Vion: Diagnóstico Inteligente para Redes Domésticas

Error 504

Emile Cristine Gomes Nogueira

Ivan Henrique Ferreira da Silva

Mariana Cardamoni Araripe da Silveira

Pedro Santana Filipini

Rafael de Colle

ETEC de Hortolândia

São Paulo, Agosto, 2025

DESAFIO DOS DADOS 2025

SUMÁRIO

PREÂMBULO

"Um bug não é um erro, é um professor disfarçado."

(Rafael de Colle)

Resumo:

O presente trabalho apresenta o desenvolvimento do Vion: Diagnóstico Inteligente para Redes Domésticas, uma solução de segurança digital voltada para redes domésticas e pequenos escritórios (SOHO), com foco na prevenção de ciberataques e educação em segurança digital.

O projeto surge diante do crescimento exponencial de ataques cibernéticos ao Brasil, causada principalmente pelo aumento de vulnerabilidades em dispositivos IoT e roteadores residenciais, especialmente com a expansão do trabalho remoto e do uso doméstico da Internet. O cenário nacional de cibersegurança revela que o Brasil é o principal alvo na América Latina, com bilhões de tentativas de invasão anualmente e custos médios de violação de dados estimados em mais de 7 milhões de reais.

Apesar disso, muitas vulnerabilidades poderiam ter sido prevenidas com medidas simples, como atualização de firmware, fortalecimento de senhas e desativação de funções de risco. A Política Nacional de Cibersegurança (PNCiber) de 2023 busca enfrentar tais desafios, mas depende da colaboração entre governo, fabricantes e usuários residenciais.

O Vion propõe transformar a cibersegurança de uma tarefa complexa em um hábito simples e acessível. A solução consiste em um aplicativo móvel multiplataforma, que analisa redes Wi-Fi, detecta vulnerabilidades e orienta o usuário de forma prática, mesmo sem conhecimento técnico. A Inteligência Artificial permite bloquear IPs suspeitos, isolar dispositivos comprometidos e até avaliar mensagens suspeitas de phishing, dando instruções claras do que fazer.

Além de proteger o usuário, o Vion educa sobre boas práticas, fortalecendo a segurança digital tanto individual quanto coletiva. O projeto contribui para os ODS 9, 16 e 17, garantindo acesso seguro à tecnologia, prevenindo crimes digitais e promovendo a alfabetização tecnológica.

Em resumo, o Vion não é só uma ferramenta de proteção: é um guia prático para tornar a cibersegurança acessível, intuitiva e parte do dia a dia, protegendo indivíduos e fortalecendo a segurança digital do país.

1. JUSTIFICATIVA

1.1 A SEGURANÇA EM REDES DOMÉSTICAS

A segurança cibernética em redes domésticas tornou-se um uma preocupação crítica, especialmente com o crescimento de dispositivos IoT (*Internet of Things*[1]) e pela expansão do modelo de trabalho *home office* (FERNANDES et al., 2015). Roteadores sem fio e modems, que são dispositivos essenciais para a interconexão em redes, tornaram-se alvos primários para ataques sofisticados, como phishing e ransomware[2] (ITFORUM, 2024). A principal razão para isso é que, muitas vezes, esses dispositivos operam com configurações inseguras, como senhas padrão ou recursos desnecessários habilitados (por exemplo, WPS[3] ou acesso remoto), o que amplia as possibilidades de exploração por agentes mal-intencionados.

Essas vulnerabilidades podem ser exploradas de diferentes formas para comprometer a integridade da rede. O phishing, aliado ao *DNS hijacking*[4], por exemplo, permite que criminosos redirecionem os usuários para sites falsos e coletem dados sensíveis, como credenciais bancárias (TEIXEIRA, 2021). Além disso, quando um roteador é comprometido, ele pode servir como porta de entrada para ataques direcionados a dispositivos IoT conectados, como câmeras de segurança ou assistentes virtuais (ANALYTICS, 2023). Dessa forma, ameaças que antes se restringiam ao computador do usuário agora se expandem para todo o ecossistema digital presente no ambiente doméstico.

