CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA - CEFET/RJ

CURSO DE SISTEMAS DE INFORMAÇÃO

CONTROLE E MONITORAMENTO DE ACESSO À INTERNET EM AMBIENTES DOMÉSTICOS

LUÍS FERNANDO BARROS PITTA

Orientador: Prof. Me. Nilson Mori Lazarin

CEFET/RJ Campus Nova Friburgo

NOVA FRIBURGO

2025

LUÍS FERNANDO BARROS PITTA

CONTROLE E MONITORAMENTO DE ACESSO À INTERNET EM AMBIENTES DOMÉSTICOS

Trabalho de Conclusão de Curso (Graduação) apresentado ao Curso de Sistemas de Informação do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, como requisito parcial para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Me. Nilson Mori Lazarin
CEFET/RJ Campus Nova Friburgo

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA - CEFET/RJ
CURSO DE SISTEMAS DE INFORMAÇÃO
NOVA FRIBURGO
2025

CONTROLE E MONITORAMENTO DE ACESSO À INTERNET EM AMBIENTES DOMÉSTICOS

Monografia apresentada ao Curso de Sistemas de Informação do Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, como requisito parcial para a obtenção do título de Bacharel.

LUÍS FERNANDO BARROS PITTA

Banca Examinadora:

gov.br Documento assinado digitalmente
NILSON MORI LAZARIN
Data: 12/12/2025 16:42:38-0300
Verifique em https://validar.iti.gov.br

Presidente, Prof. Me. NILSON MORI LAZARIN (CEFET/RJ) (Orientador(a))

gov.br Documento assinado digitalmente
HELGA DOLORICO BALBI
Data: 12/12/2025 16:58:42-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. HELGA DOLORICO BALBI (CEFET/RJ)

gov.br Documento assinado digitalmente
BRUNO FERNANDES GUEDES
Data: 12/12/2025 16:48:14-0300
Verifique em https://validar.iti.gov.br

Prof. Me. BRUNO FERNANDES GUEDES (CEFET/RJ)

NOVA FRIBURGO

DEZEMBRO 2025

CEFET/RJ – Sistema de Bibliotecas / Biblioteca Uned Nova Friburgo

P688c Pitta, Luis Fernando Barros.
Controle e monitoramento de acesso à internet em ambientes domésticos / Luis Fernando Barros Pitta. – , RJ: 2025.
xi, 36f.: il. (color.) : em PDF.

Trabalho de Conclusão de Curso (Sistemas de Informação) - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, 2025.
Bibliografia: f. 35-36.
Orientador: Nilson Mori Lazarin.

1. Sistemas de Informação. 2. Internet – medidas de segurança. 3. Microcomputadores – controle de acesso. I. Lazarin, Nilson Mori. (Orientador). II. Título.

CDD 658.4038

Elaborada pela bibliotecária Cristina Rodrigues Alves CRB7/5932

Agradecimentos

Gostaria de registrar meus sinceros agradecimentos a todas as pessoas e instituições que, de alguma forma, contribuíram para a realização desta pesquisa e para a elaboração desta monografia.

Em primeiro lugar, agradeço ao orientador, professor Nilson Mori Lazarin, pela orientação dedicada, pelos conselhos valiosos e pelo constante incentivo ao longo de todo o processo. Suas contribuições foram essenciais para o desenvolvimento e aprimoramento deste trabalho. Estendo também minha gratidão ao CEFET-RJ, pelo suporte acadêmico prestado e pelos recursos disponibilizados durante a trajetória acadêmica.

Aos familiares e amigos, pelo apoio incondicional, compreensão e incentivo em todos os momentos desta jornada, manifesto meu profundo reconhecimento.

Por fim, agradeço a todos aqueles que, direta ou indiretamente, colaboraram para a concretização deste estudo, mesmo que não tenham sido mencionados nominalmente. Cada contribuição, interação e experiência vivenciada foi fundamental para a conclusão desta etapa.

Resumo

O acesso irrestrito à internet por crianças e adolescentes pode expô-los a conteúdos potencialmente prejudiciais, como pornografia, apologia à violência e desafios perigosos. Este trabalho apresenta o desenvolvimento de um sistema integrado de controle e monitoramento de rede para ambientes domésticos, com o objetivo de oferecer uma infraestrutura segura e supervisionada de acesso à internet. A solução é composta por múltiplas camadas de proteção, incluindo bloqueio de domínios via *DNS*, restrição de serviços específicos, identificação de palavras-chave sensíveis em *URLs*, ativação forçada do modo restrito do Google e YouTube (*SafeSearch*) e aplicação de regras de *firewall* com *iptables* para restringir acessos e obrigar o uso de *proxy*. Os dados de navegação são coletados e apresentados em um painel administrativo acessível, permitindo a configuração personalizada das políticas de bloqueio. O sistema visa promover a segurança digital de forma proativa, combinando tecnologias de rede com uma interface de fácil uso por responsáveis legais. Como parte da validação, uma pesquisa exploratória com oito responsáveis apontou intenção de uso da solução proposta e percepção de que ela facilita o processo de controle de acessos.

Palavras-chave: Controle de acesso, Políticas de Prevenção, Monitoramento de rede

Abstract

Unrestricted internet access by children and adolescents can expose them to potentially harmful content, such as pornography, advocacy of violence, and dangerous challenges. This work presents the development of an integrated network control and monitoring system for home environments, aiming to provide a safe and supervised internet access infrastructure. The solution is composed of multiple layers of protection, including domain blocking via DNS, restriction of specific services, detection of sensitive keywords in URLs, forced activation of Google and YouTube restricted mode (SafeSearch), and the application of firewall rules with iptables to restrict access and enforce the use of a proxy. Browsing data are collected and presented in an accessible administrative panel, allowing personalized configuration of blocking policies. The system aims to promote digital safety proactively, combining network technologies with an interface designed for ease of use by legal guardians. As part of the validation process, an exploratory survey with eight guardians indicated an intention to use the proposed solution and a perception that it facilitates the process of access control.

Keywords: Access Control, Prevention Policies, Network Monitoring

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

DNS	*Domain Name System* (Sistema de Nomes de Domínio)
TAM	*Technology Acceptance Model* (Modelo de Aceitação de Tecnologia)
ACL	*Access Control List* (Lista de Controle de Acesso)
IP	*Internet Protocol* (Protocolo de Internet)
URL	*Uniform Resource Locator* (Localizador Uniforme de Recursos)
HTTP	*Hypertext Transfer Protocol* (Protocolo de Transferência de Hipertexto)
HTTPS	*Hypertext Transfer Protocol Secure* (Protocolo de Transferência de Hipertexto Seguro)
RAM	*Random Access Memory* (Memória de Acesso Aleatório)
DHCP	*Dynamic Host Configuration Protocol* (Protocolo de Configuração Dinâmica de Hosts)
MAC	*Media Access Control* (Controle de Acesso ao Meio)

Sumário

1 Introdução

O acesso à internet tem apresentado crescimento contínuo ao longo dos anos, abrangendo também crianças e adolescentes. Conforme pesquisa da *TIC KIDS ONLINE KIDS BRASIL* (CETIC, 2022), nove em cada dez crianças utilizam a internet. A presença assídua em redes sociais, salas de bate-papo, comunidades virtuais e novos serviços digitais torna *"muito difícil impedir o contato de menores com outras pessoas na internet"* (BARROS; SILVA, 2019), o que os torna suscetíveis a diferentes tipos de riscos *online*.

A adoção de ferramentas de monitoramento digital configura-se como uma medida relevante para que pais e responsáveis possam exercer, de forma efetiva, sua responsabilidade legal no acompanhamento das atividades virtuais dos filhos. Tal responsabilidade está prevista no artigo 1.634 do Código Civil brasileiro, o qual atribui aos pais o dever e não apenas o direito de educar os filhos, sendo essa obrigação extensível ao ambiente virtual (PERES, 2016).

Para Flávio Tartuce (TARTUCE, 2017), os *"modernos aparatos da virtualidade, seus instrumentos e redes, tornam aqueles ainda mais vulneráveis; vítimas"*. O uso da internet sem a devida supervisão expõe o público infantil a conteúdos impróprios, como violência, pornografia, assédio, desafios de suicídio e *cyberbullying*. Diante disso, é imprescindível que medidas preventivas e ferramentas adequadas sejam adotadas para mitigar tais riscos.

Neste contexto, este trabalho propõe desenvolver uma solução para controle e monitoramento de rede voltado para ambientes domésticos, com o objetivo de oferecer uma solução tecnológica capaz de bloquear domínios, restringir serviços, identificar acessos a conteúdos sensíveis e exibir essas informações de forma simplificada em um painel de controle. A proposta busca contribuir com a segurança digital de crianças e adolescentes, aliando recursos de rede, como bloqueios por *firewall*, uso de *proxy*, redirecionamento *DNS* e ativação do *SafeSearch*, à supervisão responsável do uso da internet.

1.1 Definição do Problema

A ausência de mecanismos eficazes de monitoramento do acesso de crianças e adolescentes à internet configura um problema de grande relevância social. Conforme o relatório *Norton Cyber Safety Insights Report* (NORTON, 2022), mais de 40% dos responsáveis não monitoram o acesso dos filhos à internet, o que contribui para a exposição desse público a conteúdos potencialmente nocivos, como violência, pornografia e material de caráter criminoso.

Motores de busca amplamente utilizados, como o Google, embora ofereçam meca-

nismos de segurança, não os tornam suficientemente robustos para o público infantojuvenil, uma vez que esses filtros podem ser facilmente desativados com poucos cliques, inclusive pela própria criança. Essa fragilidade evidencia a necessidade de instrumentos de supervisão mais eficazes, que concedam aos responsáveis maior controle sobre os conteúdos acessados e contribuam para a criação de um ambiente digital verdadeiramente seguro e apropriado à faixa etária.

Um caso emblemático foi mostrado pelo *Fantástico* (FANTASTICO, 2023), quando um grupo de indivíduos utilizou o *Discord* para cometer crimes como ameaças, incentivo à automutilação, maus-tratos a animais, pornografia infantil e estupros. As vítimas, preferencialmente adolescentes do sexo feminino, eram convencidas a produzir e compartilhar material íntimo, que posteriormente era usado para chantageá-las e coagi-las a participar de desafios perigosos, incluindo automutilação e encontros presenciais que resultaram em abusos. Este caso ganhou destaque ao ser exibido em rede nacional, onde se evidenciou a gravidade e a complexidade dos riscos associados ao ambiente *online*.

Outros casos semelhantes surgem com frequência, como as mortes de duas meninas que participaram do “Desafio do Desodorante”. No início de março de 2025, uma menina de 11 anos faleceu em Bom Jardim (PE) após inalar *spray* de desodorante, seguindo um vídeo compartilhado nas redes sociais (Veja, 2025). Pouco depois, no Distrito Federal, outra menina, de apenas 8 anos, morreu em Ceilândia após repetir o mesmo desafio, que resultou em parada cardiorrespiratória e posterior diagnóstico de morte cerebral (**??**).

