

# **CyberFiasco – Porque todo mundo já caiu em uma cilada digital pelo menos uma vez.**

Gabriel Marques Da Silva Barros<sup>1</sup>

Letícia Valença Timóteo<sup>2</sup>

Thiago Matias Rodrigues<sup>3</sup>

## **Introdução**

A segurança cibernética tem se tornado um dos pilares fundamentais da era digital. Com o crescimento das ameaças virtuais, empresas e indivíduos enfrentam riscos constantes de ataques. Este projeto visa expor os principais ataques cibernéticos ocorridos entre 2015 e 2024, demonstrando seus impactos financeiros e apresentando estratégias eficazes de proteção, proporcionando uma abordagem relevante para o usuário comum, com informação assertiva e de fácil compreensão. A abordagem baseada em Rapid Application Development (RAD) permite que a aplicação seja desenvolvida de forma ágil e interativa, garantindo uma melhor adaptação às necessidades de segurança.

## **Justificativa**

A escolha deste projeto se baseia na necessidade urgente de conscientização e combate às ameaças cibernéticas. O aumento do número de ataques e seus impactos financeiros tornam essencial a criação de uma ferramenta que informe sobre os riscos e ajude na prevenção. A demanda por soluções educacionais sobre segurança digital está em constante crescimento, e esta aplicação busca atender essa necessidade.

## Objetivos

- **Objetivo Geral:** Desenvolver uma aplicação interativa que exponha os principais ataques cibernéticos entre 2015 e 2024, detalhando os prejuízos financeiros e formas de proteção em gráficos.
- **Objetivos Específicos:**
  - Organizar e visualizar dados sobre ataques cibernéticos no período determinado.
  - Criar gráficos ilustrativos sobre o impacto dos ataques.
  - Oferecer recomendações práticas de segurança para usuários.
  - Facilitar o entendimento de padrões e tendências nos ataques cibernéticos.

## Base de Dados

O projeto utiliza o banco de dados "Global\_Cybersecurity\_Threats\_2015-2024", que contém informações detalhadas sobre ataques cibernéticos.

- **Origem dos dados:**  
<https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024>;
- **Formato:** CSV, facilitando a manipulação dos dados com bibliotecas Python.
- **Colunas:**
  - **Country** - (País)
  - **Year** - (Ano)
  - **Attack Type** - (Tipo de Ataque)
  - **Target Industry** - (Industria Alvo)
  - **Financial Loss (in Million \$)** - (Perda Financeira (em Milhão \$))
  - **Number of Affected Users** - (Números de Usuários Afetados)
  - **Attack Source** - (Fonte do Ataque)
  - **Security Vulnerability Type** - (Tipo de Vulnerabilidade de Segurança)
  - **Defense Mechanism Used** - (Mecanismo de Defesa Usado)
  - **Incident Resolution Time (in Hours)** - (Tempo de Resolução do Incidente (em Horas))

- **Pré-processamento:** Limpeza dos dados, remoção de inconsistências e padronização para melhor análise. Vide em anexo o código utilizado no tratamento do banco.

## Tecnologias Utilizadas

O projeto foi desenvolvido em Python, utilizando as seguintes bibliotecas:

- **CustomTkinter** – Construção da interface gráfica da aplicação.
- **Pandas** – Manipulação e análise de dados.
- **Pillow** – Manipulação de imagens.
- **Plotly** – Visualização gráfica de padrões e tendências.
- **Subprocess** - Permite executar e gerenciar processos externos dentro de um programa.
- **Sqlite3** – Para tratamento dos bancos de dados.
- **Sys** – Construção da interface gráfica da aplicação.

O editor de código-fonte utilizado foi o *Visual Studio Code* (VS Code), desenvolvido pela *Microsoft*. Escolhido por ser leve, multiplataforma, flexível e personalizável.

## Metodologia de Desenvolvimento

### Abordagem Utilizada:

- RAD, permitindo entregas rápidas e feedback contínuo.
- Comunicação frequente entre membros para ajustes ágeis.

### Etapas de Desenvolvimento:

- **Análise e Tratamento do Banco de Dados:** Tratar os dados presentes no banco.
- **Interface Gráfica:** Desenvolvimento inicial da interface.
- **Manipulação do Banco de Usuários:** Gerenciamento dos dados dos usuários.

- **Visualização de Dados e Gráficos:** Visualização a partir dos filtros aplicados pelo usuário.
- **Implementação Final:** Versão otimizada da aplicação.

## Organização do Trabalho

### Análise e tratamento do banco de dados

O processo inicia-se com o download da base de dados, seguido da avaliação criteriosa das informações contidas. Para garantir a integridade dos dados, são realizadas manipulações para identificar e tratar possíveis duplicidades e valores nulos. Além disso, são examinadas a origem e a estrutura dos dados, assegurando sua adequação para análise.

A manipulação da base de dados foi conduzida com suporte da biblioteca *Pandas*, permitindo a leitura, filtragem e tratamento eficiente das informações. Todas as operações foram implementadas em *Python*, sob a execução de Letícia Valença.

### Interface gráfica

A interface interativa foi projetada com o objetivo de proporcionar uma experiência intuitiva e acessível ao usuário. O desenvolvimento seguiu uma abordagem estruturada, iniciando-se com a prototipagem preliminar em rascunhos, cujas imagens podem ser consultadas nos anexos.

Para a construção da interface, foi utilizada a biblioteca *Pandas*, *Pillow* e *CustomTkinter*, permitindo a criação de uma experiência visual moderna e adaptável. A estrutura da interface é composta pelas seguintes páginas:

### Desenvolvidas por Gabriel Marques:

**Página inicial:** Construída usando a biblioteca *customtkinter*, configurada com o modo escuro e tema azul. A classe *AplicativoSegurancaCibernetica* inicializa a janela principal com título, dimensões fixas (1100x700) e um ícone. A interface é dividida em um título central e uma descrição, seguidos por um frame principal horizontal que contém duas seções: à esquerda, um frame de imagem exibe uma imagem temática (*imagem\_main.jpeg*) com botões de "Login" e "Criar Conta" que

chamam funções externas (*abri\_janela\_login* e *abri\_janela\_cadastro*) para navegação; à direita, um frame de curiosidades (*frame\_curiosidades*) que apresenta estatísticas impactantes sobre ataques cibernéticos no Brasil, destacando a relevância da ferramenta. Todo o layout é cuidadosamente organizado para proporcionar uma experiência de usuário intuitiva e informativa na página inicial da aplicação.