Nesse cenário, especialistas defendem que a proteção técnica por si só não é suficiente se não vier acompanhada de conscientização. A dimensão educativa surge como o fator chave para reduzir vulnerabilidades, pois os usuários representam a linha de frente contra ataques digitais. Como destaca Kelly Begosso, bacharel em Sistemas de Informação, pós-graduada em Educação e instrutora da Cisco-Netacademy (2025), *"a educação de usuários domésticos pode e realmente reduz significativamente as vulnerabilidades. Ao capacitar os usuários com conhecimento, eles se tornam mais aptos a reconhecer e evitar golpes, adotar boas práticas de senha, manter software atualizado, usar ferramentas de segurança e gerenciar a privacidade."*

Como destaca Marcondes (2008), as formas mais comuns de configurar redes em casa incluem conexões por cabo e sem fio. Embora a conexão cabeada seja mais estável e rápida, a opção sem fio tornou-se a mais utilizada devido à sua praticidade,

---

[1] **Internet of Things (IoT)**: refere-se à interconexão de dispositivos físicos com a internet, permitindo a coleta e troca de dados, como câmeras, sensores e eletrodomésticos inteligentes.
[2] **Fishing e ransomware**: *Phishing*: fraude digital que busca enganar o usuário para roubo de dados; *Ransomware*: malware que sequestra arquivos e exige pagamento para devolução.
[3] **WPS**: abreviação para *Wi-Fi Protected Setup*, recurso de configuração rápida de redes sem fio que, apesar de prático, apresenta vulnerabilidades que facilitam invasões.
[4] **DNS hijacking**: técnica de ataque que altera o tráfego de DNS, redirecionando usuários para sites falsos para roubo de informações ou distribuição de malware.

custo-benefício e versatilidade. Isso porque ela permite conectar uma ampla gama de dispositivos móveis (como smartphones, televisões, notebooks e tablets) desde que compatíveis com Wi-Fi, garantindo mobilidade e conveniência dentro de uma área de cobertura do sinal.

Em síntese, a segurança em redes domésticas deixou de ser uma preocupação individual e passou a ocupar um papel fundamental na proteção digital contemporânea. As vulnerabilidades exploradas em roteadores e dispositivos IoT demonstram que a defesa digital do ambiente residencial é parte fundamental da cibersegurança como um todo, uma vez que qualquer brecha pode servir de porta de entrada para ataques de maior alcance e proporção. Desta forma, evidencia-se que a segurança doméstica não pode ser analisada isoladamente, mas deve ser considerada dentro do contexto nacional de cibersegurança, onde políticas públicas, iniciativas coletivas e campanhas de conscientização desempenham papel fundamental.

1.2 CENÁRIO NACIONAL DE CIBERSEGURANÇA

O Brasil está entre os países da América Latina mais visados por ciberataques, com bilhões de tentativas de invasão anualmente (ITFORUM, 2024; JOBIM, 2024). Relatórios indicam que os ataques a roteadores domésticos no Brasil aumentaram 18% em 2023 (ANALYTICS, 2023), e que os custos médios de violações de dados chegam a R$6,75 milhões (ITFORUM, 2024).

Apesar desses números alarmantes, boa parte das vulnerabilidades poderiam ser evitadas com medidas simples, como desativar funções de risco, atualizar firmwares[5] e reforçar senhas e credenciais (TEIXEIRA, 2021). Oliveira e Souza (2024) destacam que muitos usuários nem sabem como acessar o painel administrativo de seus roteadores, mostrando uma lacuna preocupante no conhecimento básico de segurança.

A Política Nacional de Cibersegurança (PNCiber)[6], lançada em 2023, foi criada para enfrentar esses desafios, mas sua eficácia depende da colaboração entre governo, fabricantes e usuários. Enquanto roteadores corporativos já vêm com firewalls[7] e monitoramento avançado, os modelos residenciais muitas vezes nem recebem atualizações de segurança básicas (FERNANDES et al., 2015).