A juíza da Vara da Infância e Juventude do Rio de Janeiro, Vanessa Cavalieri, alertou que crianças e adolescentes estão sendo expostos à pornografia antes mesmo de iniciarem sua vida sexual (Câmara dos Deputados, 2024). Segundo ela, plataformas como *Discord*, *Twitter*, *Instagram* e *Telegram* abrigam comunidades que promovem a exploração sexual infantil, muitas vezes sem qualquer tipo de moderação. Esse cenário reforça a necessidade de ferramentas que permitam aos responsáveis restringir o acesso a esses ambientes e proteger os menores no ambiente *online*.

Diante desse cenário, observa-se a necessidade de ferramentas eficazes de monitoramento e controle parental que permitam aos responsáveis supervisionar e restringir o acesso dos menores a conteúdos e interações potencialmente perigosos na internet, visando à proteção e ao bem-estar das crianças e adolescentes no ambiente digital. Nesse contexto, soluções baseadas em mecanismos de filtragem, supervisão ativa e controle do tráfego de rede surgem como alternativas promissoras para fortalecer a segurança no ambiente doméstico.

1.2 Contribuição

O presente trabalho propõe o desenvolvimento de uma solução integrada para redes domésticas, com foco no monitoramento do tráfego de dados, no bloqueio de conteúdos sensíveis e na supervisão do uso da internet por parte de usuários em idade infantojuvenil. A proposta baseia-se em uma arquitetura composta por múltiplas camadas de controle, incluindo o uso de *proxy* para controle de tráfego *web*, redirecionamento forçado de *DNS* para um servidor local com resoluções filtradas, ativação do modo restrito em mecanismos de busca, e aplicação de políticas de bloqueio de palavras-chave e serviços específicos (como plataformas de mensagens ou redes sociais) via *firewall*. Nesse modelo, o acesso à internet é permitido exclusivamente aos dispositivos que estiverem corretamente configurados para utilizar o *proxy*, garantindo que todo o tráfego passe pelos filtros e registros definidos no sistema.

A partir dos registros gerados pelo *proxy*, o sistema realiza a análise automática dos dados de navegação, identificando tentativas de acesso a termos previamente classificados como sensíveis. Essas ocorrências podem ser consultadas pelos responsáveis por meio de uma interface gráfica intuitiva. Esse painel administrativo também permite visualizar os acessos realizados, aplicar novas regras de bloqueio e acompanhar métricas de uso em tempo real.

Para avaliar a efetividade do sistema proposto, foi realizada a demonstração de um protótipo funcional executado em uma *Raspberry Pi*, configurado como núcleo da rede doméstica. O sistema foi apresentado para os responsáveis com todos os seus recursos ativos. Durante os testes, os participantes puderam navegar sob supervisão e observar, na prática, o funcionamento das camadas de proteção implementadas. Adicionalmente, foi aplicada uma pesquisa baseada no modelo *Technology Acceptance Model (TAM)*, com o objetivo de avaliar a aceitação, utilidade percebida e facilidade de uso do protótipo por parte dos participantes. Essa abordagem permitiu obter dados qualitativos e quantitativos sobre a experiência de uso, contribuindo para a análise do potencial do sistema enquanto ferramenta de apoio ao controle parental e à segurança digital no ambiente doméstico.

Os resultados da pesquisa indicaram alta aceitação da proposta. A maioria dos participantes relatou facilidade no aprendizado e clareza da interface, além de perceber utilidade prática na adoção da solução no ambiente doméstico. A intenção de uso também foi destacada, visto que todos os respondentes afirmaram que utilizariam a ferramenta para configurar uma rede mais segura e a recomendariam a outros responsáveis. Esses achados reforçam a contribuição do trabalho, demonstrando que, além da viabilidade técnica, o sistema atende a requisitos de usabilidade e valor percebido, fundamentais para sua adoção em ambientes reais.

1.3 Organização do Trabalho

Este trabalho está estruturado da seguinte maneira: no Capítulo 2, apresenta-se o referencial teórico. No Capítulo 3, discutem-se os trabalhos relacionados. O Capítulo 4 descreve as etapas de desenvolvimento do sistema proposto, bem como os métodos utilizados para sua implementação e avaliação. No Capítulo 5, é apresentada a prova de conceito. No Capítulo 6, são exibidos os resultados da pesquisa. Por fim, no Capítulo 7, apresentam-se as conclusões do estudo e ideias para trabalhos futuros.

2 Fundamentação Teórica

Com o objetivo de contextualizar os componentes tecnológicos que sustentam a solução desenvolvida, é apresentado neste capítulo os principais conceitos teóricos relacionados à infraestrutura de rede, segurança e controle de acesso utilizados no projeto. São abordados, de forma estruturada, os fundamentos sobre roteadores, resolução de nomes via *DNS*, funcionamento do *proxy* com foco no *Squid*, mecanismos de filtragem via *firewall* com *iptables*, a aplicação obrigatória do recurso *SafeSearch*, além das bases do controle parental e das características do dispositivo *Raspberry Pi*, que serve como plataforma de execução do sistema.

2.1 Roteador

De acordo com (FOROUZAN; MOSHARRAF, 2013), *"um roteador é um dispositivo de interconexão"*, ou seja, tem a função básica de receber e direcionar pacotes de dados dentro de uma rede ou para outras redes. Sua principal função consiste em analisar os pacotes de dados recebidos e encaminhá-los de forma eficiente ao seu destino, utilizando algoritmos de roteamento para determinar a melhor rota disponível.

Em redes domésticas, os roteadores acumulam geralmente as funções de distribuição do sinal de internet, *firewall* básico e ponto de acesso sem fio. Modelos mais avançados oferecem recursos adicionais de segurança e gerenciamento, como controle de largura de banda, filtragem de pacotes, bloqueio de portas e suporte à integração com servidores *proxy*, facilitando a implementação de políticas de acesso e restrição de conteúdo.

2.2 Domain Name System — DNS

O *DNS* é um sistema responsável por traduzir nomes de domínios amigáveis (como *www.google.com*) em endereços *IP* compreensíveis pelos dispositivos de rede (CloudFlare, s.d.). Esse processo é essencial para a navegação na internet, pois permite que os usuários acessem serviços *online* sem a necessidade de memorizar números de *IP*.

No contexto do presente trabalho, o *DNS* também atua como camada de controle. Ao forçar o uso de um servidor *DNS* local, torna-se possível aplicar filtros que impedem a resolução de nomes associados a sites ou serviços indesejados, bloqueando o acesso antes mesmo que a requisição chegue ao servidor de destino. Essa abordagem complementa as funções do *proxy* e adiciona um nível de segurança e supervisão ainda na etapa inicial da comunicação.

2.2.1 OpenDNS FamilyShield

Como complemento de *DNS*, optou-se pelo uso do *OpenDNS FamilyShield*[1], um serviço gratuito oferecido pela Cisco. Ele disponibiliza servidores *DNS* pré-configurados com filtros automáticos para bloquear conteúdos considerados inadequados, como sites de pornografia e violência explícita, sem necessidade de cadastro ou configuração adicional. Essa escolha garante uma camada inicial de proteção já no momento da resolução de nomes de domínio, fortalecendo o controle parental proposto e complementando os mecanismos de filtragem implementados localmente.

2.3 Proxy

Conforme definido por (RICCI; MENDONçA, 2006), *o proxy refere-se a um software que atua como gateway de aplicação entre o cliente e o serviço a ser acessado, interpretando as requisições e repassando-as ao servidor de destino*. Em vez de serem encaminhadas diretamente ao servidor final, as solicitações são direcionadas ao *proxy*, que avalia seu conteúdo e, com base em configurações específicas, decide sobre seu encaminhamento. A resposta do servidor também passa pelo *proxy*, retornando ao cliente após filtragem.

Essa abordagem adiciona uma camada de controle e segurança, sendo particularmente útil em ambientes nos quais se deseja restringir ou monitorar o tráfego de rede. Vale destacar que, normalmente, o *proxy* filtra domínios e padrões de *URL*, e não o conteúdo completo das páginas. Por meio de listas de controle, é possível bloquear sites, palavras-chave e protocolos, oferecendo maior granularidade no controle de acesso.

2.3.1 Squid

O *Squid*[2] é um *software* livre que atua como *proxy* do tipo *forward*, amplamente utilizado para controle e otimização do tráfego *web*. Ele funciona como intermediário entre os dispositivos da rede e os servidores da internet, permitindo o *cache* de conteúdo frequentemente acessado e a aplicação de regras de acesso baseadas em listas de controle (*ACLs*).

Essas listas possibilitam a filtragem de acesso com base em critérios como endereços *IP*, horários, domínios, protocolos e palavras-chave. No presente trabalho, o uso do Squid foca exclusivamente nas funcionalidades de *proxy* e registro de atividades por meio de arquivos de *log*. Essas informações são analisadas e apresentadas em uma interface própria de visualização, construída especificamente para o sistema proposto.

[1] <https://www.opendns.com/home-internet-security/>
[2] <http://www.squid-cache.org/>

2.4 Firewall

O *firewall* é um componente essencial em arquitetura de segurança de redes, responsável por controlar o tráfego de dados entre diferentes interfaces com base em regras definidas previamente. De acordo com (NAKAMURA; GEUS, 2007), *"Pode ser definido como um sistema ou um grupo de sistemas que reforça a política de controle de acesso entre duas redes."* Em ambientes domésticos ou educacionais, sua utilização permite restringir conexões indesejadas, proteger dispositivos vulneráveis e garantir que o tráfego siga os caminhos previamente autorizados.

2.4.1 Iptables

O *iptables*[3] é uma ferramenta de linha de comando utilizada para configurar regras de filtragem de pacotes no *firewall* do sistema operacional *Linux*. Por meio da definição de políticas de entrada, saída e encaminhamento de tráfego, o *iptables* permite bloquear conexões, redirecionar requisições e aplicar diferentes níveis de controle de acesso a redes locais e externas.

No contexto deste trabalho, o *iptables* desempenha um papel estratégico ao impedir o uso de servidores *DNS* externos, forçando os dispositivos conectados à rede a utilizarem exclusivamente o servidor *DNS* local, previamente configurado com filtros de conteúdo. Além disso, ele é responsável por garantir que apenas os dispositivos configurados com o *proxy* manual tenham acesso à internet, funcionando como uma barreira de controle que impede acessos não supervisionados. Com isso, o *iptables* atua como uma camada essencial na estrutura de segurança e supervisão da rede doméstica proposta.

