

PROPOSTA DE INFRAESTRUTURA DE REDE ACESSÍVEL PARA GARANTIR ACESSO SEGURO E EFICIENTE À INTERNET EM COMUNIDADES RIBEIRINHAS DA AMAZÔNIA.

**Desbravando Conexões: Desenvolvendo Soluções Interativas baseada em Redes de
Computadores para a Comunidade.**

Matheus Eduardo Lima Pinheiro
Universidade da Amazônia-UNAMA
matheusedulimapinheiro@gmail.com

Mauro Margalho Coutinho
Universidade da Amazônia-UNAMA
mauro.margalho@unama.br

RESUMO

Este artigo tem como objetivo propor uma forma segura de acesso a redes locais em comunidades ribeirinhas, sugerindo uma infraestrutura de rede com alto custo-benefício que garanta acesso seguro à internet para pessoas em áreas distantes dos centros urbanos. O projeto visa promover o letramento digital através de recursos educacionais, informativos e de desenvolvimento humano, contribuindo para a melhoria da qualidade de vida populacional. Para assegurar um acesso à internet seguro e controlado, será implementado um recurso conhecido como captive portal, solução que garante a autenticidade dos usuários e protege grupos socialmente vulneráveis contra possíveis ameaças. A questão central do projeto é garantir que essas comunidades possam usufruir dos benefícios da conectividade de maneira segura e inclusiva, utilizando captive portals como uma ferramenta crucial para essa proteção, proporcionando não apenas segurança, mas também uma boa usabilidade ao se conectar.

Palavras-Chave: Captive Portal; Inclusão Digital; Infraestrutura de Rede; Comunidades Ribeirinhas;

1. INTRODUÇÃO

“As redes Wi-Fi trouxeram uma grande praticidade para vida das pessoas, proporcionando grande liberdade no acesso, baixo custo de implementação, além de facilidade de instalação e configuração (Ramachandran, 2011; Rufino, 2014). Entretanto, novas vulnerabilidades surgiram com a adoção crescente e maciça dessa nova tecnologia. A frequência de tentativas de violação e ataques a essas redes tem se intensificado nos últimos anos (Ramachandran, 2011). Administradores sem muito conhecimento acabam por negligenciar as práticas de gestão e segurança das redes Wi-Fi (Ramachandran, 2011; Rufino, 2014).” (Figueiredo et al., 2020, p. 2).

“A inclusão digital permite o acesso a uma gama de serviços públicos e privados, proporcionando o acesso a coleções de bibliotecas, acesso à educação, interação social, entretenimento digital e assistência médica [Fanea-Ivanovici and Pană, 2020]. Entre as barreiras à inclusão digital, poderíamos listar: i) falta de infraestrutura, ii) custos de acesso e acessibilidade, iii) falta de instrução e iv) motivação sociocultural. No Brasil, a precariedade do acesso à internet nas escolas públicas forma uma quinta barreira [Fernandes et al., 2020]”. (Gomes et al., 2021, p. 1).

“O bairro de São João está localizado a nordeste do município de Abaetetuba, seu número de habitantes é de aproximadamente 4.459 (IBGE 2010). Segundo o censo do IBGE, no ano de 2010 o município possuía 141.100 habitantes; em 2017, o IBGE estimou 153.380. Ou seja, em um curto intervalo de tempo (sete anos) houve um acréscimo de mais de 12.280 habitantes, o que compreende no aumento da infraestrutura municipal (IBGE, 2016).” (Dias, p. 8)

“Os grandes empreendimentos instalados no estado do Pará criaram um conjunto de modificações territoriais e impulsionaram as migrações de pessoas em busca de empregos e melhores condições de vida em várias cidades, a título de exemplo, as cidades de Barcarena, Marabá e Parauapebas, que em seus territórios possuíam atividades ligadas direta e indiretamente aos grandes empreendimentos minerais. A Região de Carajás no sudeste paraense é um desses lócus que atreladas às fontes minerais de ferro principalmente, ferrovia e porto de Itaqui entre o Pará e o Maranhão que intensificaram

as migrações e a urbanização das cidades através da presença dos grandes empreendimentos num cenário de avanços e conflitos territoriais que marcaram as configurações socioespaciais das cidades do sudeste paraense.” (Machado et al., 2024, p. 2).