**Atualização e Exclusão de Dados:** A função *abrir\_janela\_atualizar* cria uma janela *CTkToplevel* para gerenciar a atualização e exclusão de dados do arquivo *Global\_Cybersecurity\_Threats\_2015-2024.csv*. A interface possui um frame de filtros (*filtros\_frame*) com *CTkEntry* para filtrar os dados e um frame de tabela (*tabela\_frame*) com *ttk.Treeview*, permitindo edição direta de células e rolagem. A tabela mantém um histórico de ações para a funcionalidade "Desfazer". Três botões principais controlam as ações: "Aplicar Filtros" para atualizar a visualização, "Deletar Linha" para remover registros e "Desfazer" para restaurar alterações, garantindo maior controle sobre os dados.

#### **Desenvolvidas por Letícia Valença:**

**Cadastro de Novos Usuários:** Acessada pela função *abri\_janela\_cadastro*, é uma janela *CTkToplevel* que se sobrepõe a qualquer outra janela, permite registrar novos membros no sistema. Inclui campos para "Nome de Usuário", "Senha" e "Confirmar Senha". Se os campos "Senha" e "Confirmar Senha" coincidirem, a função *cadastrar\_usuario* do módulo *bancousuario*, cadastra o novo usuário e um *CTkLabel* (*mensagem\_status\_cadastro*) indicando sucesso ou erro na operação.

**Quiz:** A função *abri\_janela\_quiz* inicia uma janela *CTkToplevel* para um Quiz de Cibersegurança, gerando perguntas dinâmicas a partir do arquivo *Global\_Cybersecurity\_Threats\_2015-2024.csv*. As questões abordam estatísticas como país com mais incidentes, tipo de ataque mais comum e maior prejuízo financeiro, além de perguntas fixas sobre conceitos de cibersegurança. As perguntas aparecem em um *CTkLabel*, com respostas em *CTkButtons* que verificam e atualizam a pontuação, exibindo feedback ao usuário. O *CTkProgressBar* indica o progresso, e a pontuação total é mostrada ao final. As questões são embaralhadas, garantindo diversidade a cada sessão.

## Desenvolvidas por Thiago Matias:

**Home:** Ao iniciar, a aplicação carrega dados do banco (*Global\_Cybersecurity\_Threats\_2015-2024.csv*) e exibe uma interface intuitiva com CustomTkinter. A janela principal (janela) possui um cabeçalho com o título e os botões "Atualizar/Deletar Base de Dados" e "Cadastrar Novo Ataque", que invocam funções de outras janelas (*abrir\_janela\_atualizar*, *abrir\_janela\_cadastro*). O frame central divide-se entre a mascote à esquerda e o frame de filtros à direita, onde *checkboxes* (*CTkScrollableFrames*) e *comboboxes* permitem selecionar anos, países, tipos de ataque e configurar gráficos interativos (Barras, Pizza, Linha) e suas respectivas orientações de eixo. As funções *gerar\_grafico* e *limpar\_filtros* quando acionadas, permitem visualizar os gráficos ou resetar as seleções. Por fim, o "Que tal um quiz?" abre uma nova janela de quiz (*abri\_janela\_quiz*).

**Login:** Controlada pela função *abri\_janela\_login*, é uma janela *CTkToplevel* que se sobrepõe à janela principal, a interface possui campos de usuário e senha válidos. O botão "Entrar" aciona a função *entrar*, que valida às credenciais usando *validar\_login* do módulo *bancousuario*; em caso de sucesso, a janela de login e a principal são destruídas, e a página *home* é iniciada via subprocess. Há também "Esqueci minha senha" que abre uma sub-janela, permitindo verificar o usuário e, se encontrado, definir e salvar uma nova senha com as funções *usuario\_existe* e *editar\_senha*.

**Cadastro de Novos Dados:** A função *abri\_janela\_cadastro* cria uma janela *CTkToplevel* para inserção de registros na base, manipulada com Pandas. Um *CTkFrame* central organiza os campos de entrada dinamicamente, criando um *CTkLabel* e um campo de entrada (*CTkEntry* ou *CTkComboBox*) para cada coluna do *DataFrame*. "Country" e "Year" usam listas pré-definidas, enquanto colunas com até 100 valores únicos geram um *CTkComboBox*; caso contrário, um *CTkEntry* é usado. O botão "Salvar" aciona a função *salvar\_dado*, que coleta os dados, adiciona a nova linha ao *DataFrame* e salva o arquivo CSV, exibindo uma mensagem de sucesso.

## Manipulação do Banco de Usuários

O módulo gerencia a persistência de dados de usuários via *SQLite3*, criando e interagindo com o banco *usuarios.db*. A função *criar\_banco* assegura a existência da tabela *usuarios* (*id*, *nome*, *senha*). Para operações CRUD, oferece funções como *criar\_usuario*, *listar\_usuarios*, *editar\_senha* e *remover\_usuario*. Além disso, *validar\_login* verifica credenciais e *usuario\_existe* confirma se um nome de usuário já está cadastrado. O bloco `if __name__ == '__main__'` permite testes das funcionalidades via linha de comando.

Esse passo foi desenvolvido por Thiago Matias, assegurando um sistema robusto para gerenciamento dos usuários.

## Visualização de Dados e Gráficos

O código desenvolvido carrega a base de dados e permite ao usuário aplicar filtros para refinar sua análise. A partir desses filtros, são gerados gráficos dinâmicos utilizando a biblioteca *Plotly Express*, possibilitando uma interpretação clara dos dados.

Os principais tipos de visualização incluem:

- **Gráfico de Barras (px.bar)** – Representa a distribuição das ameaças por país, categorizadas pelo tipo de ataque.
- **Gráfico de Pizza (px.pie)** – Exibe a proporção dos diferentes tipos de ataques em relação ao total de eventos.
- **Gráfico de Linha (px.line)** – Mostra a evolução das ameaças ao longo dos anos, considerando a perda de registros em diferentes países.

Essa atividade foi desenvolvida e refinada por Thiago Matias, garantindo gráficos interativos que contribuem para a análise detalhada dos dados.

## Documentação do Projeto

A documentação detalha as etapas da criação da aplicação, desde a concepção da ideia inicial até o produto final, abordando as motivações, funcionalidades, tecnologias utilizadas e organização do projeto. Também inclui a

coleta e análise dos dados aplicados em cada fase, proporcionando um registro do desenvolvimento.

Essa etapa foi conduzida por Letícia Valença, assegurando um acompanhamento da implementação do sistema.

## Resultados e Funcionalidades

A aplicação fornece uma visualização interativa dos principais ataques cibernéticos do período de 2015 a 2024, incluindo:

- Gráficos mostrando tendências e frequência dos ataques.
- Interface intuitiva desenvolvida com *CustomTkinter* para facilitar o acesso às informações.
- Quiz interativo para treinar o conhecimento.