2.5 SafeSearch

O *SafeSearch* é um recurso oferecido por mecanismos de busca, como o *Google*, que filtra resultados considerados inapropriados, como conteúdos explícitos, violentos ou ofensivos. Embora configurável manualmente nos navegadores, esse filtro pode ser forçado por administradores de rede por meio de parâmetros de *URL* ou redirecionamentos *DNS*, garantindo que todas as buscas realizadas na rede sejam submetidas à filtragem.

No sistema desenvolvido neste trabalho, o uso do *SafeSearch* é aplicado de forma obrigatória, complementando o controle exercido pelo *proxy* e pelo *DNS* local. Essa medida visa reduzir o risco de exposição a conteúdos impróprios diretamente na etapa de consulta aos buscadores, fortalecendo a estratégia de proteção digital em ambientes domésticos.

[3] <https://www.netfilter.org/projects/iptables/>

2.6 Controle Parental

Segundo (BARROS; SILVA, 2019), *"a ideia do controle parental é ser uma ferramenta de auxílio aos pais e responsáveis na tarefa de evitar os riscos que os menores estão expostos na internet."* Diversos *softwares* foram desenvolvidos com o propósito de viabilizar esse tipo de controle, destacando-se o uso de *proxy* e de servidores *DNS* como métodos de filtragem de conteúdo, considerados entre as abordagens mais eficazes nesse contexto.

Quando configurado com finalidades de controle parental, o sistema permite filtrar e bloquear conteúdos considerados inadequados, como material pornográfico, violento ou que promova condutas prejudiciais. Dessa forma, busca-se promover um ambiente de navegação mais seguro, protegendo o público infantojuvenil contra ameaças digitais.

2.7 Raspberry Pi

O *Raspberry Pi*[4] é um exemplo de *Single-Board Computer*, ou computador de placa única. É um tipo de dispositivo que integra em uma única placa todos os componentes essenciais de um computador — como processador, memória, interfaces de entrada e saída, e conectividade de rede — diferindo dos computadores tradicionais, que distribuem esses elementos em múltiplos módulos e placas. *Raspberry Pi* se destaca pelo tamanho reduzido, baixo custo e consumo energético eficiente, características que possibilitam sua aplicação em educação, automação residencial, Internet das Coisas e prototipagem de soluções tecnológicas.

[4] <https://www.raspberrypi.com/>

3 Trabalhos Relacionados

A fim de embasar teoricamente a proposta desenvolvida, foi realizada uma busca sistemática por estudos científicos relevantes utilizando a plataforma *Google Scholar*. A estratégia de pesquisa foi construída com base na combinação de termos relacionados ao controle parental, segurança na internet e ferramentas de rede, por meio da seguinte string de busca:

```
("parental control" OR "internet content filtering")
AND ("safe internet use" OR "internet safety for children")
AND (network OR proxy OR squid OR dns)
```

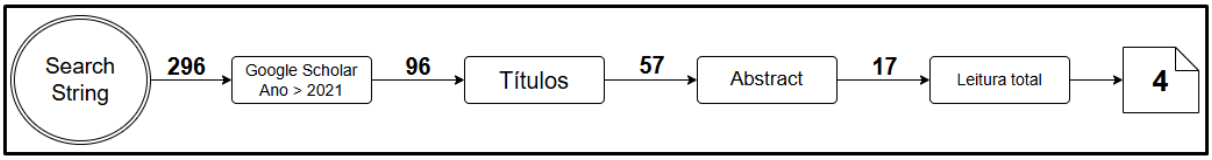

Figura 1 – Fluxograma da pesquisa cientifica.

Inicialmente, foram identificados 296 resultados. Em seguida, aplicou-se um filtro temporal, restringindo a busca a publicações a partir do ano de 2021, o que resultou em 96 trabalhos. Posteriormente, foram selecionados somente os títulos que continham termos diretamente relacionados à temática central, como *"children"*, *"child"*, *"parent"*, *"parental control"* e *"parenting"*, reduzindo a amostra para 57 artigos. A leitura dos resumos permitiu a identificação de 17 estudos com potencial relevância para o escopo deste trabalho. Por fim, após a leitura integral dos textos, 4 estudos foram selecionados por apresentarem contribuições significativas, em especial aqueles que destacam a preferência dos responsáveis por soluções técnicas automatizadas. Esse processo está sintetizado no fluxograma da Figura 1.

3.1 Abordagens na Literatura

Diversos estudos vêm explorando as estratégias utilizadas por pais e responsáveis para mediar o uso da internet por crianças e adolescentes. Nesta seção, são apresentadas e discutidas contribuições relevantes da literatura recente, selecionadas a partir do processo descrito na seção anterior.

3.1.1 Preferência dos Pais por Soluções Técnicas na Mediação Digital

O trabalho de (YAMAN; KARADEMIR; YAMAN, 2023) investigou as estratégias de mediação digital adotadas por pais de crianças em idade pré-escolar, identificando uma tendência significativa à adoção de intervenções diretas e soluções técnicas para lidar com os riscos associados ao uso da internet. O estudo, de caráter misto, apontou que, embora fatores como o papel parental (mãe ou pai) e o nível educacional influenciem as estratégias adotadas, o uso de ferramentas técnicas — como filtros, bloqueadores e restrições automatizadas — foi fortemente preferido em relação a formas de mediação baseadas exclusivamente no acompanhamento ou diálogo. Essa preferência está relacionada às preocupações com os impactos socioemocionais e físicos da exposição digital precoce. Os achados reforçam a importância do desenvolvimento de sistemas automatizados de controle parental, como o proposto neste trabalho, que integra filtros *DNS*, *proxy* com bloqueio de conteúdo e mecanismos de *SafeSearch*, voltados especialmente ao público infantil.

3.1.2 Percepções Parentais sobre Benefícios e Riscos do Uso da Internet por Adolescentes

Já (KIMBALL *et al.*, 2023) analisou as percepções de 1005 pais sobre os impactos do uso da internet em filhos adolescentes (9 a 15 anos), com foco em aspectos como bem-estar, segurança, conexão familiar e uso problemático. Os resultados revelaram que, embora uma parcela expressiva dos pais tenha relatado preocupações com a exposição a conteúdos nocivos (64,3%) e *cyberbullying* (53,0%), muitos também reconheceram benefícios no uso da internet, como o fortalecimento dos vínculos familiares imediatos (46,6%) e com parentes distantes (56,5%).

O estudo também identificou uma correlação significativa entre o uso problemático da internet em adolescentes e os próprios comportamentos digitais dos pais, além de práticas parentais inconsistentes. Esses achados ressaltam a importância de envolver não somente os filhos, mas também os responsáveis no desenvolvimento de estratégias de controle parental, uma vez que os padrões familiares influenciam diretamente o comportamento online dos jovens. Nesse contexto, a solução proposta neste trabalho — que integra ferramentas automatizadas de filtragem de conteúdo, controle por palavras-chave, redirecionamento seguro de buscas e registros de navegação — busca justamente oferecer aos pais recursos acessíveis e eficazes para exercer essa mediação digital de forma mais consistente e estruturada, contribuindo para a redução de riscos associados à exposição indevida, ao mesmo tempo em que preserva os benefícios de uma internet bem utilizada no ambiente familiar.

3.1.3 Mecanismos de Busca Segura e o Papel da Filtragem de Conteúdo

Por sua vez, (BOUSNANE, 2022) destaca a importância da utilização de mecanismos de busca segura (*safe search engines*) como estratégia fundamental para proteger crianças contra conteúdos digitais nocivos como *(pornography, violence, extremism, and drugs)*, sendo essencial garantir que crianças e adolescentes desenvolvam habilidades e consciência de riscos. O estudo identifica mecanismos de busca com filtros ativados como ferramentas eficazes de proteção, e ressalta ainda o papel complementar de pais e escolas no suporte à segurança digital infanto-juvenil.

Essa abordagem dialoga diretamente com a proposta do presente trabalho, que também incorpora a filtragem segura em buscadores por meio do mecanismo *SafeSearch*, aplicado a domínios como Google e YouTube via redirecionamento de *DNS*. No entanto, a solução desenvolvida vai além: além de aplicar o *SafeSearch*, ele integra bloqueios personalizados por *DNS* e *proxy*, controle de palavras-chave, restrição por categorias e geração automatizada de listas de bloqueio. Ao unificar diferentes estratégias técnicas em uma única plataforma de controle parental, o projeto amplia a efetividade das ferramentas citadas por (BOUSNANE, 2022), oferecendo uma solução mais robusta, flexível e adaptável às necessidades das famílias no contexto da segurança *online*.

3.1.4 Importância do Uso de Ferramentas de Controle Parental

Por fim, (ARTA *et al.*, 2021) discute a baixa adoção de filtros e ferramentas de controle parental por parte dos responsáveis, com base em dados do *UK Internet Safer Centre*, que apontam que apenas metade dos pais de crianças entre 9 e 16 anos utilizam algum tipo de filtragem em computadores domésticos. O trabalho destaca a importância da utilização de *software* de controle parental para garantir a segurança das crianças na internet e detalha três funções centrais dessas ferramentas: filtragem de conteúdo (via listas de bloqueio ou permissão), monitoramento de atividades e definição de horários de uso (*scheduling*). Essa abordagem reforça a necessidade de soluções que vão além da supervisão passiva, oferecendo intervenções técnicas automatizadas alinhadas à proposta deste trabalho, que integra mecanismos como restrições baseadas em palavras-chave, filtragem *DNS* e controle por *proxy*. Embora o presente trabalho não implemente funcionalidades de agendamento de acesso, ele amplia o escopo de proteção ao incorporar níveis adicionais de bloqueio, como o controle de serviços específicos por meio de regras no `iptables`, oferecendo uma abordagem mais robusta de contenção e segurança digital para o público infantojuvenil.

A proposta apresentada por (ARTA *et al.*, 2021) baseia-se em soluções voltadas ao ambiente doméstico, com ênfase no uso de *softwares* de controle parental nativos de sistemas operacionais, como o Windows 10. Embora eficazes para controle local e com interface acessível aos pais, essas soluções tendem a operar de forma isolada em dispositivos específicos e dependem da correta configuração por parte do usuário final. Em contraste, a

implementação proposta neste trabalho adota uma abordagem centralizada baseada em rede, por meio do uso de ferramentas como `dnsmasq`, `Squid`, `iptables` e mecanismos de *SafeSearch*, permitindo o controle e monitoramento de múltiplos dispositivos conectados à mesma rede. Essa arquitetura não somente viabiliza uma gestão unificada e automatizada, como também possibilita a aplicação de bloqueios gerais por aplicativos(e.g., WhatsApp, Discord, Tik Tok) por meio de regras de *firewall*, algo não contemplado diretamente nas soluções baseadas apenas em *software* de sistema operacional.