Diante desse cenário, a necessidade de enfrentar a problemática da falta de uma infraestrutura de rede minimamente segura torna-se evidente. A proposta de um Captive Portal surge como uma solução eficaz, utilizando uma infraestrutura que não é facilmente prevista por indivíduos com intenções maliciosas, tornando o acesso à rede local (LAN) mais seguro. As ferramentas utilizadas neste projeto são selecionadas para diminuir o risco de fraudes e garantir a segurança no acesso à rede.

Captive Portals figuram como uma possibilidade de aumentar os níveis de segurança e são páginas web locais que os usuários devem visualizar e interagir antes de obter acesso à rede. Em outras palavras, os usuários são obrigados a se autenticar para poderem utilizar demais recursos na rede. No caso deste projeto, foi desenvolvida tanto uma página de login quanto de cadastro. No entanto, é comum que esses sistemas já possuam uma base de dados pronta, com usuários previamente identificados no banco de dados, contendo informações como nome, e-mail, senha, e o momento de registro de cadastro, conhecido como timestamp.

Além disso, no sistema operacional utilizado, OpenWRT, é possível monitorar em tempo real quem está conectado à rede e quantas pessoas estão utilizando-a, através do interno dos dispositivos, conhecido como MAC (Medium Access Control)

O endereço MAC é um identificador único atribuído a cada dispositivo de rede. Ele é composto por uma série de números e letras e é utilizado para identificar dispositivos em uma rede local (LAN). Diferente de um endereço mais genérico, que pode mudar conforme a conexão do dispositivo, o endereço MAC é fixo e específico para o hardware de cada dispositivo, pois vem gravado de fábrica. Isso permite ao administrador da rede rastrear e controlar quais dispositivos estão conectados, aumentando a segurança e a capacidade de gestão da rede.

Este projeto servirá como suporte para o Dispositivo S.A.N.D.R.O. Esse dispositivo atuará como meu provedor de internet (ISP) (MARGALHO, Diego. Disponível em: <https://www.margalho.pro.br/site-humanidades/>.)

2.FUNDAMENTAÇÃO TEÓRICA

O trabalho apresentado foca em uma pesquisa experimental sobre Captive Portal, oferecendo uma reflexão sobre sua implementação, em vez de aprofundar-se em termos técnicos. A fundamentação teórica foi baseada em estudos de Redes de Computadores, com ênfase nos livros "Redes de Computadores e a Internet: Uma Abordagem Top-Down" de Kurose e Ross (6ª edição), esse livro aborda redes de maneira mais peculiar visualizando a mesma do ponto de vista metodológico vindo a partir da Camada de Aplicação descendo até a Camada Física, por isso que é uma abordagem "top-down" e "Redes de Computadores" de Tanenbaum e Wetherall (5ª edição), esse livro é conhecido por pegar redes de modo mais robusto, pois, abrange com excelência o universo da telecomunicação. Essas obras fornecem um arcabouço teórico sólido, essencial para os estudos na graduação de cursos vinculados a área de tecnologia. Durante esse período, houve oportunidade de aplicar e aperfeiçoar conhecimentos com orientação dos professores da Universidade da Amazônia.

3. CONSTRUÇÃO DA INFRAESTRUTURA

Para esse Projeto, utilizou-se um Raspberry Pi Model 3B, mas caberia qualquer modelo que tenha a firmware disponível no site OpenWRT (<https://firmware-selector.openwrt.org/>). A firmware é um tipo de software que fornece controle, monitoramento e manipulação de dados para sistemas eletrônicos embarcados. Em termos simples, é o programa que vem embutido no hardware e é essencial para que o dispositivo funcione corretamente.