## Conclusão

O desenvolvimento deste projeto proporcionou uma análise aprofundada dos ataques cibernéticos e suas consequências, permitindo identificar padrões recorrentes e reforçar a importância da educação digital na mitigação de riscos. A aplicação mostrou-se uma ferramenta valiosa para profissionais e empresas que buscam aprimorar suas práticas de segurança cibernética. Além disso, para o usuário comum, esta aplicação desempenha um papel fundamental na conscientização sobre ameaças digitais e práticas seguras na internet.

Construído seguindo a Metodologia RAD (Rapid Application Development), permitindo um ciclo ágil na construção da aplicação. Esse modelo possibilitou ajustes rápidos com base na comunicação contínua dos integrantes do grupo, garantindo uma interface mais intuitiva, uma estrutura funcional eficiente e os recursos interativos foram desenvolvidos para tornar o aprendizado acessível a todos, independentemente do nível de conhecimento técnico. Desenvolvida com *customtkinter* para uma interface intuitiva, *pandas* para manipulação de dados e *sqlite3* para gerenciamento de usuários, a aplicação se destaca como um recurso valioso para educar e informar sobre o cenário da segurança cibernética.



# Links

Acesso ao *Trello*

[Divisões | Trello](#)

Base de dados

<https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024>

Link do GitHub

<https://github.com/tehvati/CyberFiasco-Porque-todo-mundo-j-caiu-em-uma-cilada-digital-pelo-menos-uma-vez>

# Anexos

- **Código para tratamento do banco de dados:**

```
import pandas as pd
```

```
# Carregar o banco de dados
```

```
file_path = "Global_Cybersecurity_Threats_2015-2024.csv"
```

```
df = pd.read_csv(file_path)
```

```
# Exibir informações gerais do dataset
```

```
print(f"O dataset possui {df.shape[0]} linhas e {df.shape[1]} colunas.\n")
```

```
# Verificar valores ausentes
```

```
missing_values = df.isnull().sum()
```

```
print("Valores ausentes por coluna:\n", missing_values)
```

```
# Verificar duplicatas
```

```
duplicates = df.duplicated().sum()
```

```
print(f"\nTotal de linhas duplicadas: {duplicates}")
```

```
# Verificar inconsistências nos tipos de dados
```

```
print("\nTipos de dados:\n", df.dtypes)
```

```
# Exibir as primeiras linhas do DataFrame para inspeção
```

```
print("\nExemplo dos primeiros registros do banco de dados:")
```

```
print(df.head())
```

```
# Exibir os ataques mais recorrentes
```

```
print("\nTop 5 tipos de ataques mais frequentes:")
```

```
print(df["Attack Type"].value_counts().head())
```

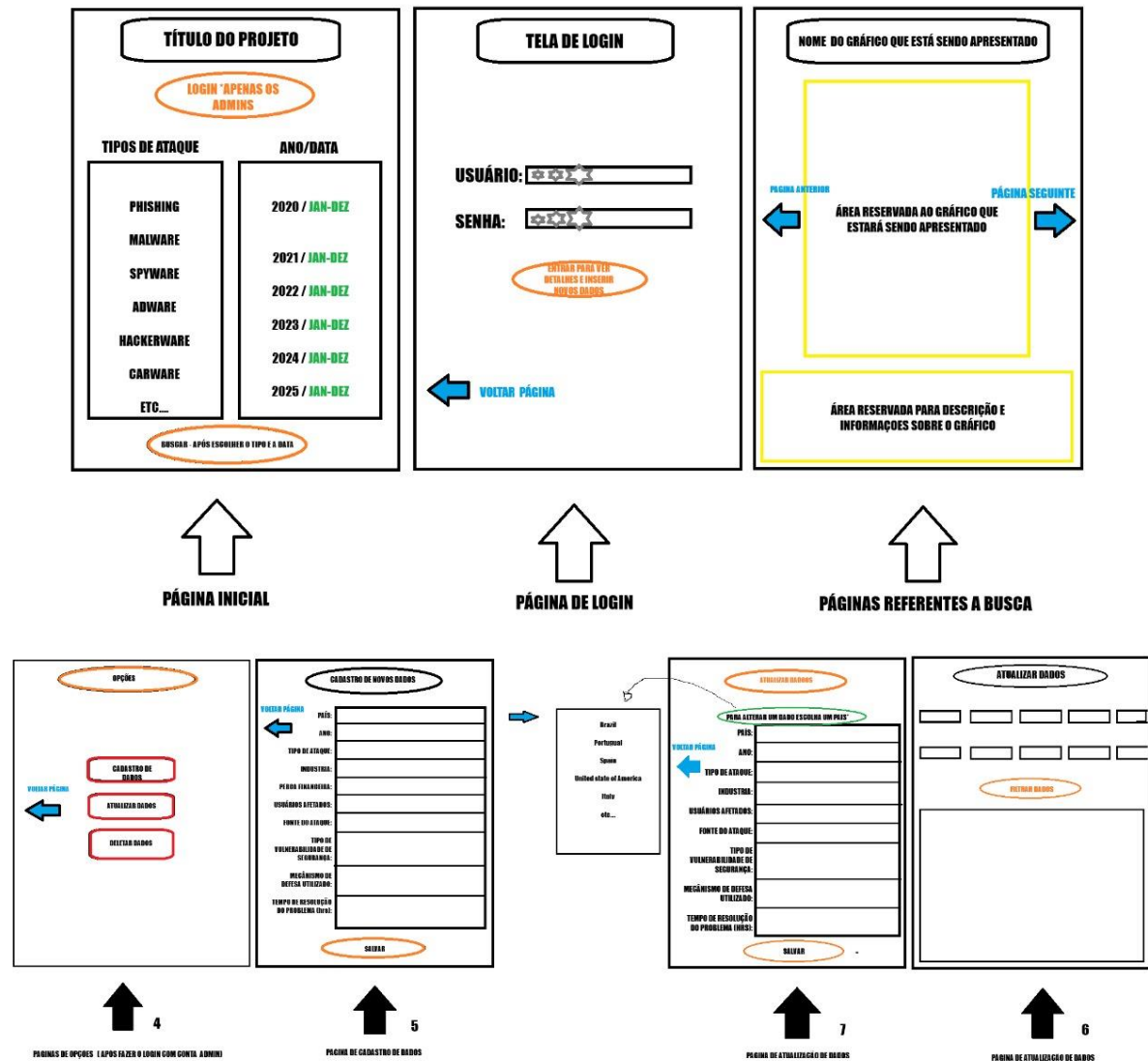
```
# Exibir os 5 maiores valores de perda financeira
```

```
print("\nTop 5 maiores perdas financeiras registradas:")
```