[5] **Firmware**: conjunto de programas gravados no hardware que controlam seu funcionamento básico e permitem que o dispositivo opere corretamente.
[6] **Política Nacional de Cibersegurança (PNCiber)**: estratégia governamental lançada em 2023 para promover a proteção de infraestrutura crítica e conscientização sobre segurança digital no Brasil.
[7] **Firewall**: sistema de segurança que monitora e controla o tráfego de rede, bloqueando acessos não autorizados e protegendo dispositivos contra ameaças externas.

1.3 ESTUDO DE CASO: PHISHING DA VIVO E O MALWARE GRANDOREIRO

A evolução das ameaças digitais fez do **phishing** uma das práticas mais recorrentes e sofisticadas no cenário da cibersegurança. Um caso recente, divulgado pela empresa de segurança ESET (2024), mostrou como golpistas usam técnicas de **spoofing**[8] para imitar a identidade visual da operadora telefônica Vivo. Nessa fraude, mensagens falsas eram enviadas aos usuários simulando notificações de faturas digitais próximas ao vencimento.

Os criminosos exploram a **urgência** sentida pelo usuário. Ao criar a impressão de um prazo curto para pagamento, as pessoas tendem a agir de forma impulsiva, o que reduz sua capacidade de pensamento e análise crítica e aumenta a probabilidade de sucesso do golpe. É explorando e manipulando o comportamento humano que essas fraudes se tornam ainda mais perigosas e eficazes.

Ao contrário de ataques de phishing comuns, que geralmente buscam apenas enganar o usuário para roubar informações pessoais ou dados de cartão de crédito, esse golpe tinha um objetivo mais complexo: a instalação do **malware**[9] **Grandoreiro**. Diferente de vírus tradicionais, esse tipo de trojan[10] funciona como um "dropper",[11] que utiliza a fraude inicial (o phishing) apenas como uma porta de entrada para introduzir um programa malicioso mais sofisticado no dispositivo da vítima.

O Grandoreiro é classificado como um *Tiny Banking Trojan*[12], documentado desde 2017 e projetado especificamente para atacar o setor financeiro. Entre suas principais funções estão a injeção de código malicioso em páginas de banco, o que permite alterar a interface exibida ao usuário e coletar coletar informações sem que ele perceba, e a captura de teclas digitadas no teclado (keylogging[13]), recurso que possibilita registrar logins, senhas e outros dados sigilosos em tempo real (ESET, 2024). Combinando essas técnicas, o trojan se torna altamente eficaz no roubo de credenciais financeiras, permitindo que os criminosos acessem contas bancárias de forma efetiva e potencialmente causem prejuízos significativos às vítimas.

---

[8] **Spoofing**: técnica usada por criminosos cibernéticos para se passar por outra pessoa ou entidade confiável, com o objetivo de enganar a vítima e obter acesso a informações, dados ou dinheiro. Essa prática pode envolver a falsificação de endereços de e-mail, números de telefone, endereços IP, sites e até mesmo a localização geográfica de um dispositivo.

[9] Malware: programa criado com intenção maliciosa, capaz de danificar o dispositivo, roubar dados ou comprometer a segurança do usuário.

[10] Trojan: tipo de malware que se disfarça como um programa legítimo ou inofensivo, mas quando executado realiza ações prejudiciais, como roubo de informações ou instalação de outros malwares.

[11] Droppers: são um subtipo de malware que tem como propósito "liberar" outro arquivo executável malicioso.

[12] Tiny Banking Trojan: O Tiny Banker Trojan (TBT), ou Tinba, é um trojan que infecta dispositivos de usuários finais e tenta comprometer suas contas financeiras e roubar fundos.

[13] Keylogging:

1.4 PROPOSTA DA SOLUÇÃO

Para enfrentar esses desafios, propomos o desenvolvimento de uma ferramenta integrada e automatizada capaz de **diagnosticar vulnerabilidades**, **orientar o usuário e incentivar boas práticas de segurança digital**. O projeto visa transformar a cibersegurança de uma tarefa complexa e reativa em um hábito simples, proativo e acessível, democratizando a proteção digital para todos.

