|  |  |  |  |
| --- | --- | --- | --- |
| A picture containing icon  Description automatically generated | | Curso de TeSP em  Programação de Sistemas de Informação  Tópicos de Segurança | |
|  |  | |  |
| **Ano Letivo 2021/2022** | **Av. Periódica** | | **1º Ano, 2º Semestre** |

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

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

|  |  |  |
| --- | --- | --- |
| **Turno**: PL1/2 | **Grupo**: 3 | **Docente**: Iolanda Bernardino |
| **Nº 2213128** | Fábio Cabaceira | |
| **Nº 2211904** | Pedro Norberto | |
| **Nº 2211907** | Tiago Januário | |

**ÍNDICE**

[1 Introdução 5](#_Toc101550715)

[2 Especificação do Sistema 6](#_Toc101550716)

[2.1 Especificação de Requisitos 7](#_Toc101550717)

[2.1.1 Requisitos Funcionais (RF) 7](#_Toc101550718)

[2.1.2 Requisitos Não Funcionais (RNF) 8](#_Toc101550719)

[2.1.2.1 Requisitos Não Funcionais de Usabilidade 8](#_Toc101550720)

[2.1.2.2 Requisitos Não Funcionais de Fiabilidade 9](#_Toc101550721)

[2.1.2.3 Requisitos Não Funcionais de Segurança 10](#_Toc101550722)

[2.1.2.4 Requisitos Não Funcionais de Eficiência 12](#_Toc101550723)

[2.1.2.5 Requisitos Não Funcionais de Disponibilidade 12](#_Toc101550724)

[2.1.2.6 Requisitos Não Funcionais de Ambiente 13](#_Toc101550725)

[2.1.2.7 Requisitos Não Funcionais de Desenvolvimento 13](#_Toc101550726)

[2.1.3 Wireframes UI 14](#_Toc101550727)

[3 Conclusão 17](#_Toc101550728)

**ÍNDICE DE TABELAS**

[Tabela 1 - Requisitos Funcionais 7](#_Toc101550729)

[Tabela 2 - Requisitos Não Funcionais de Usabilidade 8](#_Toc101550730)

[Tabela 3 - Requisitos Não Funcionais de Fiabilidade 9](#_Toc101550731)

[Tabela 4 - Requisitos Não Funcionais de Segurança 11](#_Toc101550732)

[Tabela 5 - Requisitos Não Funcionais de Eficiência 12](#_Toc101550733)

[Tabela 6 - Requisitos Não Funcionais de Disponibilidade 12](#_Toc101550734)

[Tabela 7 - Requisitos Não Funcionais de Ambiente 13](#_Toc101550735)

[Tabela 8 - Requisitos Não Funcionais de Desenvolvimento 13](#_Toc101550736)

**ÍNDICE DAS ILUSTRAÇÕES**

[Figura 1 - Wireframe do Login 14](#_Toc101550737)

[Figura 2 - Wireframe do Registo 15](#_Toc101550738)

[Figura 3 - Wireframe da Zona Cliente 16](#_Toc101550739)

# Introdução

Este projeto consiste no desenvolvimento de um sistema de chat com troca de mensagens de uma forma segura, em C#. Onde vários clientes poderão aceder a este, através da sua conta pessoal.

# Especificação do Sistema

Como já referido, este sistema será um lugar onde utilizadores poderão enviar e receber mensagens de uma forma segura. Também terá outras funcionalidades como:

* Autenticação com uma conta pessoal;
* Possibilidade de criar uma conta nova;

A aplicação será composta por 2 módulos, estes sendo, o **módulo cliente** (com UI) e o **módulo servidor** (sem UI).

O **módulo cliente** pode:

* Enviar a sua chave pública;
* Autenticar-se no servidor fornecendo as credenciais;
* Enviar e receber as mensagens de conversação;
* Tornar todas as comunicações o mais seguras possível;
* Validar todas as mensagens trocados com recurso a assinaturas digitais;

Já no **módulo servidor**, este pode:

* Receber ligações de cliente;
* Guardar a chave pública do cliente;
* Autenticar um utilizador já registado no sistema;
* Validar as assinaturas do cliente;
* Enviar e receber as mensagens de conversação de forma segura;
* Receber e processar os dados relativos às mensagens de forma segura;