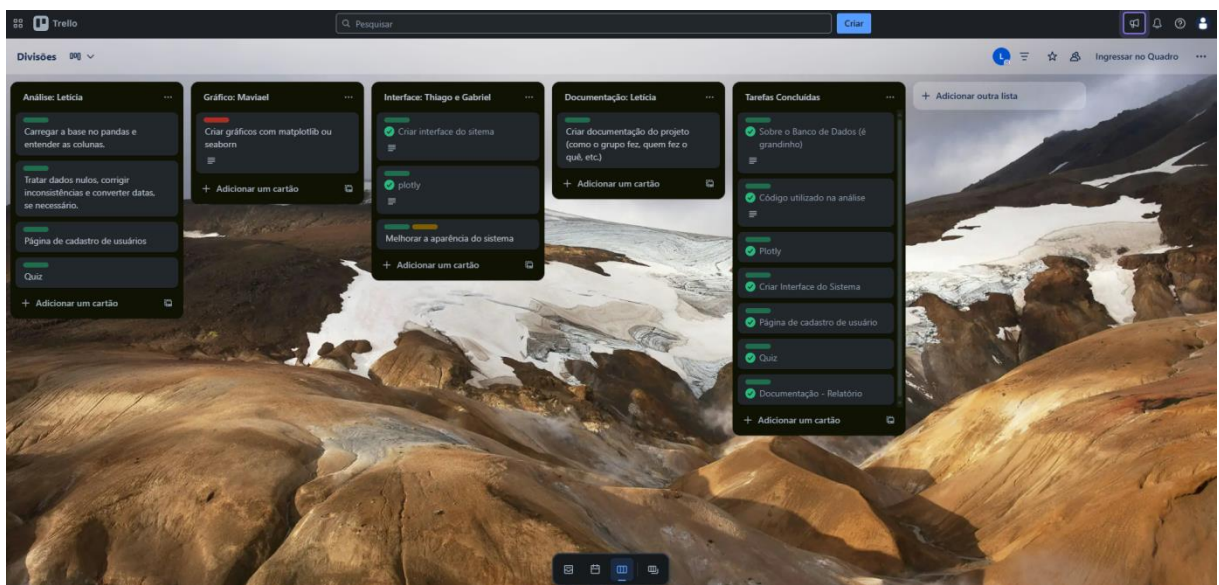
```
print(df.nlargest(5, "Financial Loss (in Million $)")["Attack Type", "Financial Loss (in Million $)", "Country", "Year"])
```

```
print("\nAnálise concluída.")
```

- Rascunho do protótipo inicial

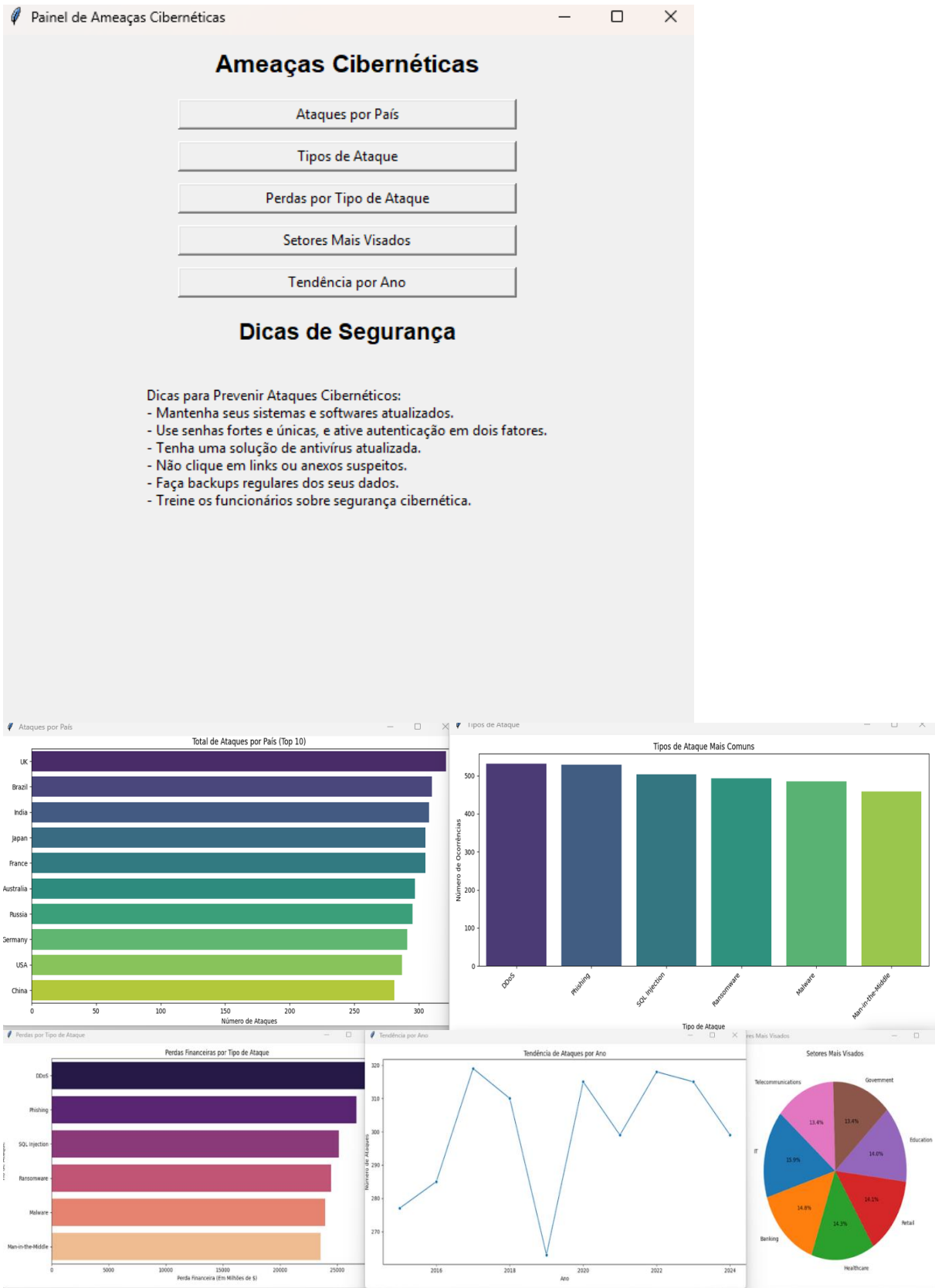


- Divisão no Trello



- Versões da aplicação

V1 - Interface Gráfica



## V2 - Login e Opções

The image displays two side-by-side screenshots of a web application interface.