A relevância desse tipo de recurso já é reconhecida por profissionais da área, que destacam o papel da automação como aliada na proteção de usuários leigos. Ao reduzir a necessidade de conhecimento técnico e intervir antes que ameaças se concretizem, a tecnologia passa a agir como uma camada extra de defesa. Nesse sentido, Begosso (2025) ressalta: *"ferramentas automatizadas têm um papel enorme (e crescente) na melhoria da segurança digital, especialmente para usuários leigos. A tecnologia certa pode proteger mesmo quem não entende nada de cibersegurança, justamente porque automatiza decisões complexas ou intervém antes que algo perigoso aconteça."*

O foco principal são os usuários residenciais e pequenos escritórios, que formam a maior parte das conexões domésticas e costumam ser mais vulneráveis. Indiretamente, toda a sociedade se beneficia, pois a redução de falhas em redes domésticas contribui para um ambiente digital mais seguro em escala nacional.

A viabilidade do projeto é garantida pela combinação de tecnologias de ciência de dados, machine learning e integração com APIs de segurança consolidadas, implementadas por meio de um aplicativo móvel multiplataforma. O momento é estratégico: com o crescimento da Internet das Coisas (IoT) e o fortalecimento de políticas nacionais como a PNCiber (2023), o projeto ganha relevância tanto social quanto técnica.

1.5 O PAPEL DA INTELIGÊNCIA ARTIFICIAL NA PROPOSTA

A Inteligência Artificial (IA) é o ponto central da nossa proposta para lidar com a complexidade crescente dos ataques cibernéticos. Sistemas baseados em IA conseguem analisar grandes volumes de dados em tempo real (RODRIGUES, 2025) e identificar padrões estranhos no tráfego de rede, permitindo detectar ameaças antes que causem danos significativos (CRUZ; CASEMIRO, 2025).

Outra característica importante é a automação que a IA proporciona. Com ela, o aplicativo poderá, por exemplo, bloquear IPs suspeitos ou isolar dispositivos comprometidos sem que o usuário precise fazer nada, reduzindo riscos e tornando a segurança mais prática, especialmente para quem não tem conhecimento técnico.

Além disso, o sistema funciona como um guia para o usuário, traduzindo informações técnicas em recomendações claras e passos concretos para corrigir problemas. Dessa forma, o projeto não se limita a detectar vulnerabilidades, mas também contribui para a criação de hábitos de segurança proativos e conscientes.

Exemplo de atuação prática da IA:

O usuário poderá, por exemplo, enviar um print de um SMS suspeito e perguntar: *"Recebi esta mensagem, é golpe?"* O sistema analisará o conteúdo e fornecerá um retorno detalhado:

- **Análise da mensagem**: palavras típicas de phishing, como *urgente*, *atualização de senha* ou *risco de bloqueio*.
- **Sinais suspeitos detectados**: links encurtados, linguagem de urgência, domínio diferente do banco oficial.
- **Veredito**: Perigoso – não clique!
- **Orientações para o usuário**: ignore a mensagem, exclua o SMS e, se necessário, entre em contato diretamente com o banco pelo aplicativo oficial.

Além disso, a IA poderá responder perguntas gerais sobre cibersegurança, dando dicas sobre senhas seguras, configuração de roteadores, atualização de sistemas e cuidados com links suspeitos. Assim, o usuário não só recebe proteção automática, como também aprende boas práticas de forma contínua, tornando a segurança digital mais acessível e consciente.

Figura 1 - Interface da Inteligência Artificial no aplicativo

1.6 OBJETIVOS DE DESENVOLVIMENTO SUSTENTÁVEL (ODS)

O Vion, como solução de segurança digital para redes domésticas, contribui diretamente para diversos Objetivos de Desenvolvimento Sustentável (ODS) estabelecidos pela ONU, destacando-se principalmente nos ODS 9, 16 e 17.

