|  |  |  |  |
| --- | --- | --- | --- |
| A picture containing icon  Description automatically generated | | Curso de TeSP em  Programação de Sistemas de Informação  Tópicos de Segurança | |
|  |  | |  |
| **Ano Letivo 2020/2021** | **Av. Periódica** | | **1º Ano, 2º Semestre** |

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

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

|  |  |  |
| --- | --- | --- |
| **Turno**: PL1 | **Grupo**: | **Docente**: Nuno Salvador |
| **Nº 2220852** | Francisco Sousa | |
| **Nº 2220859** | Rúben Gomes | |

**Índice**

[1 Introdução 4](#_Toc133064618)

[2 Especificação do Sistema 5](#_Toc133064619)

[2.1 Especificação de Requisitos 5](#_Toc133064620)

[2.1.1 Requisitos Funcionais (RF) 5](#_Toc133064621)

[2.1.2 Requisitos Não Funcionais (RNF) 6](#_Toc133064622)

[2.1.3 Wireframes UI 13](#_Toc133064623)

[3 Conclusão 15](#_Toc133064624)

**Índice de tabelas**

[Tabela 1 Requisitos Funcionais 5](#_Toc133064625)

[Tabela 2 Requisitos Não Funcionais de Usabilidade 6](#_Toc133064626)

[Tabela 3 Requisitos Não Funcionais de Fiabilidade 7](#_Toc133064627)

[Tabela 4 Requisitos Não Funcionais de Segurança 8](#_Toc133064628)

[Tabela 5 Requisitos Não Funcionais de Eficiência 9](#_Toc133064629)

[Tabela 6 Requisitos Não Funcionais de Disponibilidade 10](#_Toc133064630)

[Tabela 7 Requisitos Não Funcionais de Ambiente 11](#_Toc133064631)

[Tabela 8 Requisitos Não Funcionais de Desenvolvimento 12](#_Toc133064632)

# Introdução

No âmbito da Unidade Curricular de Tópicos de Segurança, foi-nos proposto como projeto desenvolver um chat com troca de mensagens de forma segura. O nosso trabalho vai ser dividido em dois módulos, o modulo do cliente e o módulo do servidor. Começando pelo desenvolvimento da interface gráfica e criação de formulários de login, depois avançando com a encriptação das mensagens e comunicação com a base de dados.

# Especificação do Sistema

Nesta secção é possível ver uma melhor descrição e especificação do sistema, ou seja, são representados os objetivos do projeto a realizar. Esta secção tem como principal objetivo explicar o que é o projeto.

## Especificação de Requisitos

### Requisitos Funcionais (RF)

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RF-01 | O sistema deve permitir trocar mensagens entre um cliente e um servidor | Alto |
| RF-02 | O sistema deve permitir trocar ficheiros em qualquer formato e tamanho entre um cliente e um servidor | Alto |
| RF-03 | O sistema deve permitir ao cliente enviar a sua chave publica | Alto |
| RF-04 | O sistema deve permitir ao cliente enviar e receber as mensagens de conversação de ficheiros | Alto |
| RF-05 | O sistema deve permitir ao servidor receber ligações de cliente | Alto |
| RF-06 | O sistema deve permitir ao servidor receber as mensagens ficheiros do cliente | Alto |
| RF-07 | O sistema deve permitir que o cliente se autentique | Alto |

Tabela 1 Requisitos Funcionais

### Requisitos Não Funcionais (RNF)

#### Requisitos Não Funcionais de Usabilidade

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-USA-01 | O sistema deve conter um módulo Cliente e um módulo Servidor | Alto |
| RNF-USA-02 | A UI deve ter um design simples intuitivo | Alto |
| RNF-USA-03 | A UI deve estar em português | médio |

Tabela 2 Requisitos Não Funcionais de Usabilidade

#### Requisitos Não Funcionais de Fiabilidade

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-FIA-01 | Em 1000 (por exemplo) conversações, o chat não deve falhar mais de 2 vezes | Alto |
| RNF-FIA-02 | O chat tem de estar disponível 24h/7dias | Alto |