Figura 1: Imagem do Raspberry Pi model 3B. Fonte: do Autor.

A escolha do Raspberry Pi foi motivada pela necessidade de aumento na segurança, pois alguns roteadores não disponibilizam o serviço de Captive Portal (conforme constatado ao longo do projeto, o roteador utilizado não disponibilizava esse recurso). O Captive Portal é uma página de autenticação que se abre antes de acessar a rede interna, geralmente usada em redes Wi-Fi públicas para gerenciar o acesso dos usuários.

Como mencionado no capítulo 1, a capacidade de administrar redes de maneira eficiente é de suma importância. Visto isso, ativa o protocolo SSH (Secure Shell), permitindo a interação remota com o dispositivo (Raspberry pi) através do Computador pessoal.

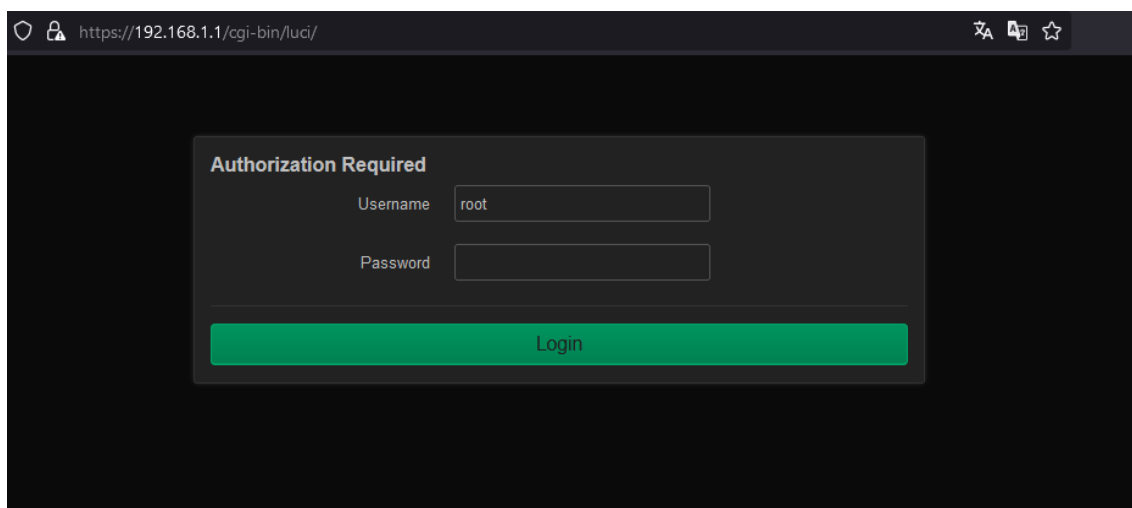


Figura 2: Imagem capturada do Sistema Operacional OpenWRT (GUI). Fonte: do Autor.

O OpenWRT possui uma apresentação gráfica de usuário (GUI), que é uma interface visual que facilita a interação com o sistema através de elementos gráficos como botões, menus e janelas. A GUI será utilizada para futuras configurações de forma intuitiva e acessível.