ODS 9 – Indústria, Inovação e Infraestrutura

O Vion está alinhado ao objetivo 9.c, que busca aumentar significativamente o acesso às tecnologias de informação e comunicação garantindo internet universal e acessível, principalmente em países menos desenvolvidos. Mais do que fornecer conexão, o Vion assegura que ela seja segura, estável e fácil de usar, mesmo para quem tem pouca familiaridade com tecnologia. Assim, fortalece a infraestrutura digital básica e promove um acesso mais justo e significativo à internet.

ODS 16 – Paz, Justiça e Instituições Eficazes

O Vion atua na prevenção de crimes cibernéticos, que constituem formas modernas de crime organizado, contribuindo para os objetivos 16.4 e 16.a:

- **16.4:** Reduz fluxos financeiros ilícitos gerados por fraudes bancárias, roubo de dados e ataques de ransomware, prevenindo o uso de redes comprometidas para atividades ilegais.
- **16.a:** Fortalece a capacidade individual dos cidadãos de se proteger digitalmente, descongestionando o trabalho das autoridades policiais e de segurança cibernética. Essa abordagem preventiva torna o ecossistema digital mais resiliente, eficiente e seguro.

ODS 17 – Parcerias e Meios de Implementação

O Vion também atua como uma ferramenta de capacitação, alinhando-se ao objetivo 17.8, que busca ampliar o uso de tecnologias para educação em ciência, tecnologia e inovação. Além de identificar vulnerabilidades, o Vion ensina os usuários com guias passo a passo, promovendo alfabetização digital em segurança cibernética e criando uma base sólida para novas inovações tecnológicas.

1.7 OBJETIVOS

Objetivo Geral

Nosso Objetivo Geral é desenvolver uma solução acessível, por meio de um aplicativo móvel, que realize a análise automatizada de redes domésticas, identifique vulnerabilidades de segurança e forneça orientações claras para sua correção, visando aprimorar a proteção digital dos usuários de forma intuitiva, eficiente e educativa, fortalecendo a segurança individual e coletiva no ambiente digital.

Objetivos Específicos

- **Mapear e analisar vulnerabilidades comuns em roteadores domésticos**, como firmwares desatualizados e o uso de configurações padrão, com base na literatura de referência (BERTOLINO et al., 2024);
- **Desenvolver um protótipo funcional de aplicativo móvel**, utilizando React Native (front-end) e Node.js (back-end), garantindo compatibilidade multiplataforma;
- **Projetar uma interface intuitiva e acessível**, priorizando a experiência do usuário para que, mesmo aqueles que não possuem conhecimento técnico, consigam utilizar a solução com facilidade;
    - **Criar um painel de monitoramento simples e informativo**, que apresente o status de segurança da rede, destacando riscos e orientando o usuário sobre como corrigi-los;
- **Implementar mecanismos automatizados de análise de redes Wi-Fi**, capazes de identificar falhas de segurança e vulnerabilidades em tempo real;
- **Gerar relatórios detalhados** sobre os riscos e fornecer orientações guiadas para a correção das falhas identificadas;
- **Integrar APIs de segurança cibernética** (como Have I Been Pwned, Shodan e AbuseIPDB) para detectar vazamentos de credenciais, dispositivos vulneráveis e endereços IP maliciosos;
- **Promover educação digital e conscientização sobre proteção de dados**, combinando tecnologia e instruções passo a passo para fortalecer a cultura de segurança entre os usuários;
- **Avaliar continuamente a eficácia do aplicativo**, com base em feedback de usuários e testes, aprimorando recursos e garantindo aderência às melhores práticas de cibersegurança.

1.8 PÚBLICO-ALVO

O público alvo deste projeto são usuários residenciais e pequenos escritórios (SOHO), que representam a maior parte das conexões domésticas e, geralmente, não têm conhecimento técnico sobre segurança digital. Essa falta de familiaridade torna esse grupo mais vulnerável a ataques como phishing, ransomware e invasões a dispositivos IoT.