3.2 Ferramentas Similares

Diversas ferramentas têm sido desenvolvidas com o objetivo de oferecer controle parental sobre o uso da internet. Nesta seção, são apresentadas soluções tecnológicas existentes que compartilham funcionalidades ou objetivos semelhantes à proposta deste trabalho, destacando seus principais recursos, limitações e abordagens adotadas para filtragem e monitoramento de conteúdo. A Tabela 1 apresenta um comparativo entre as principais ferramentas analisadas (Pi-hole, AdGuard Home, Qustodio) e a solução desenvolvida neste trabalho.

3.2.1 PI-hole

Além da análise dos trabalhos acadêmicos, também foi realizada uma comparação entre a solução desenvolvida e uma ferramenta consolidada no contexto do controle de conteúdo em redes domésticas: o *Pi-hole*[1]. A escolha do *Pi-hole* como referência baseou-se em sua ampla adoção como sistema de bloqueio de domínios baseado em *DNS*, frequentemente instalado em dispositivos de baixo custo como a *Raspberry Pi*, sendo reconhecido por sua eficiência, simplicidade de uso e integração com listas públicas de bloqueio.

O *Pi-hole* destaca-se por funcionalidades como bloqueio de anúncios, aplicação de listas personalizadas de domínios, visualização de estatísticas de tráfego e uma interface administrativa acessível. No entanto, sua atuação limita-se ao nível do *DNS*, o que restringe sua capacidade de realizar bloqueios mais granulares, como por conteúdo ou por aplicação.

Neste sentido, a solução proposta neste trabalho diferencia-se ao adotar uma arquitetura integrada que amplia os mecanismos de controle disponíveis. O sistema incorpora, além do bloqueio por *DNS*, recursos como filtragem por *proxy* (`Squid`), aplicação forçada do *SafeSearch*, controle de palavras-chave e bloqueios específicos por portas e *IPs* utilizando `iptables`. Essa combinação de técnicas visa oferecer um controle parental mais robusto e flexível, com foco específico na proteção do público infantojuvenil em ambientes educacionais ou residenciais.

[1] <https://pi-hole.net>

3.2.2 AdGuard Home

O AdGuard Home[2] é uma solução de bloqueio de conteúdo baseada em *DNS*, desenvolvida como alternativa ao Pi-hole, com foco em controle parental, privacidade e bloqueio de anúncios. Ele atua como um resolvedor *DNS* local, interceptando requisições de nomes de domínio feitas pelos dispositivos da rede. Quando uma requisição coincide com domínios presentes em listas de bloqueio (*blocklists*), o AdGuard retorna uma resposta nula ou redirecionada, impedindo o acesso ao conteúdo.

Diferentemente do Pi-hole, o AdGuard Home fornece filtros configuráveis por categorias (ex: conteúdo adulto, redes sociais, rastreadores), suporte nativo ao *SafeSearch* em mecanismos de busca (Google, Bing, YouTube), além de permitir a criação de regras por dispositivo. Sua interface *web* é moderna e permite a visualização de estatísticas de acesso, tempo real de consultas *DNS* e *logs* detalhados.

Embora eficiente, o AdGuard Home atua exclusivamente utilizando *DNS*, não oferecendo inspeção de tráfego, bloqueio por *URL* completa, nem controle por porta ou protocolo.

3.2.3 Qustodio

O Qustodio[3] é uma solução de controle parental baseada em *software* cliente-servidor, instalada diretamente nos dispositivos que se deseja monitorar. Ele oferece monitoramento em tempo real, controle de tempo de uso, bloqueio de aplicativos, filtragem de conteúdo *web* e relatórios detalhados por usuário. É multiplataforma, com versões para Windows, macOS, Android, iOS e Kindle.

O funcionamento do Qustodio se dá através de um agente local que intercepta e analisa o tráfego de rede no próprio dispositivo, independentemente do *DNS* utilizado. Com isso, ele consegue bloquear tanto domínios como *URLs* específicas, mesmo que estejam dentro de domínios permitidos (ex: bloquear apenas o caminho `/chat` de um domínio válido).

Além disso, permite aplicação de regras por horários, alertas de atividade suspeita, rastreamento de localização (em dispositivos móveis) e gestão centralizada via painel *online*. No entanto, como se trata de uma solução cliente, sua eficácia depende da instalação e manutenção ativa nos dispositivos alvo, podendo ser desabilitado por usuários com permissões administrativas.

[2] <https://adguard.com/en/adguard-home/overview.html>
[3] <https://www.qustodio.com/pt-br/product-features/l>

Tabela 1 – Comparativo entre Pi-hole, AdGuard Home, Qustodio e a Solução Proposta

Funcionalidade	**Pi-hole**	**AdGuard**	**Qustodio**	**Solução Proposta**
Bloqueio de domínios via *DNS*	✓	✓	✓	✓
Bloqueio de anúncios (ads)	✓	✓	–	–
Bloqueio de conteúdo via *proxy* (`Squid`)	–	–	–	✓
Aplicação de *SafeSearch* em mecanismos de busca	–	✓	✓	✓
Bloqueios personalizados por dispositivo ou usuário	–	✓	✓	–
Bloqueio de serviços por portas e IPs	–	–	–	✓
Interface de administração baseada na *web*	✓	✓	✓	✓
Relatórios e estatísticas de tráfego	✓	✓	✓	✓
Controle de tempo de uso	–	–	✓	–
Dependência de instalação local nos dispositivos	–	–	✓	–

4 Metodologia

O presente trabalho propõe uma solução que atua como uma ponte segura entre os usuários e a internet, com o objetivo de proporcionar um ambiente supervisionado e tecnicamente controlado. Em um cenário comum, um dispositivo como um celular ou *tablet* é utilizado para acesso à internet por menores de idade. Embora a interface pareça simples e amigável, existe por trás dela uma arquitetura robusta que monitora, registra e, quando necessário, restringe as requisições realizadas.

Entre o dispositivo e os conteúdos disponíveis na rede, estabelece-se uma camada de proteção: um intermediário técnico que acompanha o tráfego, impede acessos a conteúdos inadequados, aplica filtros em mecanismos de busca e consolida informações relevantes para análise posterior. Diferentemente de soluções passivas, o sistema proposto permite a atuação ativa dos responsáveis, tanto na supervisão quanto na definição de políticas de acesso.

A experiência de navegação permanece fluida na maior parte do tempo, mas pode ser interrompida quando são identificados conteúdos classificados como sensíveis ou restritos. Essa reação imediata é parte essencial da proposta, que busca promover um equilíbrio entre liberdade digital e proteção supervisionada.

Essa arquitetura pode ser visualizada de forma conceitual como uma barreira inteligente: embora discreta, permanece constantemente ativa — analisando, protegendo e oferecendo aos responsáveis uma visão clara sobre o ambiente digital em uso.

A seguir, apresenta-se uma representação conceitual da solução (Figura 2):

- Um usuário infantojuvenil, representado pelo dispositivo móvel em mãos, como ponto inicial de acesso ao ambiente digital;
- Um roteador secundário, posicionado entre o usuário e a internet, responsável por aplicar as políticas de filtragem e monitoramento do tráfego;
- Um painel de controle, acessível aos responsáveis, que fornece relatórios e permite a configuração das regras de acesso;
- O responsável ou administrador, simbolizando a supervisão e o gerenciamento da rede doméstica;
- A internet (*World Wide Web*), destino final do tráfego após passar pelas camadas de controle.

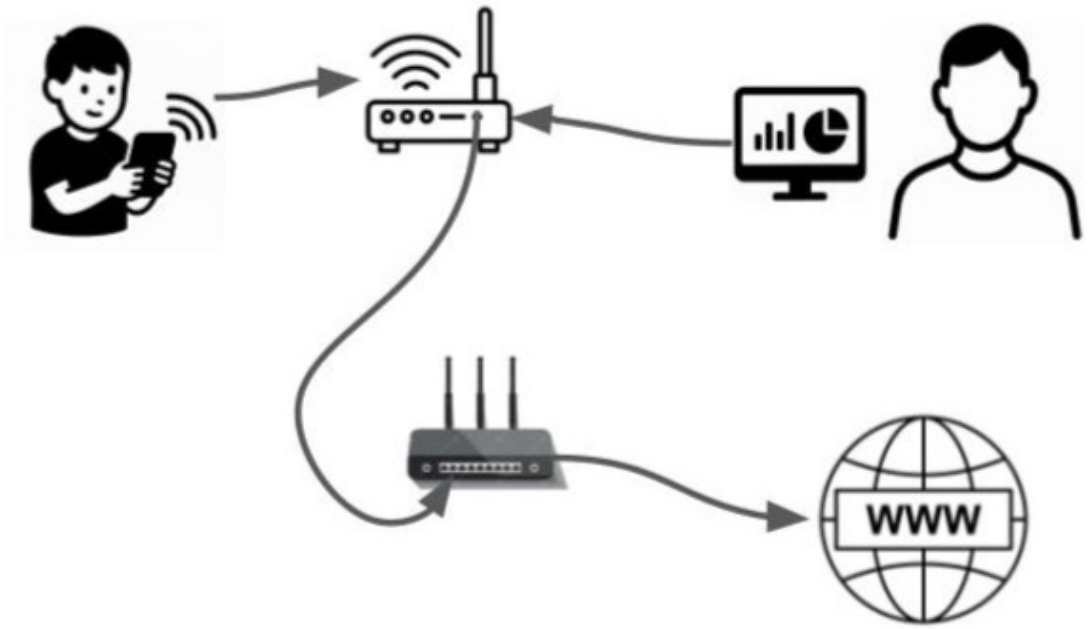

Figura 2 – Visão abstrata da estrutura de rede.

Essa abordagem busca transformar a rede doméstica em um ambiente supervisionado, seguro e formativo, por meio da combinação entre controle técnico e participação ativa dos responsáveis.

Com o propósito de equilibrar liberdade de navegação e responsabilidade, foi desenvolvido um sistema capaz de registrar acessos, identificar termos sensíveis e fornecer uma interface intuitiva para o acompanhamento em tempo real da experiência digital dos usuários.

4.1 Levantamento de requisitos

A solução desenvolvida neste trabalho opera com base em três ações principais, que atuam de forma integrada para garantir um ambiente digital seguro, supervisionado e adaptável às necessidades dos responsáveis:

(1) Garantir uma rede filtrada e segura: ao se conectar à rede local, os dispositivos passam a utilizar automaticamente um servidor *DNS* com filtragem de conteúdo, aliado à navegação via *proxy* (Squid) e à aplicação forçada do *SafeSearch* nos mecanismos de busca. Essa infraestrutura inicial bloqueia o acesso a domínios inadequados logo na origem, antes mesmo de o conteúdo ser requisitado pelo navegador.

(2) Permitir personalização das restrições: a infraestrutura implementada possibilita a configuração dinâmica de políticas de acesso, como bloqueio de domínios específicos, categorias de serviços (por exemplo, redes sociais ou mensageiros) e palavras-chave sensíveis. Essas regras podem ser aplicadas ou modificadas em tempo real por meio do painel

administrativo, permitindo adaptações conforme o perfil e a faixa etária dos usuários da rede.

