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

RELATÓRIO DE CONFORMIDADE COM SEGURANÇA E PRIVACIDADE

Projeto: Project Aegis: Painel de Inteligência de Ameaças

Versão do Documento: 1.0

Data: 25/11/2025

---

1. Introdução e Escopo

Este documento detalha as diretrizes de Segurança da Informação e Privacidade adotadas no desenvolvimento do **Project Aegis**. O objetivo é demonstrar a conformidade da solução com as melhores práticas de desenvolvimento seguro (*Security by Design*) e com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo a integridade da infraestrutura e a privacidade dos usuários finais.

2. Arquitetura de Segurança (*Security by Design*)

A arquitetura do Project Aegis foi concebida para minimizar a superfície de ataque, eliminando vetores comuns de vulnerabilidade através de uma abordagem *Serverless* (sem servidor persistente).

2.1. Gestão de Credenciais e Segredos

O projeto interage com múltiplas APIs externas (NIST, AlienVault, AbuseIPDB). Para proteger as chaves de acesso (API Keys):

- **Segurança no Repositório:** Nenhuma credencial é armazenada no código-fonte (*hardcoded*) ou no histórico do Git.
- **GitHub Secrets:** Utilizamos o cofre digital do GitHub (Secrets) para armazenar variáveis sensíveis (API_NVD_CVE, API_OTX, etc.).
- **Injeção em Tempo de Execução:** As chaves são descriptografadas e injetadas nos *containers* de execução apenas durante o ciclo de vida do pipeline de CI/CD, sendo descartadas da memória imediatamente após o uso.

2.2. Segurança de Infraestrutura e Rede

- **HTTPS/TLS:** Todo o tráfego de dados entre o cliente (navegador do usuário) e o dashboard é criptografado utilizando o protocolo TLS 1.2+ (Transport Layer Security), provido nativamente pelo GitHub Pages. Isso garante a confidencialidade e integridade dos dados em trânsito.
- **Imutabilidade do Frontend:** O site é composto por arquivos estáticos (HTML/JS/JSON). Como não há um banco de dados SQL ou processamento *server-side* (como PHP/Java) exposto à internet, eliminam-se vulnerabilidades críticas como *SQL Injection* e *Remote Code Execution (RCE)* na camada de apresentação.

2.3. Integridade do Código (Supply Chain Security)

- **Controle de Versão:** Todas as alterações no código passam por controle de versão (Git), permitindo auditabilidade completa de quem alterou o quê e quando.
- **Dependências Seguras:** Os scripts Python utilizam gerenciadores de pacotes oficiais (pip) e bibliotecas consolidadas (requests, pandas), reduzindo o risco de introdução de vulnerabilidades de terceiros.

---

3. Privacidade e Conformidade com a LGPD (*Privacy by Design*)

O Project Aegis adota uma postura de "Privacidade por Padrão", respeitando os direitos dos titulares de dados.

3.1. Princípio da Minimização de Dados

Em estrita conformidade com a LGPD:

- **Não Coleta de Dados Pessoais:** O sistema **não possui** funcionalidades de cadastro, login ou identificação de usuários. Nenhum dado pessoal (PII) dos visitantes — como nome, e-mail, CPF ou IP — é coletado, armazenado ou processado pela equipe do Project Aegis.
- **Ausência de Rastreamento:** O dashboard não utiliza *cookies* de publicidade, *trackers* de terceiros ou ferramentas de *fingerprinting* para monitorar o comportamento dos usuários.

3.2. Tratamento Ético de Dados de Vazamentos (API HIBP)

Uma das funcionalidades do painel é exibir estatísticas sobre vazamentos de dados (*Data Breaches*). Para garantir a ética e a segurança:

- **Dados Agregados:** O sistema coleta apenas **metadados** públicos fornecidos pela API *Have I Been Pwned* (ex: Nome da empresa, Data do incidente, Número de contas afetadas).
- **Não Exposição de Vítimas:** O Project Aegis **jamais** baixa, armazena ou exibe listas de e-mails, senhas ou dados pessoais das vítimas desses vazamentos. O foco é a conscientização sobre o incidente, não a exposição do indivíduo.

---

4. Plano de Resposta a Incidentes

Apesar da arquitetura segura, foram mapeados cenários de risco e seus respectivos planos de mitigação:

Cenário de Risco	Probabilidade	Impacto	Plano de Mitigação / Resposta
Vazamento de Chave de API	Baixa	Médio	Revogação imediata da chave no portal do fornecedor (ex: NIST) e rotação das credenciais no GitHub Secrets.

Cenário de Risco	Probabilidade	Impacto	Plano de Mitigação / Resposta
Injeção de Dados Maliciosos via API	Média	Alto	Os scripts Python realizam saneamento (*sanitization*) dos dados recebidos antes de gerar os arquivos JSON, prevenindo ataques de XSS (*Cross-Site Scripting*) no dashboard.
Indisponibilidade do GitHub	Baixa	Baixo	Como o site é estático, ele pode ser rapidamente migrado para qualquer outra hospedagem (Netlify/Vercel) ou rodar localmente sem perda de funcionalidade.

---

5. Conclusão

A análise técnica confirma que o **Project Aegis** atende aos requisitos de segurança e privacidade esperados para uma aplicação moderna.

A decisão arquitetural pelo modelo *Serverless* e a política de "Zero Coleta de Dados Pessoais" garantem que o projeto não apenas cumpre a legislação vigente (LGPD), mas também estabelece um padrão elevado de confiança e transparência para com seus usuários.

Aprovado por: Marcos Vinícius Rocha *Product Owner & Líder de Segurança*