Tabela 3 Requisitos Não Funcionais de Fiabilidade

#### Requisitos Não Funcionais de Segurança

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-SEG-01 | O sistema deve tornar todas as comunicações o mais seguras possíveis | Alto |
| RNF-SEG-02 | O sistema deve permitir ao cliente autenticar-se no servidor fornecendo as credenciais (username e password) | Alto |
| RNF-SEG-03 | O sistema deve validar todas as mensagens e ficheiros trocados com recurso a assinaturas digitais | Alto |
| RNF-SEG-04 | O servidor deve guardar a chave pública do cliente, na base de dados | Alto |
| RNF-SEG-05 | O servidor deve autenticar um utilizador já registado no sistema caso a verificação das credenciais seja correta | Alto |
| RNF-SEG-06 | O servidor deve validar as assinaturas do cliente | Alto |
| RNF-SEG-07 | O servidor ao receber a chave publica do cliente deve criar uma chave simétrica, cifrá-la com a chave pública do cliente e enviá-la | Alto |
| RNF-SEG-08 | O servidor deve verificar a entrada do cliente no chat com a chave simétrica | Alto |
| RNF-SEG-09 | O sistema deve criar um ficheiro .txt do sistema para guardar todos os dados processados pelo servidor | Alto |

Tabela 4 Requisitos Não Funcionais de Segurança

#### Requisitos Não Funcionais de Eficiência

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-EFI-01 | O tempo de resposta do sistema não deve ultrapassar 15 segundos | Alto |
| RNF-EFI-02 | O sistema deve suportar 2 utilizadores. | Alto |

Tabela 5 Requisitos Não Funcionais de Eficiência

#### Requisitos Não Funcionais de Disponibilidade

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-DIS-01 | O servidor deve estar disponível apenas para utilizadores registados que se autentiquem com sucesso | Alto |
| RNF-DIS-02 | O servidor deve estar disponível 24h/7dias | Alto |

Tabela 6 Requisitos Não Funcionais de Disponibilidade

#### Requisitos Não Funcionais de Ambiente

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-AMB-01 | O sistema deve funcionar no sistema operativo Windows | Alto |

Tabela 7 Requisitos Não Funcionais de Ambiente

#### Requisitos Não Funcionais de Desenvolvimento

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| RNF-DES-01 | Deverá ser utilizada a biblioteca ProtocolSI.dll | Alto |
| RNF-DES-02 | A linguagem de programação usada deve ser C# | Alto |
| RNF-DES-03 | Utilização de criptografia assimétrica | Alto |
| RNF-DES-04 | Utilização de criptografia simétrica | Alto |

Tabela 8 Requisitos Não Funcionais de Desenvolvimento

### Wireframes UI

Este Wireframe corresponde ao menu, ou seja, o ecrã principal da aplicação, no qual vai permitir dar login ou efetuar o registo na base dados.

Uma imagem com diagrama

Descrição gerada automaticamente

Figura 1 - Wireframe do menu principal

O wireframe da figura dois diz respeito a dois ecrãs, sendo esses, o do login e o do registo, estes são iguais mudando apenas o texto do botão, ou seja, dizendo “Registar” ou “Login”.

Uma imagem com diagrama

Descrição gerada automaticamente

Figura 2 - Wireframe do Registo/Login do utilizador

No wireframe seguinte, mostra o wireframe do próprio chat da aplicação, tem como indicar o utilizador que está conectado no canto superior esquerdo, mostra todo o chat da conversa e permite enviar a mensagem na caixa de texto que está na parte inferior do ecrã.

Uma imagem com texto

Descrição gerada automaticamente

Figura 3 - Wireframe do chat

# Conclusão

Para concluir este relatório, o grupo utilizou o conhecimento adquirido no semestre passado em Introdução à Análise e Projeto de Sistemas de Informação. A realização dos wireframes foi um processo rápido e simples, relativamente à especificação dos requisitos, foi algo mais complexo e demorado, no entanto, o objetivo foi alcançado com sucesso. Relativamente à aplicação que temos como objetivo realizar, que será um chat, temos boas expectativas devido às fichas que foram sendo realizadas ao longo das aulas.