(3) Fornecer visualização e relatórios de navegação: todas as atividades relevantes são registradas e consolidadas em um painel *web*, intuitivo, acessível localmente. Os responsáveis podem consultar registros de acesso, verificar tentativas de violações e tomar decisões baseadas em dados objetivos. A interface foi projetada para ser compreensível mesmo para usuários sem formação técnica e permite a busca por termos específicos, facilitando a identificação de conteúdos sensíveis como *baleia-azul*, *pornografia*, entre outros.

Essa abordagem baseada em camadas de proteção, personalização e supervisão ativa permite que a rede doméstica funcione como um espaço digital controlado, educativo e flexível, equilibrando segurança com o desenvolvimento progressivo da autonomia digital dos usuários.

4.2 Ambiente de Configuração Inicial

A base do sistema foi construída utilizando uma *Raspberry Pi*, configurada para atuar como ponto central de roteamento e filtragem da rede local.

A arquitetura da solução foi concebida para operar em três frentes principais. A primeira consiste no redirecionamento do tráfego para um servidor *DNS* com filtragem de conteúdo, focado no bloqueio de domínios impróprios e na imposição do modo restrito em mecanismos de busca, promovendo uma navegação segura desde a origem.

A segunda camada é composta por um *proxy* configurado manualmente, responsável por interceptar e analisar requisições *HTTP* e *HTTPS*, aplicando regras de bloqueio por domínio, palavras-chave e categoria de serviço — como redes sociais e aplicativos de mensagens — conforme os critérios estabelecidos pelos responsáveis.

Por fim, todas as requisições processadas são registradas em arquivos de *log* e posteriormente organizadas em um painel de administração *web*. Essa interface permite visualizações em tempo real, geração de relatórios e aplicação de novos bloqueios de forma simplificada e acessível.

Esse ambiente de configuração inicial estabelece as bases operacionais do sistema, oferecendo uma infraestrutura doméstica segura, flexível e de fácil manutenção. Tal preparação foi essencial para viabilizar a validação prática da proposta, abordada na próxima seção.

5 Implementação

A etapa de implementação consistiu na configuração e integração dos componentes que compõem a solução proposta, baseada em uma *Raspberry Pi 4 Model B*[1] com 8GB de memória RAM e cartão *microSD SanDisk Ultra G10* de 32GB, operando com o sistema *Raspberry Pi OS (Lite)*[2].

A escolha pela *Raspberry Pi* em detrimento de um computador convencional deve-se a fatores como a eficiência energética, que permite operação contínua com baixo consumo, o baixo custo de aquisição, a disponibilidade do equipamento na instituição de ensino e a familiaridade prévia do autor com a plataforma, adquirida em atividades acadêmicas. Além disso, a *Raspberry Pi 4 Model B* já dispõe de interfaces de rede integradas, como porta *Ethernet* e módulo *Wi-Fi*, possibilitando a criação e o gerenciamento da rede local sem a necessidade de placas adicionais. Tais características tornam o dispositivo especialmente adequado para a implementação de uma solução doméstica de controle parental, alinhada à proposta deste trabalho.

Para viabilizar todas as funcionalidades do sistema, foram instalados os principais serviços para controle e monitoramento da rede, incluindo o servidor *web Apache2*[3], o interpretador *PHP*[4], o banco de dados *MariaDB*[5], o agendador de tarefas *cron*[6], o resolvedor de nomes *dnsmasq*[7] e o servidor *proxy Squid*. Também foram utilizadas as ferramentas de *firewall* como *iptables* para controle do tráfego e aplicação de regras de acesso personalizadas.

Adicionalmente, foi configurado um *Virtual Host* no servidor *Apache2*, com o objetivo de permitir o redirecionamento automático para o domínio interno `safenetzone.me`, previamente definido no *dnsmasq*, proporcionando uma navegação mais intuitiva e integrada ao painel administrativo. Para facilitar a visualização e administração do banco de dados, foi instalado o *phpMyAdmin*[8], acessível via interface gráfica. Também foram definidas permissões específicas de execução por meio do utilitário *visudo*[9], garantindo que os *scripts* automatizados pudessem ser executados com privilégios elevados de forma segura e controlada. O código-fonte do projeto foi mantido em repositório no `GitHub`[10], viabilizando versionamento,

[1] <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/>
[2] <https://www.raspberrypi.com/software/>
[3] <https://httpd.apache.org/>
[4] <https://www.php.net/>
[5] <https://mariadb.org/>
[6] <https://man7.org/linux/man-pages/man8/cron.8.html>
[7] <http://www.thekelleys.org.uk/dnsmasq/doc.html>
[8] <https://www.phpmyadmin.net/>
[9] <https://man7.org/linux/man-pages/man8/visudo.8.html>
[10] <https://github.com/>

backup e reinstalação simplificada do sistema. A integração desses componentes permitiu a operação coordenada da arquitetura proposta, assegurando o bloqueio em tempo real, o registro de atividades e a personalização dinâmica das regras restritivas por meio do painel administrativo.

A seguir, são apresentadas evidências visuais dos principais componentes do sistema:

5.1 Configuração do *Proxy* (Squid)

squid.conf

```
1  # Porta do proxy (sem redirecionamento automático)
2  http_port 3128
3
4  #DNS
5  dns_nameservers 127.0.0.1
6
7  # Bloqueio por domínio
8  acl bloqueio_sites dstdomain "/var/www/html/rede-segura/arquivos-gerados-pelo-sistema/squid-blocklists/block-squid.txt"
9  http_access deny bloqueio_sites
10
11 # Bloqueio por palavras
12 acl palavras_proibidas url_regex -i "/var/www/html/rede-segura/arquivos-gerados-pelo-sistema/squid-blocklists/block-palavras.txt"
13 http_access deny palavras_proibidas
14
15 # Permite apenas conexões locais
16 acl localnet src 192.168.10.0/24
17 http_access allow localnet
18 http_access deny all
19
20 # Logs ativados (para relatórios)
21 access_log /var/log/squid/access.log
22 cache_log /var/log/squid/cache.log
23
24 # Cache desativado (para reduzir uso de disco)
25 cache deny all
26
27 # Registre URLs completas
28 logformat combined %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %Hs %<st "%{Referer}>h" "%{User-Agent}>h"
```

Figura 3 – Trecho do arquivo `squid.conf` contendo as diretivas de controle de bloqueios por domínio e palavras-chave.

O *proxy Squid* foi configurado para operar de forma explícita, o que exige que os dispositivos clientes sejam previamente ajustados para utilizar manualmente o serviço, informando o endereço IP (`192.168.10.1`) e a porta correspondente (`3128`). Essa abordagem fortalece o controle de rede, pois garante que apenas dispositivos configurados com o *proxy* tenham acesso à internet.

Uma vez configurado, todo o tráfego HTTP e HTTPS dos dispositivos passa obrigatoriamente pelo *Squid*, permitindo a aplicação de políticas de acesso por meio de *ACLs* (Listas de Controle de Acesso). Essas listas são fundamentais para o funcionamento do sistema de bloqueio, sendo em duas principais categorias:

- **Bloqueio por domínio**: Como mostrado nas linhas 8 e 9 da Figura 3, uma lista de domínios completos é mantida no arquivo `block-squid.txt`, localizado em `</var/www/html/rede-segura/arquivos-gerados-pelo-sistema/squid-blocklists/>`. Essa lista contém, por exemplo, entradas de domínios com-

pletos (como *.whatsapp.com*, *web.whatsapp.com*, *.discord.com*, etc.), os quais são bloqueadas integralmente assim que detectadas nas requisições de destino.

- **Bloqueio por palavras-chave no domínio**: Já nas linhas 12 e 13 da mesma figura, o sistema também permite o bloqueio de URLs com base em expressões regulares. A lista `block-palavras.txt`, localizada na mesma pasta, pode conter palavras ou trechos específicos (como `suicidio`, `baleia-azul`, `pornografia`, `etc`.) que, quando presentes em qualquer parte da URL requisitada, provocam o bloqueio imediato da conexão.

Essas regras são gerenciadas dinamicamente através do painel administrativo, permitindo ao responsável atualizar as listas de bloqueio em tempo real, sem necessidade de reiniciar o serviço manualmente.

Para assegurar o registro das atividades, o *Squid* foi configurado com um formato de *log* estendido, armazenando informações detalhadas sobre as requisições realizadas. O arquivo `access.log` é posteriormente processado por um *script PHP* que o consolida no banco de dados e exibe essas informações no painel administrativo.

5.2 Configurações de Rede Local e DNS com `dhcpcd` e `dnsmasq`

O serviço `dnsmasq` foi adotado como resolvedor local de nomes e servidor DHCP da rede, atuando como componente central no gerenciamento das conexões. Sua configuração foi ajustada para atender a três objetivos principais: (i) garantir o uso de servidores DNS com filtragem de conteúdo familiar, (ii) forçar o redirecionamento de domínios específicos para endereços IP internos ou filtrados e (iii) facilitar o acesso ao painel administrativo através de um domínio amigável.

Para assegurar a navegação segura, o sistema foi configurado para utilizar os servidores *OpenDNS FamilyShield* (`208.67.222.123` e `208.67.220.123`), que aplicam filtros automáticos contra conteúdos inapropriados. Todos os dispositivos conectados à rede recebem, via protocolo *DHCP*, as configurações de IP, *gateway* e DNS fornecidas pelo próprio `dnsmasq`, o que garante a correta aplicação das regras definidas.

Adicionalmente, foram definidas entradas estáticas de redirecionamento para ativar automaticamente o *SafeSearch* em serviços de busca. Por exemplo, os domínios *google.com* e *youtube.com* foram apontados, respectivamente, para os IPs `216.239.38.120` e `216.239.38.119`, utilizados oficialmente pelo Google para forçar o *SafeSearch*. Essa abordagem assegura que, independentemente das preferências de usuário ou navegador, os resultados de busca sejam sempre filtrados.

O domínio local `safenetzone.me` também foi redirecionado internamente para o IP do servidor (`192.168.10.1`), permitindo que os usuários acessem o painel administrativo por

meio de um endereço personalizado. A funcionalidade foi complementada com a criação de um *Virtual Host* no servidor `Apache2`, garantindo o encaminhamento correto das requisições HTTP.

Além disso, foram incluídas entradas de bloqueio específicas para domínios utilizados por serviços de DNS sobre HTTPS (DoH), como `dns.google`, `cloudflare-dns.com` e `nextdns.io`, impedindo que dispositivos tentem contornar o filtro DNS configurado pelo sistema.

Complementando as medidas de segurança, o `dnsmasq` opera de forma integrada com o `iptables`, que bloqueia qualquer tentativa de resolução de nomes por servidores DNS externos, reforçando a obrigatoriedade do uso do DNS interno para todos os dispositivos da rede.