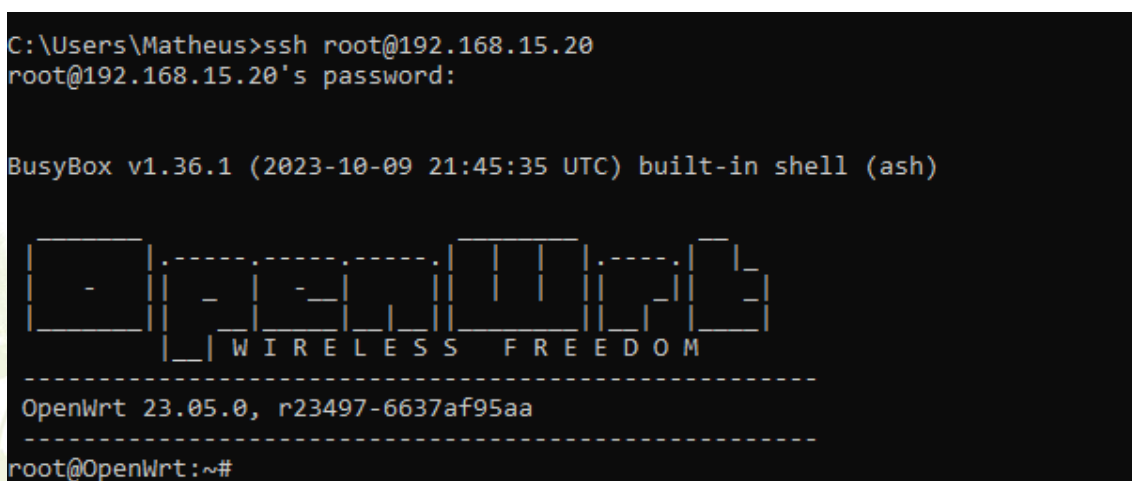


Figura 3: Imagem capturada do Sistema Operacional OpenWRT (GUI). Fonte: do Autor.

Além da GUI, também utiliza-se a interface de linha de comando (CLI), como mostrado na figura 3, que permite a interação com o sistema através de linhas de comando.

4. TORNANDO A REDE ACESSÍVEL E SEGURA PARA OS USUÁRIOS.

Neste capítulo, abordar-se a transformação do Raspberry Pi em um ponto de acesso (Access Point, AP). Para isso, faz-se necessário configurar a rede de modo que os usuários possam se conectar a ela. A administração da rede é realizada remotamente por meio de um computador pessoal, utilizando o protocolo seguro conhecido como SSH (Secure Shell). Esse método permite monitorar e gerenciar o Raspberry Pi sem a necessidade de acesso físico ao dispositivo, proporcionando maior flexibilidade e conveniência na administração da rede.

