|  |  |
| --- | --- |
|  | Escola Superior de Tecnologia e Gestão  *Instituto Politécnico de Viana do Castelo*  **CTeSP de Tecnologias e Programação de Sistemas de Informação** |
|  |  |

**Projeto de Sistemas de Informação**

Especificação do projeto

*<designação do projeto>*

2022/2023

<nº -nome Alunos>

Sumário

[1. Âmbito / Enquadramento do projeto 3](#_Toc113460895)

[*2.* Objetivos 3](#_Toc113460896)

[3. Análise de Requisitos 3](#_Toc113460897)

[4. Design e modelação da solução 3](#_Toc113460898)

[4.1 Modelo de casos de uso 3](#_Toc113460899)

[4.2 Modelo relacional 3](#_Toc113460900)

[4.3 Arquitetura geral da solução 3](#_Toc113460901)

[4.4 Tecnologias envolvidas 3](#_Toc113460902)

[5. Mockups 4](#_Toc113460903)

[6. Cronograma 4](#_Toc113460904)

[7. Implementação 4](#_Toc113460905)

[8. Conclusão 4](#_Toc113460906)

[9. Melhorias futuras 4](#_Toc113460907)

# Âmbito / Enquadramento do projeto

*Criação de uma plataforma para denuncias de ciberataques.*

# Objetivos

*Efetuar vários tipos de denuncia ( Mensagens falsas, chamadas falsas, emails falsos e ciberataques a dispositivos ou empresas );*

*Melhor comunicação com especialistas para resolver os problemas que surgem para melhorar a sua proteção.*

# Análise de Requisitos

*<fazer uma análise detalhada de requisitos, que de sistema, quer de utilizador>*

*Requisitos Funcionais:*

* *Registo de Utilizadores: Os utilizadores devem se registrar na plataforma usando um endereço de e-mail válido ou outras credenciais seguras, devem tambem conseguir aceder ao seu perfil e edita-lo .*
* *Envio de denuncias: Os utilizadores devm conseguir enviar denunciasde ciberataques, spams entre outros incidentes de seguranca deve ser possível anexar evidencias, como screenshots ou log, as denuncias.*
* *Categorizacao dos incidentes: Os utilizadores devem conseguir categorizar tipo de incidentes ( ciberataques, spam, phishing, etc ) ao enviar uma denuncia.*
* *Acompanhamento de denuncias: Os utilizadores devem ser capazes de acompanhar o status das suas denuncias, como “pendentes”, “em investigacao” ou “resolvida”.*
* *Realizacao de pedidos de submissao: Utilizadores que tenham conhecimentos na area de ciberseguranca podem fazer um pedido de submissao para obter o titulo ou um verificado de que e um especialista na area da ciberseguranca para depois conseguir ajudar os utilizadores normais nos suas denuncias.*
* *Gerenciamento de incidentes:*

*<usar ferramentas e processos lecionados no 1º ano como os use cases>*

# Design e modelação da solução

## Modelo de casos de uso

*<inserir modelo de casos de uso e respetiva decrição>*

## Modelo de dados (modelo relacional)

*<inserir modelo relacional de suporte à solução>*

## Arquitetura geral da solução

*<inserir imagem com as várias componentes e interação entre elas>*

*<inserir explicação textual>*

## Tecnologias envolvidas

*<inserir as tecnologias que serão utilizadas nos diversos componentes do projeto>*

# Mockups

*<inserir aqui os vários mockups e considerações sobre cada um>*

<**Exemplo 1**: neste primeiro ecrã faz-se a validação do login; caso dê erro o utilizador é notificado; senão avança-se para o ecrã seguinte>

<**Exemplo 2:** neste ecrã de mapas, caso não haja internet, o utilizador é notificado e avisa-se que por isso não pode ser apresentado o mapa. Caso não haja GPS, o mapa é apresentado e ao utilizador é perguntado se quer abrir as definições para ativar o GPS e ter assim acesso a todas as seguintes funcionalidades>

<**Exemplo 3**: neste ecrã de listagem de locais é invocado um web service que retornará uma listagem de locais depois de passada a cidada como argumento>

# Cronograma

*<inserir cronograma e planeamento das tarefas de acordo com UC de Gestão de Projetos>*

# Implementação

# Conclusão

# Melhorias futuras