|  |  |
| --- | --- |
| defdefdef | 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 denúncias de ciberataques.*

# Objetivos

Efetuar vários tipos de denúncias( 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

*Requisitos Funcionais:*

* ***Registo de Utilizadores****: Os utilizadores devem se registar na plataforma usando um endereço de e-mail válido ou outras credenciais seguras. Devem proceder com o registo acedendo ao seu perfil e editar informações necessárias .*
* ***Envio de denúncias****: Os utilizadores devem conseguir enviar denuncias de ciberataques, spams, entre outros incidentes de segurança. Deve ser possível anexar evidencias, como screenshots ou log, para as denúncias.*
* ***Categorização dos incidentes****: Os utilizadores devem conseguir categorizar o tipo de incidentes ( ciberataques, spam, phishing, etc ) ao enviar uma denúncia.*
* ***Acompanhamento de denúncias****: Os utilizadores devem ser capazes de acompanhar o status das suas denúncias, como “pendentes”, “em investigação” ou “resolvida”.*
* ***Realização de pedidos de submissão****: Utilizadores que tenham conhecimentos na área de ciberseguranca podem fazer um pedido de submissão para obter um título ou verificado de que é um especialista na área da ciberseguranca para depois conseguir ajudar os utilizadores normais nas suas denúncias.*
* ***Gestão de incidentes****: Os especialistas devem ter capacidade de analisar, investigar e tomar medidas em relação às denúncias recebidas.*
* ***Notificações por e-mail****: Os utilizadores devem receber notificações por e-mail sobre o status das suas denúncias, incluindo atualizações e resoluções.*
* ***Busca e filtros****: Deve ser possível pesquisar e filtrar denúncias com base nos vários critérios e categorias como (mensagens, emails, data, etc… ).*
* ***Relatórios e Estatísticas****: A plataforma deve gerar estatísticas sobre o volume e a natureza das denúncias recebidas. (Apanhado geral )*

***Requisitos não funcionais****:*

* ***Segurança****: A plataforma deve implementar medidas de segurança robustas para proteger os dados do utilizador e as suas informações confidenciais relacionadas às denuncias.*
* ***Estabilidade****: A plataforma deve ser escalável para lidar com um grande volume de denúncias à medida que o número de utilizadores e incidentes aumenta.*
* ***Desempenho****: A plataforma deve ser otimizada para um desempenho rápido e responsivo, garantido tempos de carregamento mínimos.*
* ***Disponibilidade****: A plataforma deve ser disponível, minimizando o tempo de inatividade planeado e não planeado.*
* ***Usabilidade****: A interface do utilizador deve ser intuitiva e amigável para que os utilizadores possam facilmente enviar denúncias e acompanhar o status delas mesmas.*
* ***Manutenção****: A plataforma deve ser de fácil manutenção, permitindo atualizações e correções de forma eficiente.*

# Design e modelação da solução

## Modelo de casos de uso

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

Descrição gerada automaticamente

## Modelo de dados (modelo relacional)

O modelo relacional concebido para o sistema de gestão de denúncias de ciberataques foi criado com o intuito de registar, organizar e gerir as atividades relacionadas com a denúncia e a comunicação de incidentes de cibersegurança.

A **tabela "Utilizadores"** guarda informações sobre os utilizadores que participam na plataforma. Cada utilizador é identificado por um "UserID," que atua como chave primária. Os campos desta tabela incluem o nome, o email, a palavra-passe. Cada utilizador está associado a um ou mais tipo específico (Especialista, Suporte ou Admin) através da tabela "Tipo de Utilizador." Um utilizador pode fazer parte dos especialistas, do suporte e dos admins.