## Especificação de Requisitos

### Requisitos Funcionais (RF)

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RF-01** | O cliente deve ter a possibilidade de enviar e receber mensagens na conversa | Alta |
| **RF-03** | As comunicações devem ser o mais seguras possíveis | Alta |
| **RF-04** | O sistema deve permitir que o utilizador se autentique no sistema. | Alta |
| **RF-05** | O sistema deve permitir que o utilizador crie uma conta nova | Alta |

Tabela 1 - Requisitos Funcionais

### Requisitos Não Funcionais (RNF)

#### Requisitos Não Funcionais de Usabilidade

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-USA-01** | A interface deve ser user-friendly e fácil de usar | Alta |
| **RNF-USA-02** | Os utilizadores devem ser corretamente informados de como efetuar as operações que pretendem para evitar a ocorrência de erros | Média |
| **RNF-USA-03** | O sistema deve ordenar as mensagens por data de envio | Alta |
| **RNF-USA-04** | O Sistema deverá ter a capacidade de alternar entre light mode e dark mode | Baixa |
| **RNF-USA-05** | O sistema deverá ter a capacidade de dar oportunidade ao utilizador de criar o seu próprio tema (alterar as cores) | Baixa |
| **RNF-USA-06** | Deve ser possível fazer qualquer funcionalidade com o máximo de 4 cliques do rato | Baixa |
| **RNF-USA-07** | Todos os botões devem ter as mesmas características a nível de cor e tamanho | Média |
| **RNF-USA-08** | Todas as funcionalidades do sistema devem poder ser acedidas não só com o rato, mas também com o teclado | Média |

Tabela 2 - Requisitos Não Funcionais de Usabilidade

#### Requisitos Não Funcionais de Fiabilidade

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-FIA-01** | A aplicação deve apresentar as mensagens 97% das vezes | Alta |
| **RNF-FIA-02** | A aplicação deve correr sem interrupções 95% das vezes | Alta |
| **RNF-FIA-03** | O registo e login deve estar disponível 99% das vezes | Alta |

Tabela 3 - Requisitos Não Funcionais de Fiabilidade

#### Requisitos Não Funcionais de Segurança

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-SEG-01** | O módulo cliente deve enviar a sua chave pública ao servidor | Alta |
| **RNF-SEG-02** | O módulo cliente deve autenticar-se no servidor fornecendo as credenciais | Alta |
| **RNF-SEG-03** | O módulo cliente deve enviar e receber as mensagens de conversação | Alta |
| **RNF-SEG-04** | O módulo cliente deve tornar todas as comunicações o mais seguras possíveis | Alta |
| **RNF-SEG-05** | O módulo cliente deve validar todas as mensagens trocados com recurso a assinaturas digitais | Alta |
| **RNF-SEG-06** | O módulo cliente deve enviar os dados de autenticação cifrados com a chave simétrica | Alta |
| **RNF-SEG-07** | O módulo cliente entra no chat com a chave simétrica | Alta |
| **RNF-SEG-08** | O módulo servidor deve receber as ligações do cliente | Alta |
| **RNF-SEG-09** | O módulo servidor deve guardar a chave pública do cliente | Alta |
| **RNF-SEG-10** | O módulo servidor deve autenticar um cliente já registado no sistema | Alta |
| **RNF-SEG-11** | O módulo servidor deve validas as assinaturas do cliente | Alta |
| **RNF-SEG-12** | O módulo servidor deve enviar e receber as mensagens de conversação de forma segura | Alta |
| **RNF-SEG-13** | O módulo servidor deve receber e processar os dados relativos às mensagens de forma segura | Alta |
| **RNF-SEG-14** | O módulo servidor deve criar a chave simétrica, cifrá-la com a chave pública do cliente e enviar para o cliente | Alta |
| **RNF-SEG-15** | O módulo servidor deve verificar a entrada do cliente no chat com a chave simétrica | Alta |
| **RNF-SEG-16** | A base de dados deve ser protegida para acesso apenas de utilizadores autorizados | Alta |
| **RNF-SEG-17** | O sistema deve encriptar com o algoritmo de criptografia AES | Alta |
| **RNF-SEG-18** | O sistema deve-se proteger contra SQL Injection | Alta |
| **RNF-SEG-19** | No armazenamento das credenciais deverá ser utilizado um *salt* aleatório para cada utilizador | Alta |