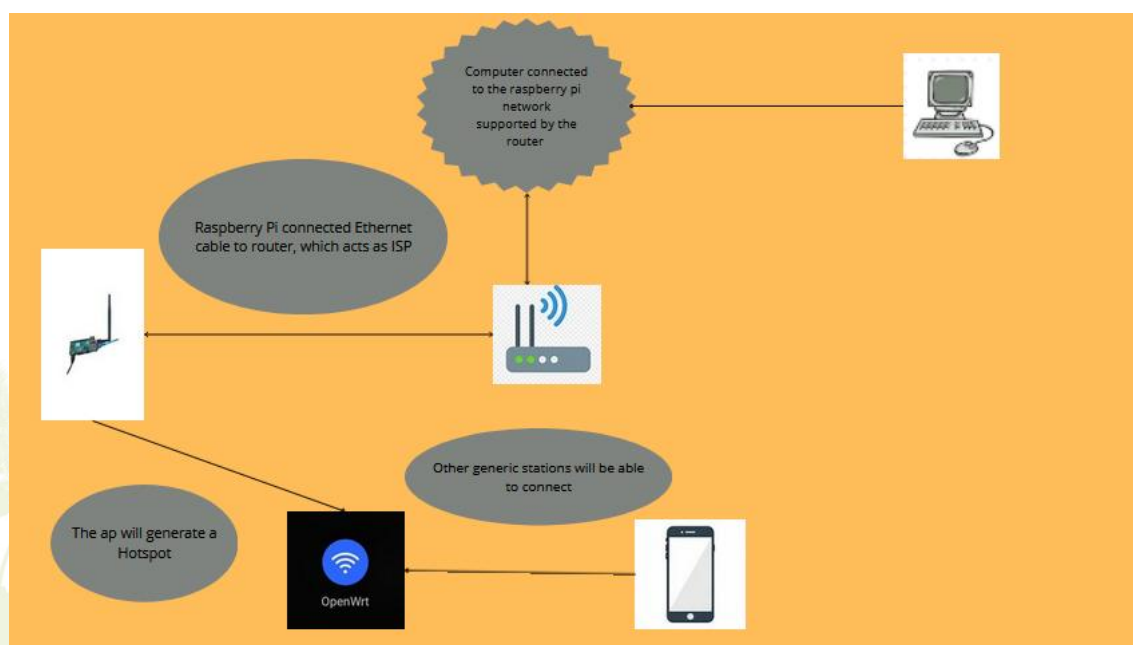


Figura 4: Modelagem da construção da infraestrutura de rede. Fonte: do autor.

Com a infraestrutura de rede estabelecida, conforme ilustrado na Figura 4, o próximo passo foi propagar a segurança pela rede, como será mostrado na figura 5.



Figura 5: Comportamento da Rede após instalar o Sistema de Segurança. Fonte: do autor.

Com a globalização e o fácil acesso à informação na área da tecnologia da informação, tornou-se muito mais fácil para usuários maliciosos utilizarem essas informações de forma prejudicial. Nossos dados estão constantemente na mira de indivíduos mal-intencionados. Embora nas áreas metropolitanas haja um suporte mais robusto, em regiões afastadas, justamente o foco deste estudo, essas práticas podem representar um grande risco. Nessas áreas, a vulnerabilidade é maior, o que pode facilitar a captura de dados por criminosos que se aproveitam dessas informações para se passar por outras pessoas, obtendo benefícios públicos indevidamente e causando prejuízos significativos para o país.

Conforme ilustrado na figura 5, os chamados firewalls (muralhas de fogo) atuam como agentes de segurança, responsáveis por definir limites para quem acessa o servidor ou a rede. O servidor, por sua vez, é responsável por armazenar informações como nome, e-mail e senha dos usuários. Além disso, são registradas informações como o tempo de cadastro, a imagem do rosto, o endereço MAC ou endereço físico, identificando de forma exclusiva cada dispositivo. Se, por exemplo, quatro pessoas se cadastraram como mostrado na figura 4, mas foi detectado um quinto dispositivo sem um nome explícito, isso ocorreu porque o administrador da rede consultou o banco de dados, que continha

quatro cadastros, e identificou um dispositivo adicional operando no roteador. Essa verificação fornece um suporte visual valioso para o profissional de TI, permitindo a identificação de atividades suspeitas na rede.

Apesar de implementar medidas de segurança em redes e sistemas, a segurança total nunca é garantida. As pessoas conectadas à rede não estão 100% seguras, e a conscientização sobre práticas seguras na web é crucial. Relaciona-se a seguir alguns pontos importantes a considerar: alertar sobre phishing (técnicas de manipulação usadas para enganar usuários e obter informações confidenciais, como senhas e dados bancários), malware (software malicioso que pode danificar sistemas, roubar informações ou permitir o controle remoto de dispositivos), engenharia social (estratégias usadas por atacantes para manipular pessoas a revelarem informações confidenciais ou realizarem ações que comprometam a segurança), boas práticas de senhas (usar senhas fortes e únicas, mudar regularmente, e evitar o uso de informações pessoais óbvias).