The left window, titled "Login", features a dark background with the word "Entrar" in large white text. Below it are two input fields labeled "Usuário" and "Senha", and a blue button labeled "Entrar".

The right window, titled "Interface de Opções", also has a dark background and displays the text "MENU DE OPÇÕES" in white. Below this text are four blue buttons: "CADASTRAR NOVOS DADOS", "ATUALIZAR DADOS", "DELETAR DADOS", and a link labeled "VOLTAR PÁGINA" with a back arrow icon.

## V3 - Interface Gráfica

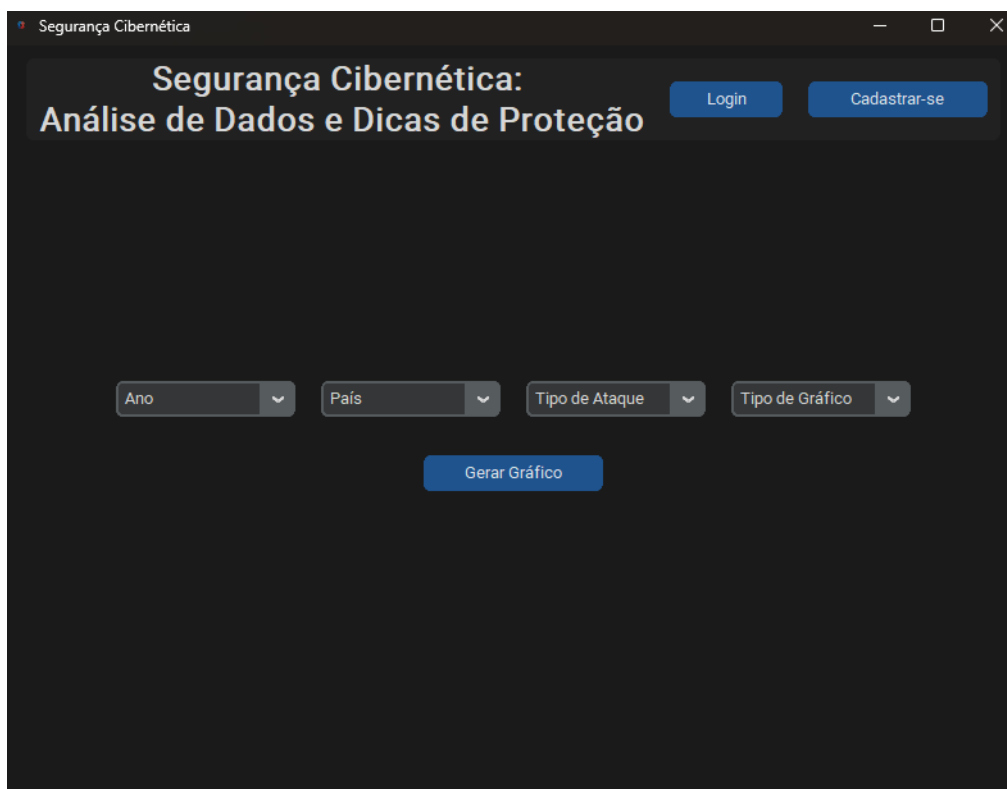
The image shows a screenshot of a web application interface titled "Segurança Cibernética: Análise de Dados e Dicas de Proteção".

The interface has a dark background. At the top right, there is a blue button labeled "Login".

Below the title, there are four dropdown menus for filtering data: "Ano", "País", "Tipo de Ataque", and "Tipo de Gráfico".

At the bottom center, there is a blue button labeled "Gerar Gráfico".