A configuração detalhada do serviço pode ser vista na Figura 4, enquanto os parâmetros de IP fixo da interface de rede estão definidos na Figura 5.

dnsmasq.conf

```
interface=wlan0
dhcp-range=192.168.10.10,192.168.10.50,255.255.255.0,24h
dhcp-option=option:dns-server,192.168.10.1

# Redirecionamento
address=/safenetzone.me/192.168.10.1

# ===== [SafeSearch - Forçar Redirecionamento] ===== #

# SafeSearch Google e Youtube
address=/google.com/216.239.38.120
address=/google.com.br/216.239.38.120
address=/youtube.com/216.239.38.119
address=/youtube.com.br/216.239.38.119

# Bing
address=/bing.com/204.79.197.220
address=/www.bing.com/204.79.197.220

# DuckDuckGo
address=/duckduckgo.com/52.250.42.157

# Permita todo o resto para o DNS do OpenDNS FamilyShield
server=208.67.222.123
server=208.67.220.123
no-resolv

# Bloqueio via DNS dos SERVIÇOS
conf-file=/var/www/html/rede-segura/arquivos-gerados-pelo-sistema/dnsmasq-blocklists/block-dnsmasq.conf

# Bloqueio de domínios de DNS over HTTPS
address=/dns.google/0.0.0.0
address=/dns.quad9.net/0.0.0.0
address=/mozilla.cloudflare-dns.com/0.0.0.0
address=/cloudflare-dns.com/0.0.0.0
address=/doh.opendns.com/0.0.0.0
address=/dns.adguard.com/0.0.0.0
address=/dns.nextdns.io/0.0.0.0
address=/security.cloudflare-dns.com/0.0.0.0
```

Figura 4 – Trecho do arquivo `dnsmasq.conf` com configuração de DHCP, redirecionamentos e bloqueios DNS.

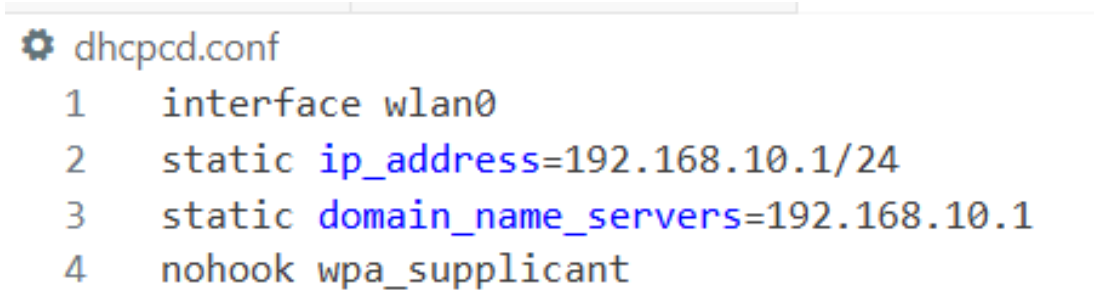

Figura 5 – Trecho do arquivo `dhcpcd.conf` com a definição do IP estático para a interface `wlan0`.

5.3 Firewall e Regras de Controle de Tráfego com `iptables`

O controle de tráfego de rede foi implementado por meio de regras específicas no `iptables`, utilizando a tabela `filter` para filtragem de pacotes e a tabela `nat` para redirecionamento de conexões, conforme ilustrado na Figura 6. O objetivo foi criar um ambiente onde o acesso à internet ocorresse somente mediante configuração manual do *proxy* `Squid`, além de impedir o uso de servidores DNS externos.

Para garantir que somente os dispositivos que utilizam o `proxy` tenham acesso à internet, foram criadas regras que bloqueiam todas as portas HTTP (`80`) e HTTPS (`443`) destinadas a endereços externos, permitindo o tráfego somente quando o destino for o próprio servidor, na porta do `Squid` (`3128`). Com isso, dispositivos não configurados com o proxy são automaticamente privados de conexão externa.

Além disso, foram definidas regras específicas destinadas a bloquear o tráfego direcionado a servidores DNS públicos amplamente utilizados, como Google DNS (`8.8.8.8`, `8.8.4.4`) e Cloudflare (`1.1.1.1`), tanto em TCP quanto UDP, nas portas `53`. Isso garante que todas as consultas DNS sejam resolvidas exclusivamente pelo `dnsmasq`, centralizando o controle de resolução de nomes e impedindo a evasão de filtros via DNS alternativo.

O sistema também recorre ao módulo *ipset*[11], permitindo o gerenciamento dinâmico de listas de IPs autorizados a acessar a internet. Essas listas são alimentadas automaticamente por um *script* que identifica dispositivos com *proxy* corretamente configurado. Uma vez incluídos na lista de IPs permitidos, esses dispositivos têm suas requisições liberadas, inclusive tráfegos por portas não convencionais, desde que a comunicação inicial tenha sido corretamente encaminhada pelo *proxy*. Isso torna o controle mais flexível e escalável, possibilitando adições e remoções em tempo real, sem a necessidade de reiniciar o serviço de *firewall*.

As regras definidas no `iptables` são carregadas automaticamente na inicialização do sistema, por meio do arquivo `/etc/iptables/rules.v4`, garantindo persistência e

[11] <https://ipset.netfilter.org/>

segurança contínua.

iptables.conf

```
# Regras Filter
*filter
:INPUT ACCEPT [13492:5192923]
:FORWARD DROP [86:5288]
:OUTPUT ACCEPT [4495:1301227]
-A FORWARD -m set --match-set liberados src -j ACCEPT
-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -d 192.168.10.1/32 -i wlan0 -p tcp -m tcp --dport 3128 -j ACCEPT
-A FORWARD -d 192.168.10.1/32 -p udp -m udp --dport 53 -j ACCEPT
-A FORWARD -d 192.168.10.1/32 -p tcp -m tcp --dport 53 -j ACCEPT
-A FORWARD -d 8.8.8.8/32 -p tcp -m tcp --dport 53 -j DROP
-A FORWARD -d 8.8.8.8/32 -p udp -m udp --dport 53 -j DROP
-A FORWARD -d 8.8.4.4/32 -p tcp -m tcp --dport 53 -j DROP
-A FORWARD -d 8.8.4.4/32 -p udp -m udp --dport 53 -j DROP
-A FORWARD -d 1.1.1.1/32 -p tcp -m tcp --dport 53 -j DROP
-A FORWARD -d 1.1.1.1/32 -p udp -m udp --dport 53 -j DROP
-A FORWARD -d 1.0.0.1/32 -p tcp -m tcp --dport 53 -j DROP
-A FORWARD -d 1.0.0.1/32 -p udp -m udp --dport 53 -j DROP
-A FORWARD -d 208.67.222.222/32 -p tcp -m tcp --dport 53 -j DROP
-A FORWARD -d 208.67.222.222/32 -p udp -m udp --dport 53 -j DROP
-A FORWARD -d 208.67.220.220/32 -p tcp -m tcp --dport 53 -j DROP
-A FORWARD -d 208.67.220.220/32 -p udp -m udp --dport 53 -j DROP
-A OUTPUT -p tcp -m owner --uid-owner 13 -j ACCEPT
COMMIT


# Regras NAT
*nat
:PREROUTING ACCEPT [779:71700]
:INPUT ACCEPT [749:51815]
:OUTPUT ACCEPT [985:71582]
:POSTROUTING ACCEPT [985:71582]
-A PREROUTING -i wlan0 -p udp -m udp --dport 53 -j DNAT --to-destination 192.168.10.1
-A PREROUTING -i wlan0 -p tcp -m tcp --dport 53 -j DNAT --to-destination 192.168.10.1
-A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADE
COMMIT
```

Figura 6 – Trecho das regras do `iptables` com bloqueio de DNS externo, controle de acesso via proxy e uso de listas dinâmicas com `ipset`.

5.4 Painel Administrativo e Monitoramento de Navegação

O sistema conta com um painel administrativo desenvolvido sob medida, acessível por meio do domínio interno *safenetzone.me*, que permite o gerenciamento dinâmico das funcionalidades de controle da rede. A interface exibe as conexões realizadas pelos dispositivos conectados, com informações como horário, destino, IP de origem, endereço *MAC* e tipo de acesso.

Por meio do painel, é possível aplicar regras de bloqueio de forma personalizada e imediata, sem a necessidade de reiniciar os serviços do sistema. As listas de bloqueio por domínio e por palavras-chave podem ser editadas diretamente, permitindo ações como bloquear temporariamente redes sociais, serviços de mensagens instantâneas ou termos

específicos relacionados a conteúdo sensível.

As requisições *web* realizadas pelos dispositivos são registradas no arquivo de *log* padrão do `Squid`, o `access.log`, que armazena dados como IP, horário, URL acessada, método HTTP, endereço MAC e código de resposta. Esse arquivo é processado por *scripts* desenvolvidos em `PHP`, que consolidam as informações em relatórios acessíveis via painel. Um dos recursos disponíveis é a busca por palavra-chave, que permite verificar se determinado termo foi pesquisado ou acessado em algum dispositivo conectado.

As Figuras 7 a 11 ilustram algumas funcionalidades do painel administrativo. A interface inicia com a tela de login, responsável por autenticar os usuários autorizados ao sistema. Em seguida, a área de configuração da rede fornece instruções para conexão e parametrização do ambiente. O módulo de bloqueios possibilita gerenciar restrições por domínio e palavra-chave, enquanto os relatórios permitem acompanhar a atividade monitorada. Entre eles, destaca-se o relatório de acessos bloqueados e a consulta por termos específicos, que oferecem aos responsáveis uma visão detalhada do tráfego e das tentativas de acesso a conteúdos indevidos.

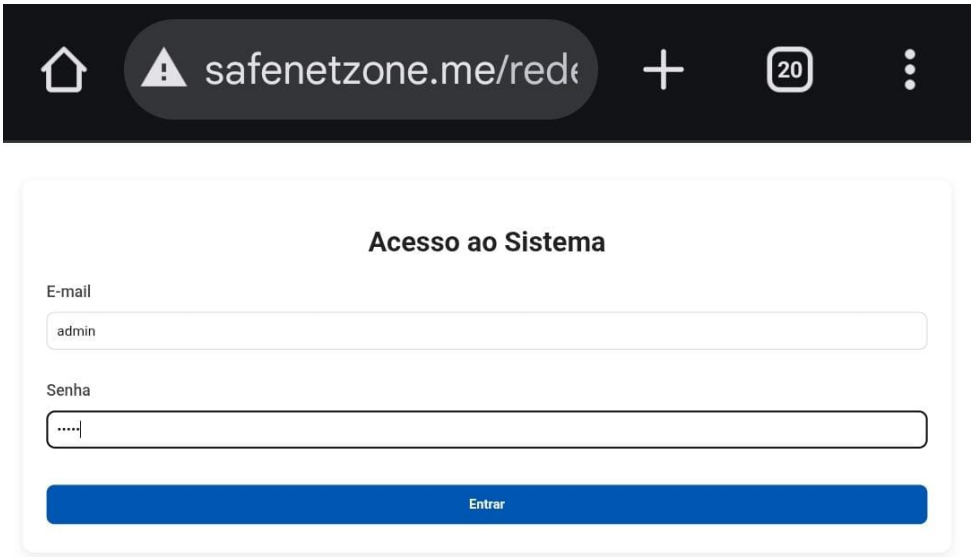

Figura 7 – Tela de login do painel administrativo da plataforma.