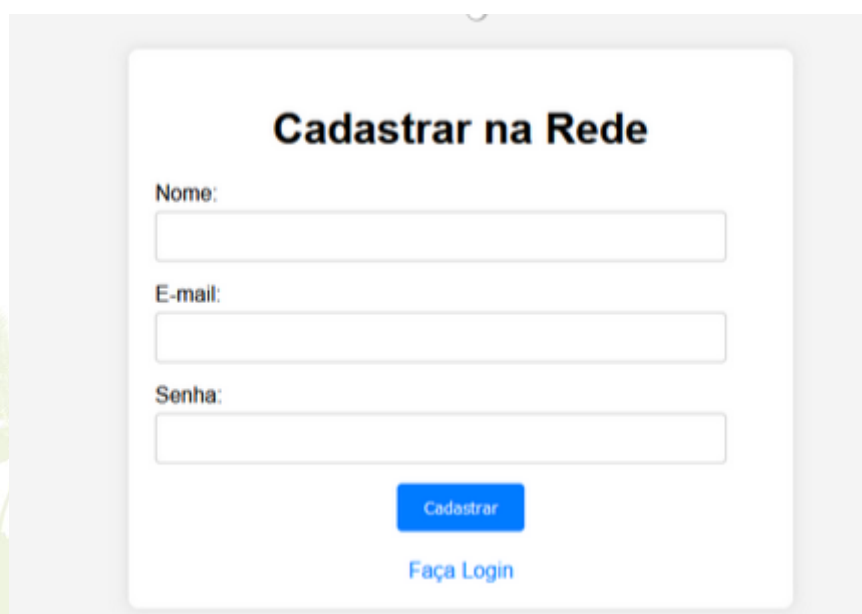


Figura 6: Tela de Cadastro. Fonte do autor.

Caso os usuários estejam visitando a rede pela primeira vez, terão a oportunidade de se cadastrar. É importante frisar que alguns captive portals adotam apenas uma tela de login, pois já possuem uma base de dados pré-estabelecida.

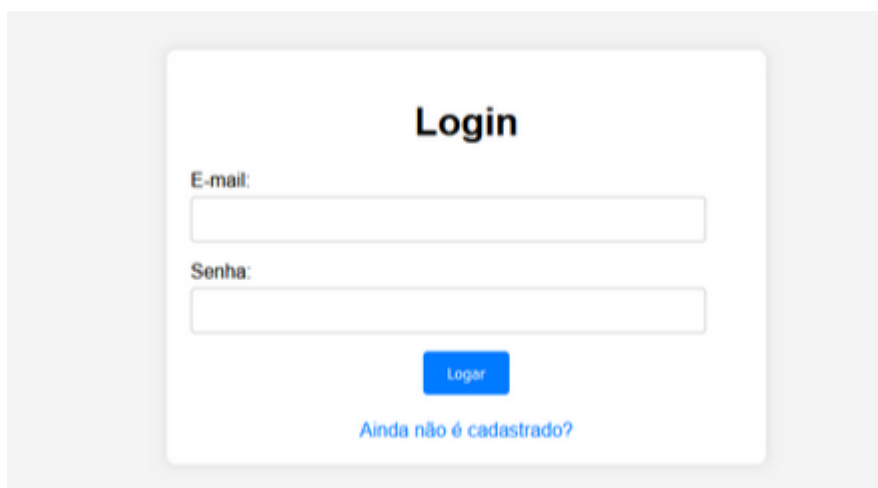
A screenshot of a web login page. At the top, the word "Login" is centered in a bold, black font. Below it, there are two input fields: the first is labeled "E-mail:" and the second is labeled "Senha:". Both fields are empty and have a light gray border. Below the password field is a blue button with the word "Login" in white text. At the bottom of the form, there is a blue link that says "Ainda não é cadastrado?". The entire form is set against a light gray background.

Figura 7: Tela de Login.Fonte do autor.

Se o usuário já estiver cadastrado na base de dados, mas acessar a rede após um longo período, as páginas web serão automaticamente atualizadas para refletir seu status. A tela de cadastro será exibida conforme mostrado na Figura 6, enquanto a tela de login será apresentada conforme ilustrado na Figura 7.

5.METODOLOGIA

Este estudo realizou uma pesquisa experimental com o objetivo de permitir que interessados na causa ribeirinha, independentemente de serem da área da computação, possam replicar o projeto e inspirar futuras pesquisas. Além disso, busca promover a geração de políticas públicas que possam efetivamente impulsionar mudanças significativas.