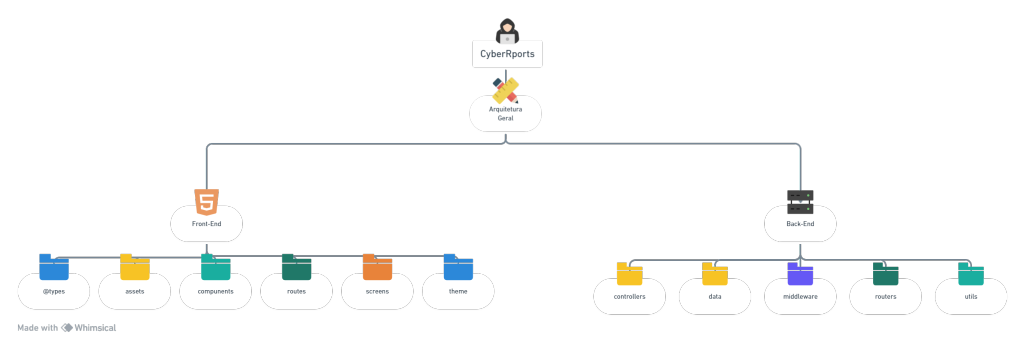
A **tabela "Tipo de Utilizador"** representa os diferentes papéis que os utilizadores podem desempenhar no sistema. Cada tipo de utilizador é identificado por um "TipoUtilizadorID." O campo "Tipo" na tabela "Tipo de Utilizador" define a função do utilizador (Especialista, Suporte ou Admin) e está associado a um utilizador específico através da chave estrangeira "UserID." Esta relação possibilita a atribuição flexível de diferentes funções a diferentes utilizadores.

A **tabela "Mensagens"** regista todas as comunicações entre os utilizadores. Cada mensagem é identificada por um "MensagemID," e a tabela regista o remetente ("DeUserID") e o destinatário ("ParaUserID") de cada mensagem, bem como o conteúdo da mensagem e a data de envio. Esta tabela permite o acompanhamento das conversas entre os utilizadores.

A **tabela "Denúncias"** é responsável pelo registo de denúncias de incidentes que os utilizadores queiram reportar. Cada denúncia é associada a um utilizador através da chave estrangeira "UserID," que identifica o denunciante. Inclui também uma referência ao incidente denunciado e uma descrição do mesmo. O campo "Estado" pode ser utilizado para monitorizar o progresso da investigação da denúncia.

A **tabela "Pedidos de Submissão"** é utilizada pelos utilizadores para solicitar a verificação na área de cibersegurança (conta de especialista). Cada pedido de submissão é identificado por um "PedidoID," e a tabela guarda informações sobre o utilizador que fez o pedido ("UserID"), o estado do pedido e outros detalhes relacionados com a solicitação. Os pedidos de submissão só podem ser avaliados pelos administradores, e a tabela permite o acompanhamento do processo de revisão.

