretos.

# Conclusão

<Apresentação de pontos importantes e conclusivos sobre o desenvolvimento do projeto>