A proposta do Vion é oferecer suporte direto a esses usuários, fornecendo ferramentas automatizadas e orientações claras para aumentar a proteção digital. Indiretamente, toda a sociedade se beneficia: ao reduzir falhas nas redes domésticas, o projeto ajuda a fortalecer a segurança coletiva, criando um ambiente digital mais confiável em nível nacional.

2. MATERIAIS E MÉTODOS

2.1 MATERIAIS UTILIZADOS (PROTÓTIPOS E MÍDIAS)

Os principais recursos utilizados no desenvolvimento do protótipo do projeto foram:

- **Figma**: para design de telas e fluxos de navegação;
- **React Native, CSS, TypeScript e Tailwind:** aplicados na criação de protótipos funcionais da interface do aplicativo;
- **Node.js:** utilizado em testes iniciais para análise de dados do roteador;
- **GitHub**: repositório para versionamento do código-fonte e organização colaborativa.
- **Vercel**: hospedagem do protótipo web.
- **Fontes de Pesquisa:** artigos científicos, relatórios de cibersegurança, manuais de fabricantes e bases públicas de dados de vulnerabilidades.

2.2 MATERIAIS PLANEJADOS (VERSÃO FINAL DA SOLUÇÃO)

- **React Native:** para coleta de informações de rede, como IP do roteador via gateway padrão.
- **Node.js:** para implementação da lógica de análise e configuração de segurança dos roteadores.
- **Python:** para desenvolvimento dos algoritmos de Inteligência Artificial e scripts de análise de tráfego.
- **Bibliotecas de IA:** Scikit-learn e TensorFlow, para modelos de detecção de anomalias.
- **APIs de Segurança:** Have I Been Pwned, Shodan e AbuseIPDB, para enriquecimento da análise de riscos.

2.3 MÉTODOS

O desenvolvimento do projeto foi fundamentado em uma abordagem integrada à Ciência de Dados, Engenharia de Software e pesquisa exploratória em cibersegurança.

1. **Pesquisa Bibliográfica e Documental:** levantamento de estudos, relatórios e boas práticas de segurança em redes domésticas, utilizados tanto para validar a relevância do problema quanto para traduzir configurações técnicas em orientações simplificadas e acessíveis ao público-alvo. Além disso, essa etapa foi fundamental para identificar as vulnerabilidades comuns em redes

domésticas e boas práticas de segurança, utilizadas como base para os conteúdos do aplicativo.
2. **Modelagem Conceitual:** definição dos requisitos do sistema a partir da análise do problema e do público-alvo.
3. **Prototipagem:** elaboração de telas no Figma e desenvolvimento de protótipos parciais em React Native, priorizando a experiência do usuário.
4. **Planejamento da Arquitetura Completa:** integração futura entre interface, back-end em Node.js e algoritmos de IA em Python.
5. **Validação Pedagógica:** tradução das configurações técnicas em orientações claras e acessíveis, garantindo que usuários sem conhecimento avançado possam aplicar as recomendações.

2.4 MÍDIAS UTILIZADAS

O projeto contou com quatro mídias principais, contando com as obrigatórias pelo desafio, que se complementam entre si e tornam a entrega mais completa e acessível:

- **Relatório**: documento técnico que reúne toda a fundamentação teórica, a metodologia aplicada, os materiais utilizados, os objetivos e os resultados esperados. Serve como registro formal do projeto e referência detalhada para futuras evoluções da solução.
- **Vídeo de Apresentação**: material audiovisual que resume os pontos principais do projeto de forma clara e dinâmica. Facilita a compreensão do problema, da solução proposta e do impacto esperado, funcionando como complemento didático ao relatório escrito.
- **Protótipo no Figma**: apresenta a interface do usuário e os fluxos de navegação da solução. Permite visualizar a experiência prática do usuário, criando uma ponte entre a teoria do relatório e a aplicação funcional.
- **Site Hospedado no GitHub/Vercel**: disponibiliza o protótipo de forma interativa. A hospedagem no Vercel garante acesso rápido e facilita a demonstração pública da solução, permitindo que interessados testem o conceito em tempo real.