## Arquitetura geral da solução

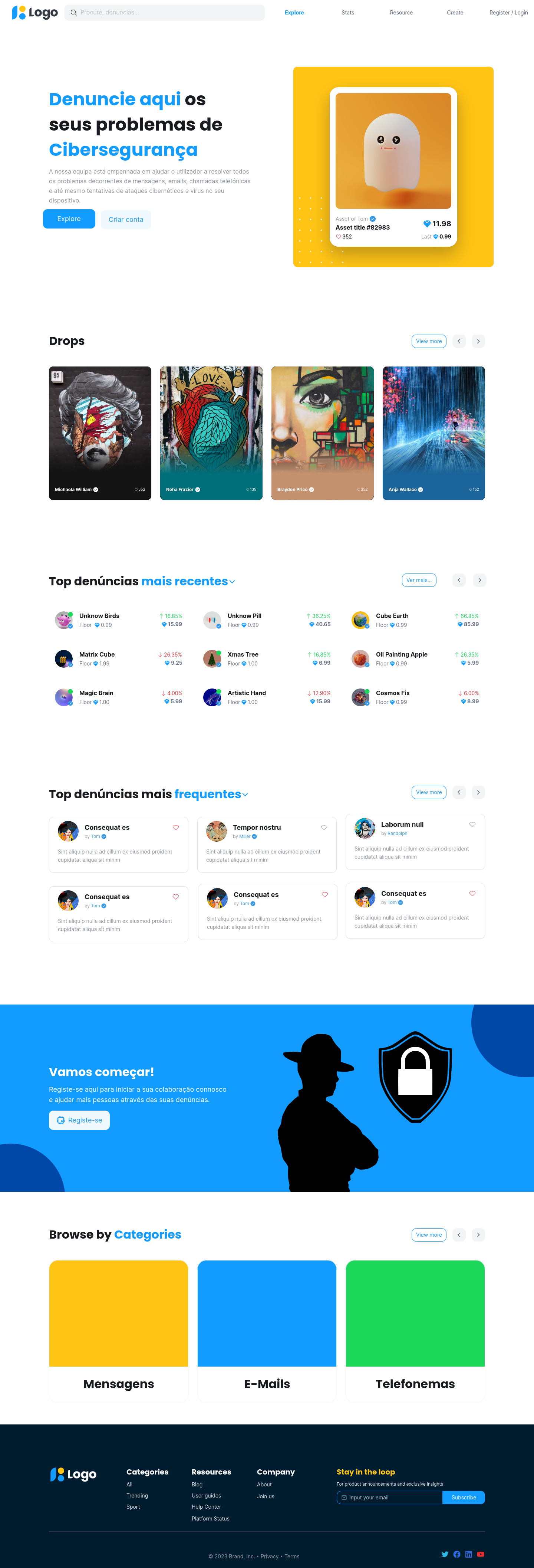
**

## Tecnologias envolvidas

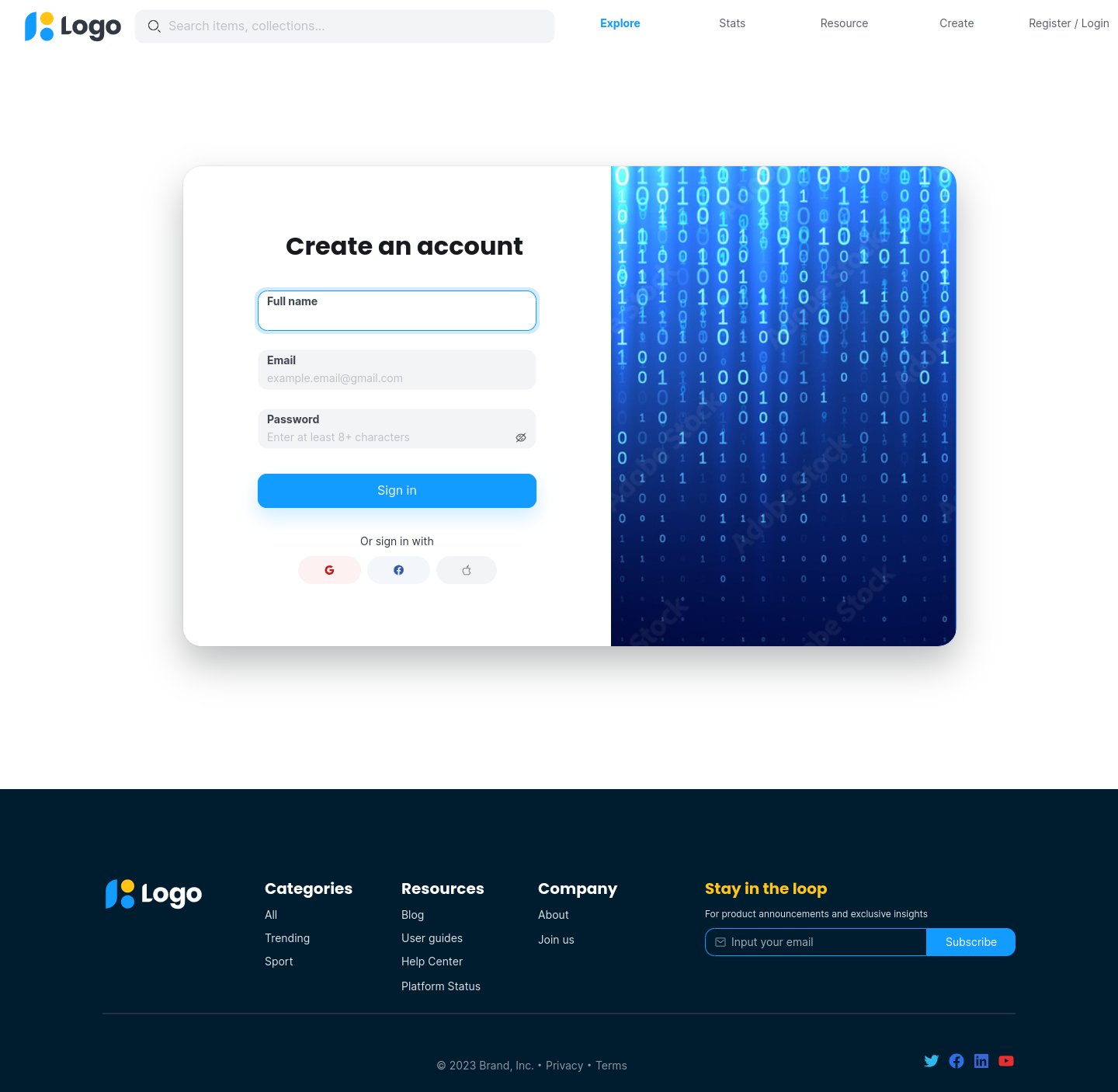
* React ( JavaScript );
* Node js;
* Vite;
* CloudFlare;
* HTML;
* Tailwind and Flowbite ( CSS );
* Banco de dados relacional.