Para a realização da pesquisa, serão utilizados alguns equipamentos essenciais, incluindo um Raspberry Pi, um cabo de par trançado com comprimento suficiente para conectar ao roteador, e um computador que atuará tanto como servidor web quanto como servidor de banco de dados. O processo começa com a formatação de um pendrive, que será preparado para a instalação do sistema operacional OpenWRT.

Em seguida, é necessário encontrar a ISO (Imagem de Disco Óptico) do OpenWRT que seja compatível com o modelo do seu Raspberry Pi. Após obter a ISO, será necessário configurar um computador ou notebook para que você possa acessar o Raspberry Pi remotamente via SSH.

Uma vez que o acesso remoto ao Raspberry Pi esteja estabelecido, o próximo passo é transformá-lo em um ponto de acesso (Access Point). Com isso, o Raspberry Pi poderá propagar as páginas de autenticação pela rede, permitindo o gerenciamento e controle dos usuários conectados.

Dessa forma, o ambiente estará preparado para conduzir a pesquisa de maneira eficiente e segura.

6.RESULTADOS E DISCUSSÕES

Os resultados obtidos durante a pesquisa destacam a importância crucial de configurar a rede diretamente no ambiente onde será utilizada. A configuração em um ambiente externo, em uma LAN diferente daquela onde será implementada, revelou-se problemática e não é aconselhável.

7.CONSIDERAÇÕES FINAIS

Ao longo da pesquisa, alcançou-se resultados significativos que merecem destaque. Um dos principais resultados foi o custo-benefício de ter usado um Raspberry Pi para proporcionar esse serviço na rede. A utilização do Raspberry Pi trouxe diversas vantagens, incluindo a redução de burocracias, pois o OpenWrt oferece suporte de otimização para roteadores. Embora fosse possível implementar o sistema diretamente no roteador, optamos pelo Raspberry Pi para evitar a complexidade de configurar equipamentos que já estavam pré-configurados na rede, como televisões, impressoras e estações domésticas (celulares e computadores). Isso evitou uma exaustão de tempo considerável.

8.REFERÊNCIAS

FIGUEIREDO, Davis Anderson et al. Vulnerabilidades em redes Wi-Fi de instituições de ensino superior: um estudo de múltiplos casos. *Research, Society and Development*, v. 9, n. 2, p. e178921979-e178921979, 2020.

MACHADO, Rodrigo; RODRIGUES, Jovenildo; FERNANDES, Rui. URBANIZAÇÃO, MORADIA E DESIGUALDADE SOCIOESPACIAL: UMA ANÁLISE A PARTIR DA CIDADE DE PARAUAPEBAS, PARÁ. *REVISTA GEONORTE*, v. 15, n. 50, 2024.

DE AGRIMENSURA, ENGENHARIA CARTOGRÁFICA E.; DIAS, PATRICK LOBATO. Análise multitemporal por imagem de satélite da expansão urbana da sede municipal de Abaetetuba-PA.

GOMES, Vitor Hugo M. et al. Modelo Georreferenciado de Disponibilidade de Internet para Educação Superior Online: Estudo de Caso no Estado do Pará. In: *Anais do XLVIII Seminário Integrado de Software e Hardware*. SBC, 2021. p. 144-154.

TANENBAUM, Andrew S. *Redes de Computadores* (2003). Tradução da Quarta Edição, Editora Campus.

COMER, Douglas E. *Redes de computadores e internet-6*. Bookman Editora, 2016.

SPLASH NETWORKS. OpenWRT Coova Chilli External Captive Portal. YouTube, 25 mar.2023. Disponível em: <https://www.youtube.com/watch?v=jG6ud1oy1hI&t=215s>.

OpenWrt. Basic WiFi. OpenWrt, [s.d.]. Disponível em: <https://openwrt.org/docs/guide-user/network/wifi/basic>. Acesso em: 19 jun. 2024.