



CENTRO UNIVERSITÁRIO DE BRASÍLIA  
CIÊNCIA DA COMPUTAÇÃO

FELIPE BARCELOS DE CARVALHO (RA: 22350044)  
MARCOS VINICIUS ROCHA (RA: 22352865)  
JOÃO MARCELO GUIMARÃES DOURADO (RA: 22350653)  
EDUARDO ARAÚJO UCHOA (RA: 22353207)  
DAVI MAIA (RA: 22305561)

PROJECT AEGIS:  
PAINEL DE INTELIGÊNCIA DE AMEAÇAS

BRASÍLIA  
2025



## TERMO DE RESPONSABILIDADE E POLÍTICA DE USO DE DADOS

**Projeto:** Project Aegis: Painel de Inteligência de Ameaças **URL Oficial:** <https://vrsmarcos26.github.io/Project-Aegis> **Data de Vigência:** 25/11/2025

---

### 1. Natureza e Propósito do Projeto

O **Project Aegis** é uma ferramenta de software de código aberto (*Open Source*), desenvolvida com fins estritamente **acadêmicos e educacionais** no âmbito do curso de Ciência da Computação do Centro Universitário de Brasília (UniCEUB).

O objetivo da plataforma é centralizar e democratizar o acesso a dados públicos de cibersegurança, facilitando a visualização de tendências de ameaças para estudantes, pesquisadores e entusiastas da área. **Esta ferramenta não constitui um produto comercial e não possui fins lucrativos.**

### 2. Isenção de Responsabilidade (*Disclaimer*)

#### 2.1. Precisão dos Dados

O Project Aegis atua como um agregador de dados. Todas as informações exibidas no dashboard (CVEs, Vazamentos, IPs Maliciosos) são obtidas automaticamente de fontes públicas de terceiros (APIs).

- A equipe de desenvolvimento **não garante** a exatidão, pontualidade, integridade ou disponibilidade contínua dos dados fornecidos por essas fontes externas.
- A classificação de severidade ou atribuição geográfica de ataques reflete os dados originais da fonte e não necessariamente a opinião da equipe do projeto.

#### 2.2. Limitação de Uso

Esta ferramenta **não substitui** soluções profissionais de segurança da informação (como Antivírus, Firewalls, SIEM ou consultorias especializadas).

- A equipe do Project Aegis isenta-se de qualquer responsabilidade por danos diretos, indiretos ou consequenciais resultantes do uso das informações aqui apresentadas para tomada de decisões críticas de negócios ou segurança.

#### 2.3. Disponibilidade do Serviço

Como um projeto hospedado em infraestrutura gratuita (*GitHub Pages* e *GitHub Actions Free Tier*), não oferecemos Garantia de Nível de Serviço (SLA). O site pode ficar indisponível ou desatualizado devido a manutenções, limites de API ou instabilidade na plataforma hospedeira.

### 3. Política de Privacidade e Proteção de Dados

Em conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), estabelecemos uma política de transparência total:

#### 3.1. Coleta de Dados do Usuário (Zero Tracking)



- **Sem Cadastro:** O acesso ao dashboard é livre e não requer criação de conta, login ou fornecimento de qualquer dado pessoal (PII).
- **Sem Rastreamento:** Não utilizamos *cookies* de rastreamento, pixels de publicidade ou ferramentas de *fingerprinting* para monitorar a navegação dos usuários.
- **Logs de Acesso:** O Project Aegis não armazena endereços IP dos visitantes. A plataforma hospedeira (GitHub) pode coletar logs técnicos de conexão para fins de segurança da infraestrutura, sobre os quais não temos controle ou acesso.

### 3.2. Tratamento de Dados de Terceiros (Vazamentos)

Ao exibir informações sobre vazamentos de dados (*Data Breaches*) provenientes da API *Have I Been Pwned*:

- O Project Aegis exibe apenas **metadados públicos** (Nome da empresa, Data, Volume de contas).
- **Compromisso Ético:** Jamais coletamos, armazenamos ou exibimos listas de e-mails, senhas, documentos ou dados pessoais das vítimas desses vazamentos.

## 4. Propriedade Intelectual e Licenciamento

### 4.1. Código-Fonte

O código-fonte do Project Aegis está licenciado sob a **Licença MIT**. Isso permite que qualquer pessoa estude, copie, modifique e distribua o software gratuitamente, desde que mantida a atribuição aos autores originais.

### 4.2. Atribuição de Dados (Fontes)

O conteúdo exibido no dashboard pertence aos seus respectivos detentores de direitos e é utilizado sob as políticas de uso justo (*Fair Use*) de suas APIs públicas:

- **Vulnerabilidades (CVE):** *National Institute of Standards and Technology (NIST)*.
- **Vazamentos:** *Have I Been Pwned* (cortesia de Troy Hunt).
- **Ameaças (OTX):** *AlienVault / AT&T Cybersecurity*.
- **Reputação de IP:** *AbuseIPDB*.

## 5. Conduta do Usuário

Ao utilizar o Project Aegis, o usuário concorda em:

1. Não utilizar a ferramenta para planejar ou executar ataques cibernéticos.
2. Não tentar explorar vulnerabilidades na infraestrutura do site (ex: ataques de XSS ou DDoS).
3. Não utilizar scripts automatizados (*scrapers*) de forma abusiva que possam comprometer a disponibilidade do serviço para outros usuários.

**Ao acessar e utilizar o Project Aegis, você declara estar ciente e de acordo com os termos acima descritos.**