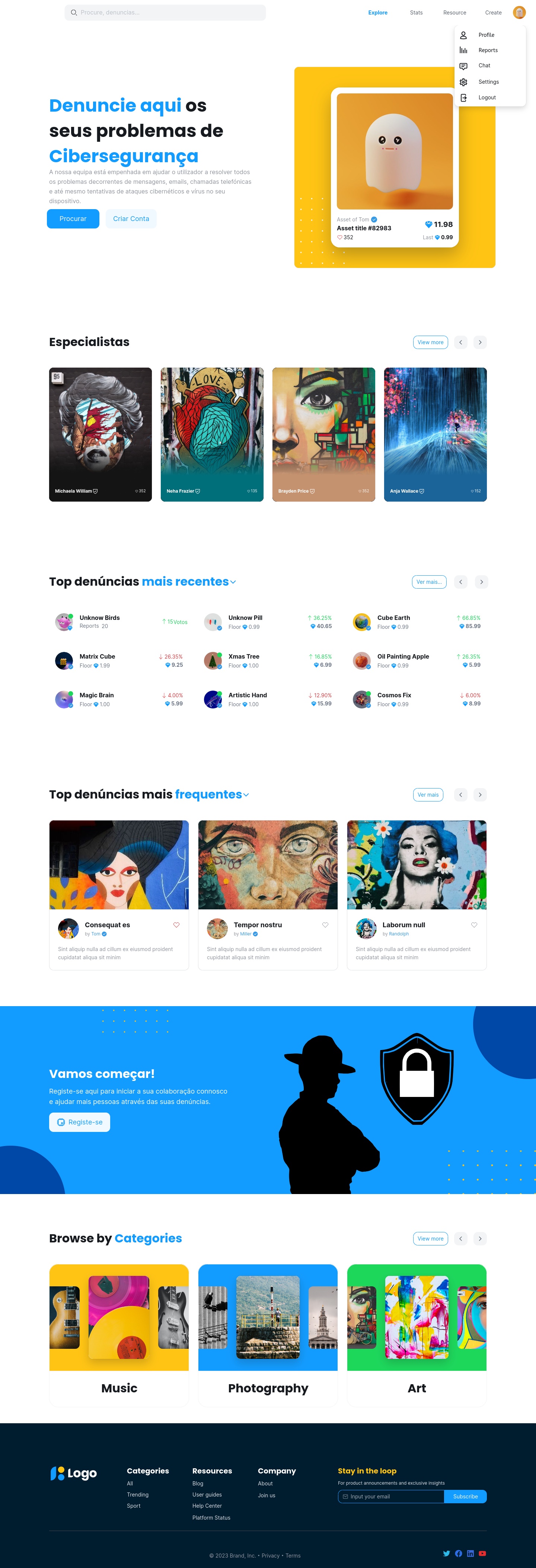
# Mockups

**Home page antes do login:**

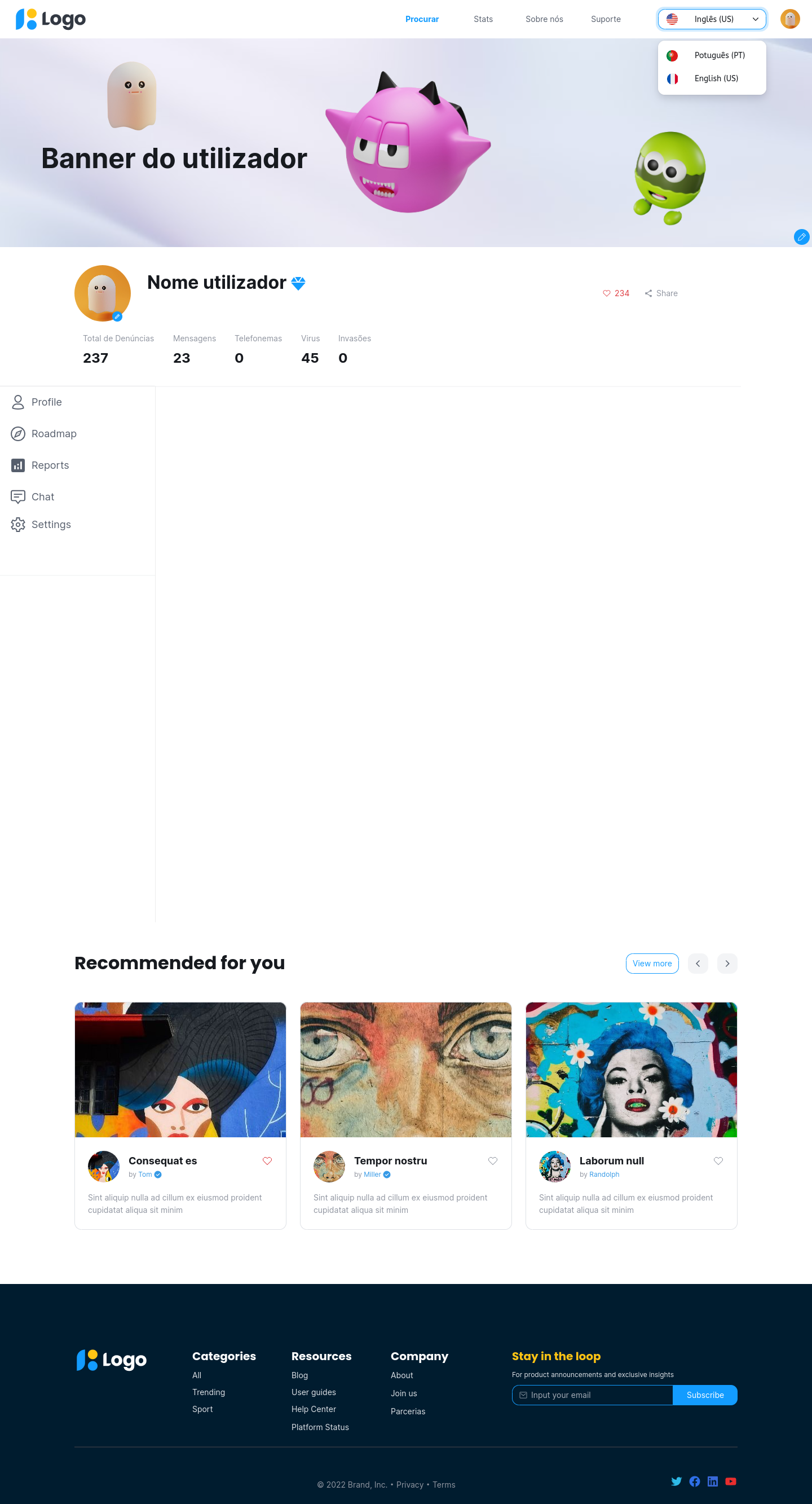


**Registo no site:**

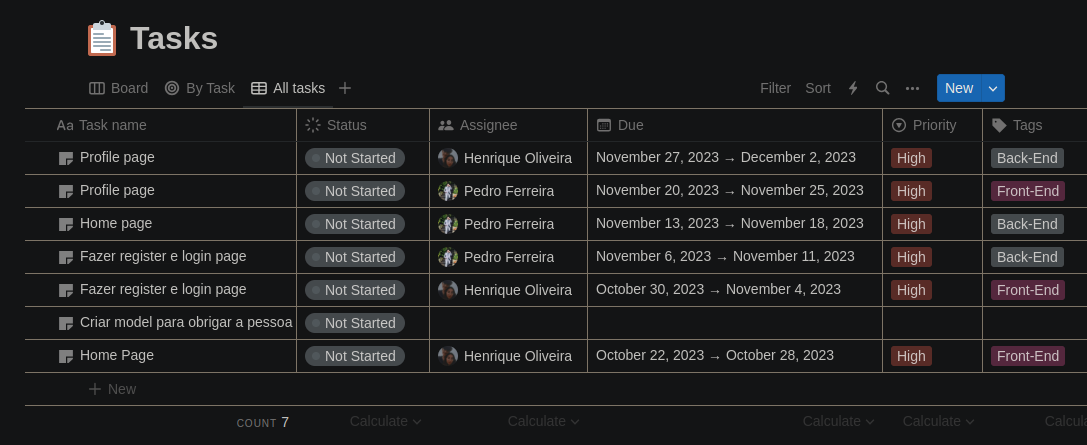


**Home page depois do login:**

**Página de perfil:**



# Cronograma



# Implementação

Nada implementado até este ponto.

# Conclusão

*Com este trabalho concluímos que o trabalho em equipa é essencial e com boa organização e algum estudo conseguimo-nos ajudar.*

# Melhorias futuras

*Pretendemos colocar online e desenvolver um chat em tempo real.*