## V4 - Interface Gráfica e cadastro de usuário



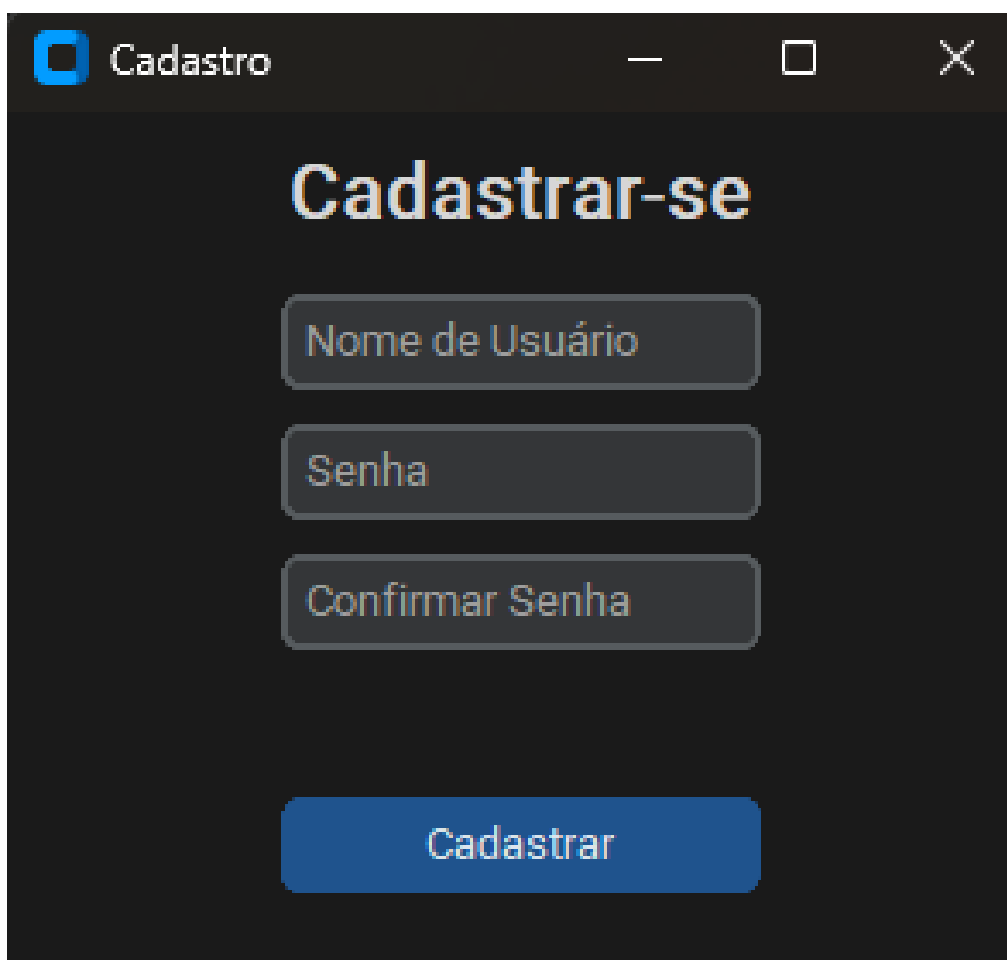
Segurança Cibernética

Segurança Cibernética:  
Análise de Dados e Dicas de Proteção

Login Cadastrar-se

Ano País Tipo de Ataque Tipo de Gráfico

Gerar Gráfico



Cadastro

# Cadastrar-se

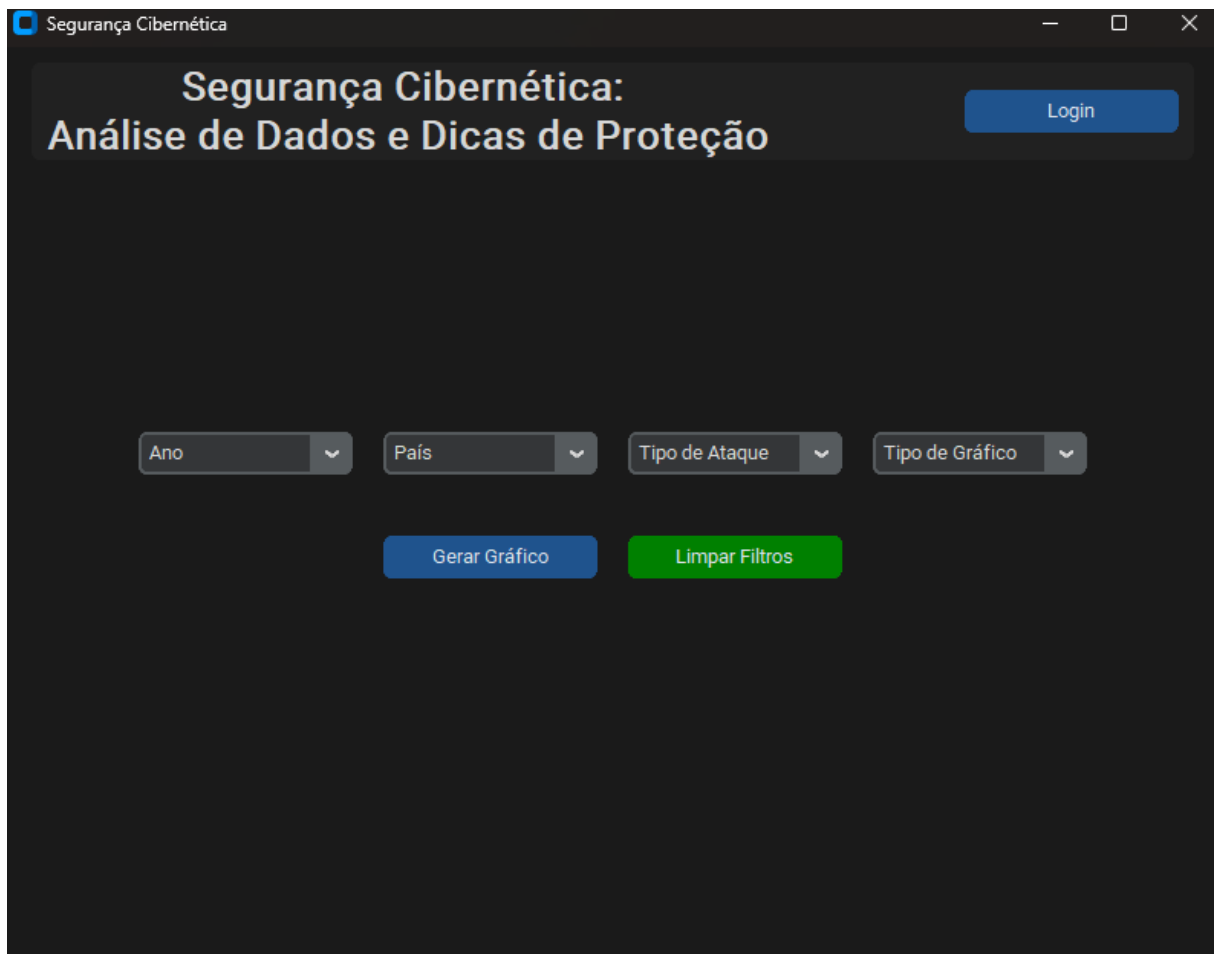
Nome de Usuário

Senha

Confirmar Senha

Cadastrar

V5 - Interface Gráfica



V6 - Página Atualizar e Deletar

Opções

Opções

Cadastrar Dados

Atualizar/Deletar Dados

Atualizar/Deletar Dados

Country

Filtrar Country

Year

Filtrar Year

Attack Type

Filtrar Attack Type

Target Industry

Filtrar Target Industry

Financial Loss (in Million \$)

Filtrar Financial Loss (i

Number of Affected Users

Filtrar Number of Affec

Attack Source

Filtrar Attack Source

Security Vulnerability Type

Filtrar Security Vulnera

Defense Mechanism Used

Filtrar Defense Mecha

Incident Resolution Time (in Hours)

Filtrar Incident Resolut

Country	Year	Attack Type	Target Industry	Financial Loss (in Million \$)	Number of Affected Users	Attack Source	Secu
China	2019	Phishing	Education	80.53	773169	Hacker Group	U
China	2019	Ransomware	Retail	62.19	295961	Hacker Group	U
India	2017	Man-in-the-Middle	IT	38.65	605895	Hacker Group	
UK	2024	Ransomware	Telecommunications	41.44	659320	Nation-state	S
Germany	2018	Man-in-the-Middle	IT	74.41	810682	Insider	S
Germany	2017	Man-in-the-Middle	Retail	98.24	285201	Unknown	S
Germany	2016	DDoS	Telecommunications	33.26	431262	Insider	U
France	2018	SQL Injection	Government	59.23	909991	Unknown	S
India	2016	Man-in-the-Middle	Banking	16.88	698249	Unknown	S
UK	2023	DDoS	Healthcare	69.14	685927	Hacker Group	U
China	2019	Phishing	Telecommunications	88.67	493675	Unknown	
China	2016	SQL Injection	Healthcare	38.81	920768	Hacker Group	U
India	2019	Ransomware	Education	30.56	583204	Insider	
France	2023	DDoS	Healthcare	58.37	599797	Nation-state	U
France	2024	DDoS	IT	48.01	922258	Unknown	S
Australia	2022	Phishing	Banking	64.31	120789	Nation-state	
Russia	2017	Man-in-the-Middle	Healthcare	13.04	850158	Hacker Group	U
India	2015	DDoS	IT	93.14	805278	Insider	S
UK	2019	Malware	Telecommunications	14.01	578443	Insider	S
India	2016	DDoS	IT	36.45	261808	Nation-state	S

Aplicar Filtros

Deletar Linha

Desfazer



## V7 - Quiz

Segurança Cibernética

— □ ×

Segurança Cibernética:  
Análise de Dados e Dicas de Proteção

Login

Cadastrar-se

Ano ▾

País ▾

Tipo de Ataque ▾

Tipo de Gráfico ▾

Gerar Gráfico

Limpar Filtros

Que tal um quiz?