Tabela 4 - Requisitos Não Funcionais de Segurança

#### Requisitos Não Funcionais de Eficiência

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-EFI-01** | A aplicação não deverá demorar mais de 30 segundos a apresentar uma nova mensagem ao utilizador | Média |
| **RNF-EFI-02** | O tempo de carregamento da aplicação não deve demorar mais que 1 segundo | Média |
| **RNF-EFI-03** | A aplicação deve suportar mais de 1000 utilizadores a enviarem mensagens | Baixa |
| **RNF-EFI-04** | O tempo de resposta do sistema não deve ultrapassar 30 segundos | Média |

Tabela 5 - Requisitos Não Funcionais de Eficiência

#### Requisitos Não Funcionais de Disponibilidade

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-DIS-01** | O sistema deve estar disponível para utilização 24 horas por dia, 7 dias por semana | Média |
| **RNF-DIS-02** | Qualquer falha que aparecer deve ser resolvida em menos de 5 horas | Média |

Tabela 6 - Requisitos Não Funcionais de Disponibilidade

#### Requisitos Não Funcionais de Ambiente

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-AMB-01** | A aplicação só poderá ser executada em Windows | Alta |

Tabela 7 - Requisitos Não Funcionais de Ambiente

#### Requisitos Não Funcionais de Desenvolvimento

|  |  |  |
| --- | --- | --- |
| # ID | Descrição | Prioridade |
| **RNF-DES-01** | A aplicação deve ser desenvolvida na linguagem de programação C# | Alta |
| **RNF-DES-02** | O sistema irá utilizar a framework .NET | Alta |
| **RNF-DES-02** | O tempo de desenvolvimento não deve ultrapassar os dias estabelecidos | Alta |
| **RNF-DES-03** | O sistema deverá utilizar a biblioteca ProtocolSI.dll | Alta |

Tabela 8 - Requisitos Não Funcionais de Desenvolvimento

### Wireframes UI

Todas as wireframes apresentadas a seguir podem ser visualizadas online a partir deste link:

<https://www.figma.com/proto/GjwffC0U6acLFcxuwqO70Y/Projeto-TPS?node-id=1%3A2&scaling=min-zoom&page-id=0%3A1&starting-point-node-id=1%3A2>