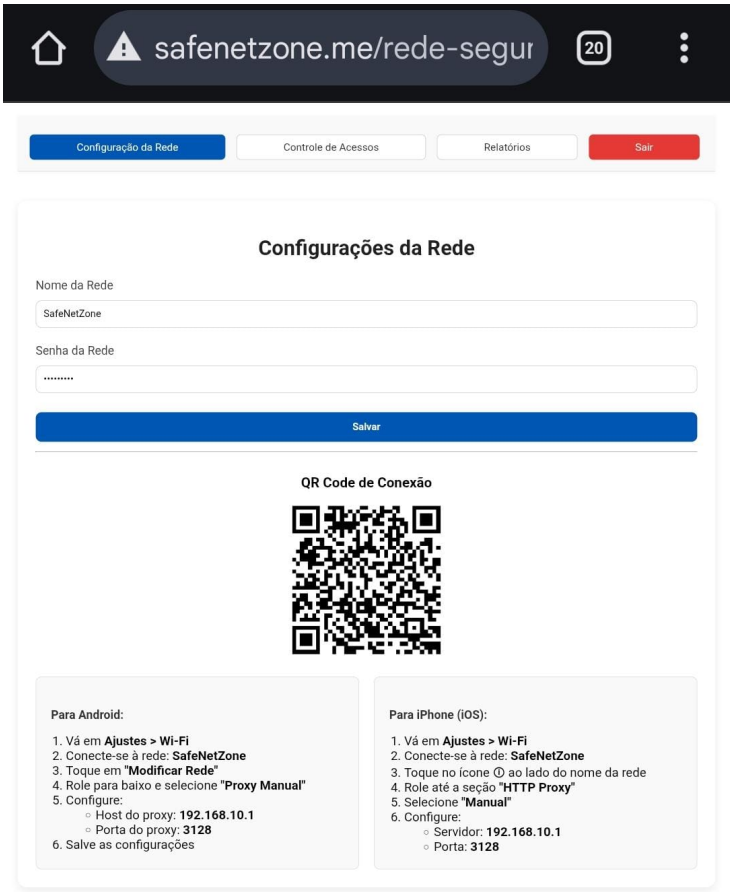

Figura 8 – Configuração da rede e instruções para conexão via painel administrativo.

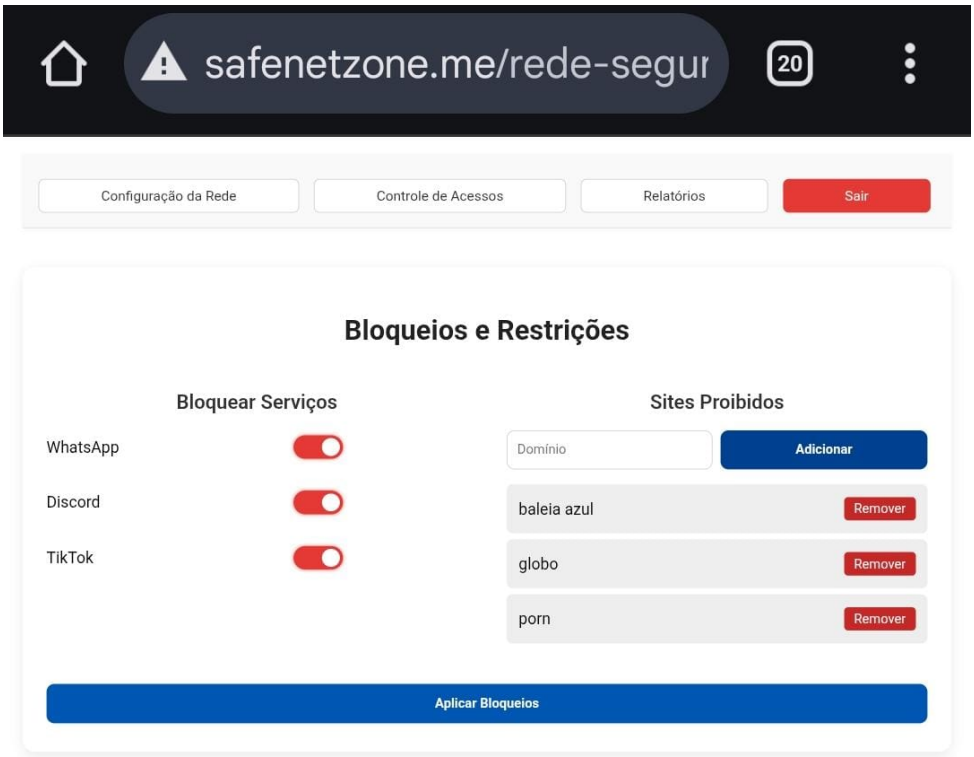

Figura 9 – Gerenciamento de bloqueios por domínio e palavra-chave.

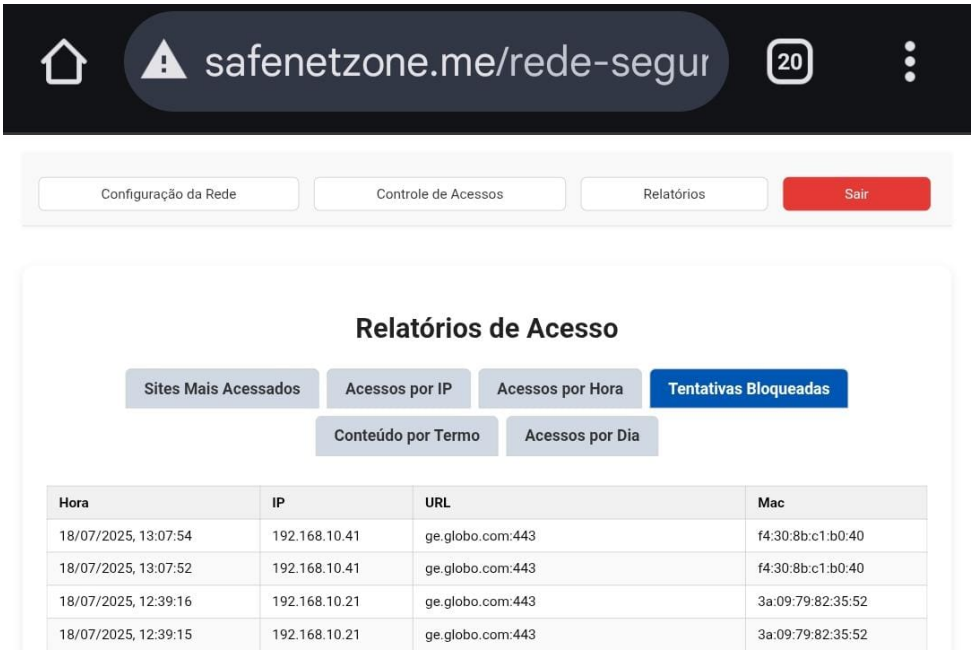

Figura 10 – Relatório de acessos bloqueados registrados pelo sistema.

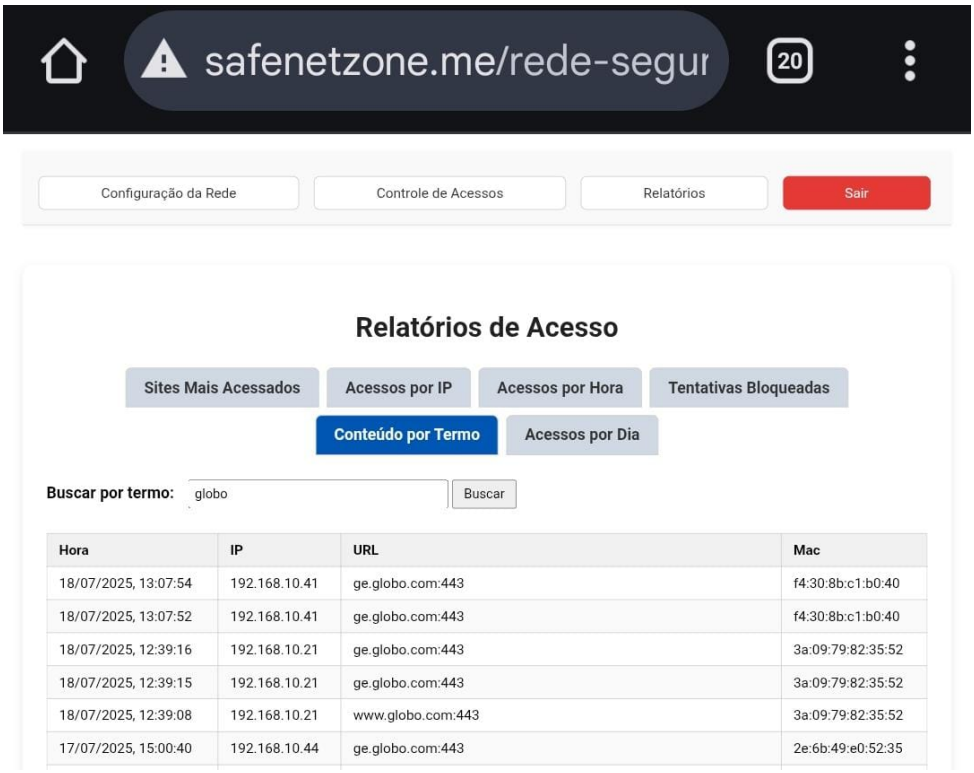

Figura 11 – Relatório com consulta por termos específicos nos registros de navegação.

Esta prova de conceito demonstra a funcionalidade completa do sistema, desde o bloqueio em camadas até a transparência na supervisão, validando sua aplicabilidade em cenários reais de uso doméstico.

5.5 Reprodutibilidade

O código-fonte do sistema proposto foi disponibilizado publicamente no GitHub, com o objetivo de promover a transparência, possibilitar reuso e permitir contribuições futuras. O repositório pode ser acessado em:

- <https://github.com/luispitta98/safenetzone/tree/main>

A imagem compactada do sistema utilizada no *Raspberry Pi* foi disponibilizada publicamente no Archive.org, com o intuito de facilitar a replicação da infraestrutura, promover a transparência do projeto e permitir reuso ou contribuições futuras; o arquivo pode ser acessado por meio do link indicado, e o primeiro acesso ao sistema deve ser realizado conectando-se à rede `SafeNetZone`, utilizando a senha `123456789` e informando o endereço IP do proxy (`192.168.10.1`) e a porta correspondente (`3128`).