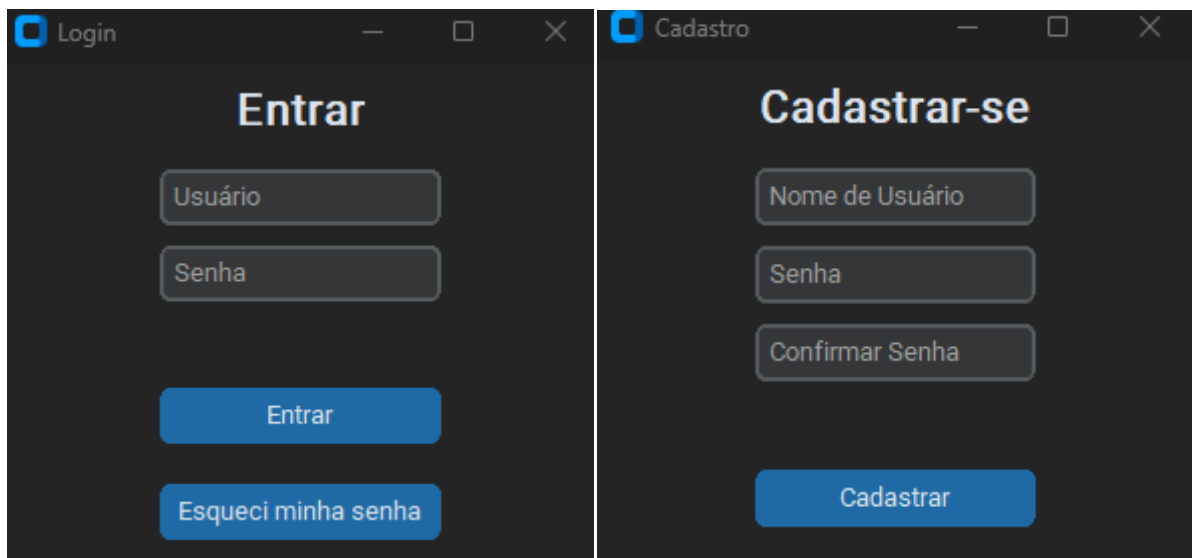
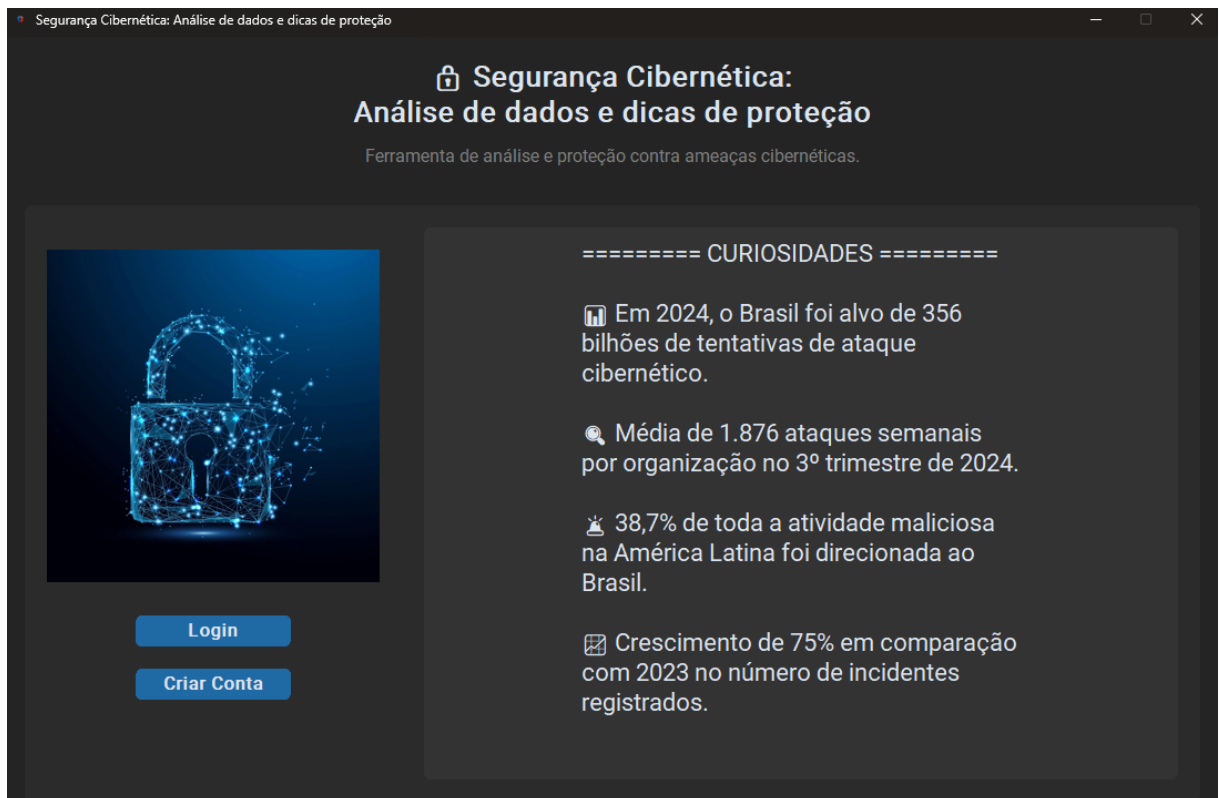
Quiz de Cibersegurança