Essas mídias não funcionam isoladamente, mas se conectam: o relatório traz a base conceitual e técnica; o vídeo traduz essa base para uma comunicação mais acessível e atraente; o Figma mostra visualmente a interface; e o site permite a interação prática com os protótipos. Juntas, formam um conjunto coeso que documenta, explica, exemplifica e torna o projeto tangível.

3. RESULTADOS

3.1 RESULTADOS TÉCNICOS

Os resultados do projeto Vion foram obtidos principalmente por meio da análise de dados de redes, o que nos permitiu identificar vulnerabilidades comuns, como senhas padrão, firmware desatualizado e dispositivos IoT configurados de forma insegura, além de oportunidades de melhoria na segurança digital.

A partir da análise, foram identificadas ações imediatas para aumentar a proteção digital:

- Alteração de senhas padrão e fortalecimento de credenciais;
- Atualização de firmware e bloqueio de funções de risco em roteadores;
- Configuração segura de dispositivos IoT e conscientização sobre boas práticas de segurança.

Essas medidas podem ser aplicadas imediatamente pelos usuários pelo nosso aplicativo, aumentando a proteção de redes domésticas e pequenos escritórios.

A longo prazo, pensamos em oportunidades aplicáveis para soluções mais sustentáveis e escaláveis, como:

- **Monitoramento automático das redes**, identificando vulnerabilidades em tempo real;
- **Alertas e relatórios periódicos** para educar os usuários e incentivar hábitos preventivos;
- **Evolução contínua do sistema** para acompanhar novas ameaças e tecnologias emergentes, garantindo segurança adaptativa ao longo do tempo.

3.2 EDUCAÇÃO DO USUÁRIO E CULTURA DE SEGURANÇA

Além dos avanços técnicos, o projeto também mostrou que a educação digital é peça-chave para reduzir as vulnerabilidades em redes domésticas. A tecnologia, por si só, não é suficiente: sem conhecimento básico de segurança, muitos usuários permanecem expostos a golpes simples, como phishing, senhas fracas ou descuido com atualizações.

Como destaca Begosso (2025), *"a educação de usuários domésticos pode e realmente reduz significativamente as vulnerabilidades. Ao capacitar os usuários com conhecimento, eles se tornam mais aptos a reconhecer e evitar golpes, adotar boas práticas de senha, manter software atualizado, usar ferramentas de segurança e gerenciar a privacidade."*

Isso mostra que a segurança não é só técnica, mas também cultural. Quando os usuários passam a enxergar práticas preventivas como parte da rotina, e não apenas como obrigações técnicas, cria-se um ambiente digital mais forte e resistente. Nesse sentido, o Vion não se limita a oferecer uma ferramenta automatizada: ele também contribui para espalhar boas práticas e fortalecer a cultura de segurança digital, ajudando a construir um espaço online mais confiável.

3.3 COLABORAÇÃO E APRENDIZAGEM

Do ponto de vista técnico, o projeto permitiu que a equipe aplicasse na prática conceitos de ciência de dados, como coleta, tratamento e visualização de informações, voltados para a análise de vulnerabilidades em redes domésticas. Os integrantes também ganharam experiência no desenvolvimento de aplicativos, integração de APIs e uso de ferramentas de inteligência artificial, fortalecendo habilidades essenciais em programação, análise de dados e segurança cibernética.

No aspecto socioemocional, o trabalho em equipe foi fundamental para o desenvolvimento de competências interpessoais importantes. A colaboração exigiu que cada integrante aprendesse a ouvir diferentes pontos de vista, lidar com conflitos, organizar tarefas em grupo e tomar decisões coletivas. Essas experiências reforçaram habilidades de comunicação, empatia e capacidade de trabalhar em ambientes colaborativos, que são valiosas para a vida profissional.

Em conclusão, o projeto Vion não apenas entregou uma solução tecnológica eficiente, mas também proporcionou crescimento técnico e pessoal para toda a equipe. A experiência mostrou que projetos de ciência de dados podem gerar impacto real, ao mesmo tempo em que ensinam habilidades práticas e socioemocionais importantes para o futuro.