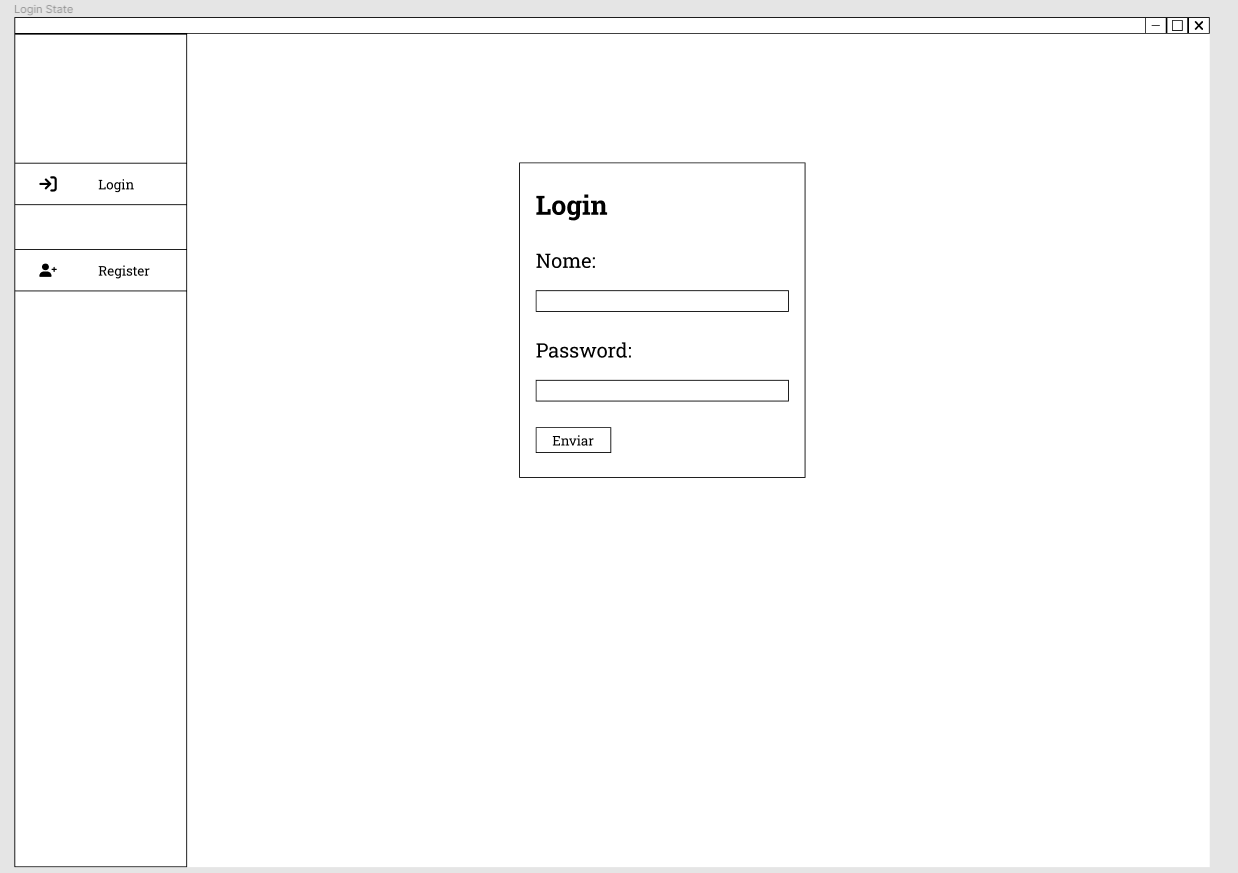


Figura 1 - Wireframe do Login

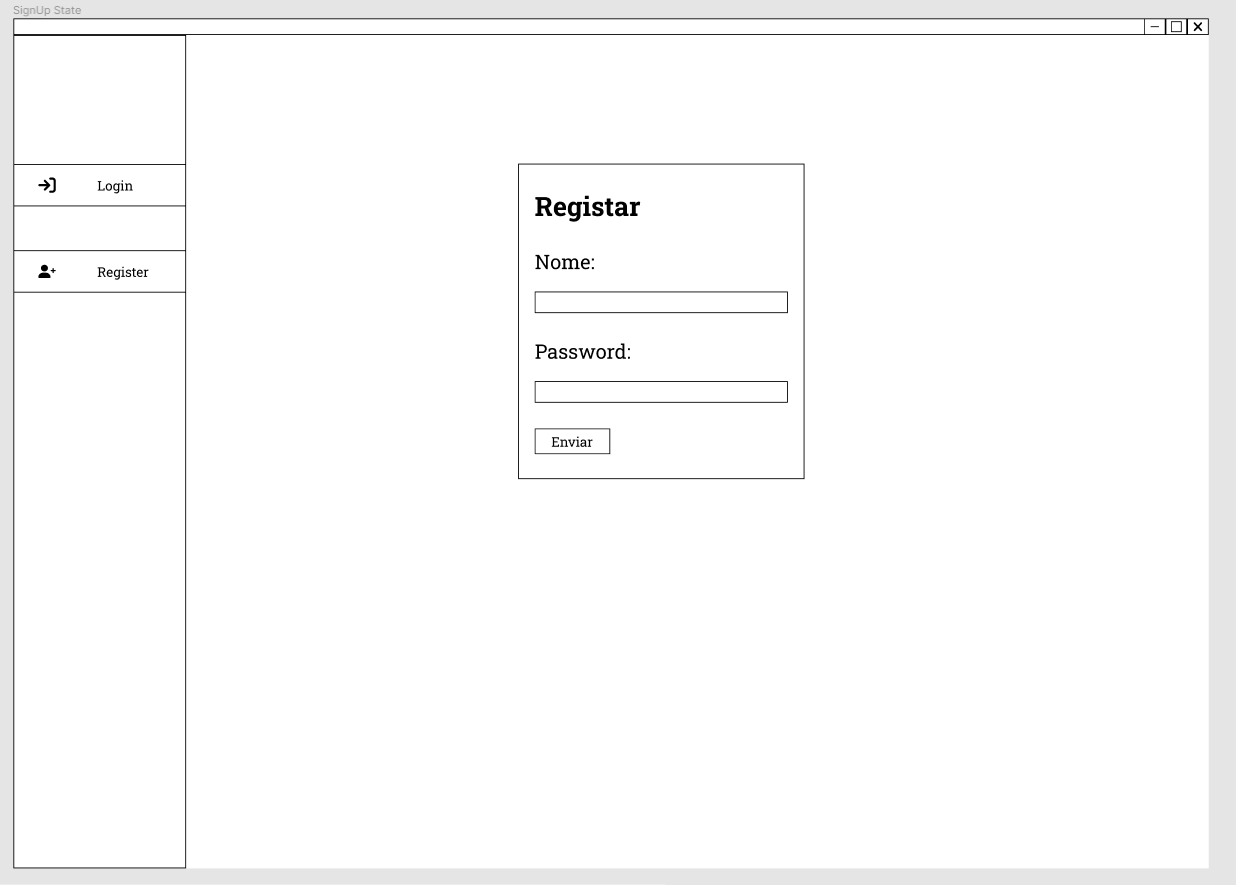


Figura 2 - Wireframe do Registo

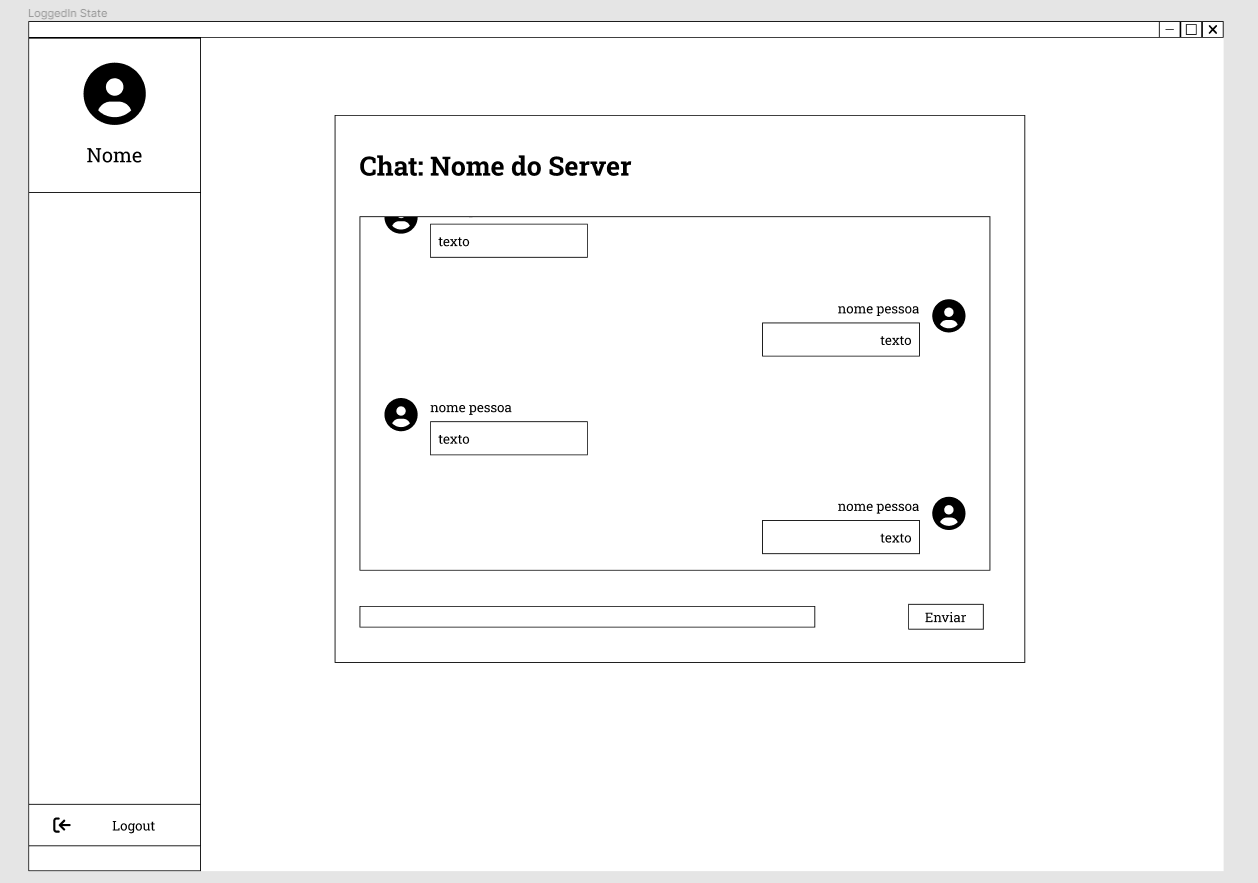


Figura 3 - Wireframe da Zona Cliente

# Conclusão

Com o UI todo feito, só falta construir toda a lógica do servidor, com a criptografia incluída, e toda a lógica do cliente para este comunicar com o servidor e vice-versa.