— □ ×

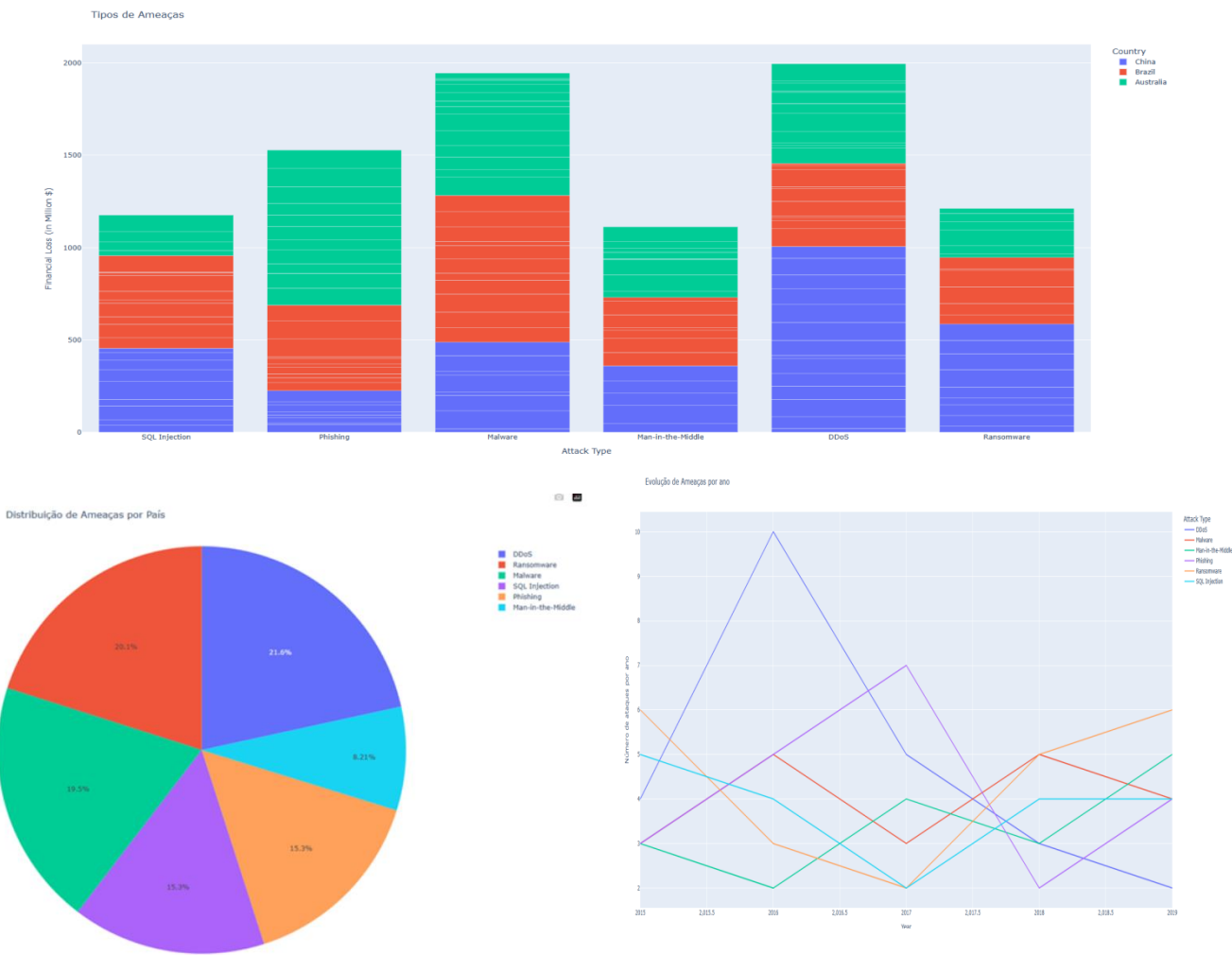
1. Qual país teve mais incidentes em 2017?

Enviar

## V8 – Página Inicial / Login / Cadastro



V9 – Página Home / Gráficos



V10 – Cadastrar Novo Ataque

Cadastro de novos ataques

Cadastros de Novo Ataque

Country:

Afghanistan

Year:

2014

Attack Type:

DDoS

Target Industry:

Banking

Financial Loss (in Million \$):

digite o valor de Financial

Number of Affected Users:

digite o valor de Number of Affect

Attack Source:

Hacker Group

Security Vulnerability Type:

Social Engineering

Defense Mechanism Used:

AI-based Detection

Incident Resolution Time (in Hours):

1

Salvar

V11 – Atualizar / Deletar Base de Dados

Atualizar/Deletar Dados

Country

Year

Attack Type

Target Industry

Financial Loss (in Million \$)

Number of Affected Users

Attack Source

Security Vulnerability Type

Defense Mechanism Used

Incident Resolution Time (in Hours)

Filtrar Country

Filtrar Year

Filtrar Attack Type

Filtrar Target Industry

Filtrar Financial Loss (l

Filtrar Number of Affect

Filtrar Attack Source

Filtrar Security Vulnera

Filtrar Defense Mecha

Filtrar Incident Resolut

Country	Year	Attack Type	Target Industry	Financial Loss (in Million \$)	Number of Affected Users	Attack Source	Security Vulnerability Type	Defense M
China	2019	Phishing	Education	80.53	773169	Hacker Group	Unpatched Software	
China	2019	Ransomware	Retail	62.19	295961	Hacker Group	Unpatched Software	F
India	2017	Man-in-the-Middle	IT	38.65	605895	Hacker Group	Weak Passwords	
UK	2024	Ransomware	Telecommunications	41.44	659320	Nation-state	Social Engineering	AI-base
Germany	2018	Man-in-the-Middle	IT	74.41	810682	Insider	Social Engineering	
Germany	2017	Man-in-the-Middle	Retail	98.24	285201	Unknown	Social Engineering	AI
Germany	2016	DDoS	Telecommunications	33.26	431262	Insider	Unpatched Software	
France	2018	SQL Injection	Government	59.23	909991	Unknown	Social Engineering	AI
India	2016	Man-in-the-Middle	Banking	16.88	698249	Unknown	Social Engineering	
UK	2023	DDoS	Healthcare	69.14	685927	Hacker Group	Unpatched Software	F
China	2019	Phishing	Telecommunications	88.67	493675	Unknown	Zero-day	
China	2016	SQL Injection	Healthcare	38.81	920768	Hacker Group	Unpatched Software	AI-base
India	2019	Ransomware	Education	30.56	583204	Insider	Zero-day	F
France	2023	DDoS	Healthcare	58.37	599797	Nation-state	Unpatched Software	AI-base
France	2024	DDoS	IT	48.01	922258	Unknown	Social Engineering	Eni
Australia	2022	Phishing	Banking	64.31	120789	Nation-state	Zero-day	Eni
Russia	2017	Man-in-the-Middle	Healthcare	13.04	850158	Hacker Group	Unpatched Software	AI-base
India	2015	DDoS	IT	93.14	805278	Insider	Social Engineering	Eni
UK	2019	Malware	Telecommunications	14.01	578443	Insider	Social Engineering	F
India	2016	DDoS	IT	36.45	261808	Nation-state	Social Engineering	AI-base
Brazil	2015	Ransomware	Retail	49.55	920172	Hacker Group	Weak Passwords	AI

Aplicar Filtros

Deletar Linha

Desfazer

## V12 – Quiz