REFERÊNCIAS

BEGOSSO, Kelly. Bacharel em Sistemas de Informação, pós-graduada em Educação e instrutora da Cisco-Netacademy. Entrevista concedida à equipe do projeto *Vion*. Hortolândia, 2025.

OLIVEIRA, Cristian Da Silva; SOUZA, Paulo Luiz Fernandes De. OLIVEIRA, Cristian da Silva; SOUZA, Paulo Luiz Fernandes de. **Segurança cibernética em ambientes residenciais**, 2024. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", Americana, 2024.. Repositório Institucional do Conhecimento - RIC-CPS, 2024. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/29731. Acesso em: 23 jul. 2025.

TEIXEIRA, Cleyson Fernando Araújo. **Segurança cibernética em redes modernas: como proteger e mitigar ataques cibernéticos**. 2021. 93 f. Monografia (Graduação em Engenharia de Controle e Automação) - Escola de Minas, Universidade Federal de Ouro Preto, Ouro Preto, 2021. Disponível em: http://www.monografias.ufop.br/handle/35400000/3567. Acesso em: 25 jul. 2025.

RODRIGUES, W. B. **Aplicação de inteligência artificial na detecção de ameaças em redes de computadores**. *Revista Di Fatto*, Joinville, v. 4, 2025. ISSN 2966-4527. DOI: 10.5281/zenodo.15083092. Disponível em: https://revistadifatto.com.br/artigos/aplicacao-de-aplicacao-de-inteligencia-artificial-na-deteccao-de-ameacas-em-redes-de-computadores/. Acesso em: 5 ago. 2025.

BERTOLINO, Guilherme; TAFFAREL, Françoa; PEREIRA JUNIOR, Lourenço Alves. **Segurança cibernética em roteadores Wi-Fi: abordagem automatizada para coleta e análise de firmware**. In: SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 24., 2024, São José dos Campos. *Anais* [...]. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 396–400. DOI: https://doi.org/10.5753/sbseg_estendido.2024.241625. Acesso em: 5 ago. 2025.

CERT.BR. **CERT.br - Estatísticas**. Disponível em: https://stats.cert.br/incidentes/. Acesso em: 5 ago. 2025.

MANNARA, Barbara. **Golpe usa boleto falso da Vivo para roubar dados bancários; proteja-se**. Tilt Uol, 2022. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2022/07/26/criminosos-usam-boleto-falso-da-vivo-para-enganar-vitimas-e-espalhar-virus.htm. Acesso em: 09 ago. 2025.

ALECRIM, Emerson. **Fatura falsa em nome da Vivo espalha malware que rouba dados bancários**. Tecnoblog, 2022. Disponível em: https://tecnoblog.net/noticias/fatura-falsa-em-nome-da-vivo-espalha-malware-que-rouba-dados-bancarios/. Acesso em: 09 ago. 2025.

TAFFAREL, Françoa; DE FREITAS, Osmany Barros; JUNIOR, Lourenço Alves Pereira. **Análise de vulnerabilidades em larga escala nos Roteadores Wi-Fi por meio de Web-Fuzzing**. Anais do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG), 2023. Disponível em: https://doi.org/10.5753/sbseg.2023.233526. Acesso em: 10 ago. 2025.

TAFFAREL, Françoa; DE FREITAS, Osmany Barros; JUNIOR, Lourenço Alves Pereira; DOS SANTOS, Aldri Luiz. **Caracterização das vulnerabilidades dos roteadores Wi-Fi no mercado brasileiro**. Anais do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSEG), 2023. Disponível em: https://doi.org/10.5753/sbrc.2023.487. Acesso em: 10 ago. 2025.

Custo médio de violações de dados no Brasil é de R$ 6,75 milhões: Valor é 9% maior do que no ano passado, indica relatório anual da IBM. Setores de saúde e serviços experimentam maiores prejuízos. itforum, 2024. Disponível em: https://itforum.com.br/noticias/custo-violacoes-de-dados-no-brasil-r-675-milhoes/. Acesso em: 19 ago. 2025.