- <https://archive.org/details/rasp_img>

6 Avaliações do Protótipo

A avaliação da solução foi realizada com base na implementação descrita anteriormente, que envolveu a instalação da proposta, intitulada *SafeNetZone*, configurada como *gateway* principal da rede local. O sistema foi equipado com funcionalidades de bloqueio de serviços e sites, geração de relatórios, forçamento de *SafeSearch* e aplicação de regras de *firewall* (iptables), *DNS* (dnsmasq) e proxy (Squid). Os testes foram conduzidos com usuários reais, que puderam experimentar o funcionamento da ferramenta, acessar o painel administrativo, aplicar restrições personalizadas, acessar relatórios e avaliar a experiência de uso.

Para mensurar a usabilidade, a percepção de segurança e a intenção de uso da plataforma, foi aplicado um questionário estruturado por meio do Google Forms. A amostra foi composta por 8 participantes, todos responsáveis legais por dependentes, que utilizaram a plataforma antes de responder à avaliação.

6.1 Perfil dos Participantes

Todos os respondentes confirmaram possuir filhos ou dependentes sob sua responsabilidade. Em relação à faixa etária, a maioria (5 participantes) informou que seus dependentes possuem 18 anos ou mais, enquanto os demais relataram faixas etárias mais jovens, incluindo combinações como 0 a 5 anos, 6 a 10 anos e 11 a 14 anos.

Quanto à preocupação com o conteúdo acessado *online*, quatro participantes relataram preocupação frequente, enquanto os demais se dividiram entre ausência de preocupação (2), preocupação ocasional (1) e rara (1).

No que diz respeito ao uso de ferramentas de controle parental, seis participantes afirmaram nunca ter utilizado esse tipo de solução, e dois declararam que sequer conheciam a existência dessas ferramentas antes da avaliação.

Quanto ao vínculo familiar dos participantes, observou-se uma diversidade de perfis, conforme apresentado na Figura 12. A maioria se declarou como responsável legal (37,5%), seguida por pais (25%), mães (25%) e avós/avôs (12,5%).

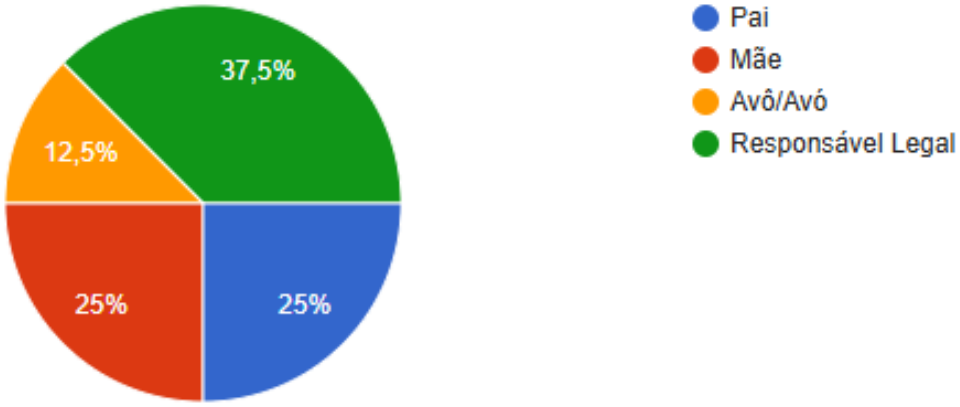

Figura 12 – Distribuição do perfil dos 8 participantes por vínculo familiar

6.2 Percepção sobre Funcionalidades

A análise das respostas revela uma aceitação significativa das funcionalidades oferecidas pela plataforma. Para três das quatro afirmativas avaliadas, todos os participantes indicaram concordância total. Apenas na segunda questão houve divergência mínima: seis concordaram totalmente e dois parcialmente, conforme apresentado na Tabela 2.

Enunciados das Questões:

- **Questão 1:** A possibilidade de bloquear serviços (como WhatsApp, Discord, TikTok) por meio de botões torna o processo mais prático e rápido ?
- **Questão 2:** A funcionalidade de bloqueio de sites por termos específicos (como "globo", "band") facilita a personalização da segurança da rede ?
- **Questão 3:** O sistema permite controlar com facilidade quais conteúdos são acessíveis na rede ?
- **Questão 4:** Os relatórios de acesso me ajudam a entender melhor o uso da internet na rede ?

Tabela 2 – Distribuição das respostas dos participantes sobre funcionalidades do sistema

Afirmativa	**Participantes**	**Resumo (% CT)**
Questão 1.	■ ■ ■ ■ ■ ■ ■ ■	**100%**
Questão 2.	■ ■ ■ ■ ■ ■ ■ ■	**75%**
Questão 3.	■ ■ ■ ■ ■ ■ ■ ■	**100%**
Questão 4.	■ ■ ■ ■ ■ ■ ■ ■	**100%**

Legenda: ■ Concordo totalmente ■ Concordo parcialmente ■ Nem concordo nem discordo ■ Discordo parcialmente ■ Discordo totalmente

6.3 Usabilidade da Plataforma

Sete dos oito participantes concordaram totalmente que aprender a utilizar a SafeNetZone foi fácil, enquanto um indicou concordância parcial. A clareza da interface apresentou a mesma distribuição: sete respostas indicando concordância total e uma parcial. Já quanto à afirmação de que a plataforma facilitou o processo de controle de acessos, todos os participantes concordaram totalmente, conforme ilustrado na Tabela 3.

Tabela 3 – Distribuição das respostas dos participantes sobre usabilidade da plataforma.

Afirmativa	**Participantes**	**Resumo (% CT)**
Aprender a utilizar a SafeNetZone foi fácil.	■ ■ ■ ■ ■ ■ ■ ■	**87,5%**
A usabilidade é clara e compreensível.	■ ■ ■ ■ ■ ■ ■ ■	**87,5%**
Facilitou o processo de controle de acessos.	■ ■ ■ ■ ■ ■ ■ ■	**100%**

Legenda: ■ Concordo totalmente ■ Concordo parcialmente ■ Nem concordo nem discordo ■ Discordo parcialmente ■ Discordo totalmente

6.4 Intenção de Uso

Todos os participantes concordaram totalmente com as três afirmativas relacionadas à intenção de uso: que utilizariam a SafeNetZone para configurar uma rede segura, que recomendariam a ferramenta a outros responsáveis e que se sentem mais seguros ao permitir que seus dependentes naveguem utilizando a plataforma.

Esse sentimento de segurança também foi reforçado por uma pergunta específica do questionário, que buscou avaliar diretamente a percepção dos usuários sobre a eficácia de ferramentas de controle parental:

> *"Você se sentiria mais seguro(a) se pudesse acompanhar e limitar o acesso à internet por meio de um sistema como o SafeNetZone?"*

Todos os participantes (100%) responderam afirmativamente, demonstrando forte adesão à proposta de monitoramento e restrição de conteúdos como medida de proteção no ambiente doméstico. A Figura 13 apresenta a unanimidade nas respostas.

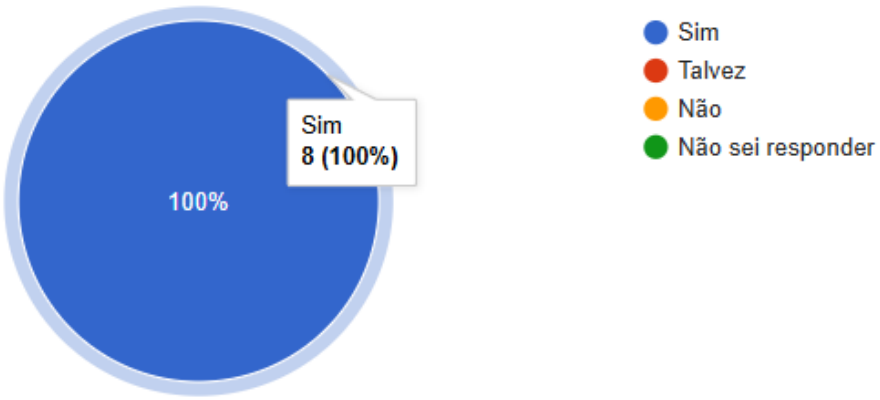

Figura 13 – Percepção de segurança em relação ao uso de um sistema de controle parental

6.5 Feedback Qualitativo

Os campos abertos do questionário foram organizados na Tabela 4, os principais pontos fortes apontados pelos participantes foram a segurança proporcionada à família, a abrangência dos recursos disponíveis e a facilidade de uso. Como ponto fraco, uma resposta mencionou a dificuldade na configuração inicial, enquanto outra expressou preocupação com a gestão de senhas familiares. Entre as sugestões de melhoria, destacaram-se o aumento de bloqueios pré-definidos e a inclusão de notificações em caso de risco.

Tabela 4 – Feedback qualitativo dos participantes sobre a plataforma

Categoria	**Comentário**
Pontos Fortes	- Facilidade para bloquear conteúdos e controlar o que é acessado. - Maior sensação de segurança, especialmente diante dos riscos atuais da internet. - Garante mais proteção para a família. - Contribui para a prevenção de acidentes *online*. - Todos os aspectos da plataforma são considerados positivos. - Filtros para proteger crianças e relatórios para acompanhamento. - Configuração facilitada por meio de botões, sem necessidade de comandos técnicos.
Pontos Fracos	- Dificuldade na configuração inicial. - Preocupação com o compartilhamento de senhas entre membros da família.
Sugestões	- Inclusão de mais opções de bloqueios pré-definidos. - Possibilidade de adicionar limitadores adicionais de uso. - Implementar controle de acesso à senha, evitando que toda a família tenha acesso. - Notificações em caso de risco ou tentativa de acesso indevido. - Agrupamento de serviços em categorias (ex: jogos, redes sociais), utilização de uma base centralizada de listas de bloqueios, evolução dos relatórios com gráficos aprimorados, aplicação de inteligência artificial na análise de dados e criação de perfis padrão com base em faixa etária.

Nota: As respostas foram levemente ajustadas para correção gramatical e padronização de estilo, com o objetivo de garantir clareza na apresentação. O conteúdo e o sentido original dos relatos foram integralmente preservados.

Para complementar a avaliação da solução, foram disponibilizados registros fotográficos dos testes realizados com os participantes, bem como a planilha contendo todas as respostas completas do questionário aplicado.

Fotos dos testes com os participantes disponíveis em:
`https://tinyurl.com/fotos-participantes-safenet`

Respostas completas do formulário disponível em:
`https://tinyurl.com/respostas-safenet`

7 Conclusão

Este trabalho apresentou o desenvolvimento e a implementação de uma solução prática e acessível para o controle e supervisão do acesso à internet em redes domésticas, com foco na proteção de crianças e adolescentes em ambientes digitais. A proposta foi concebida como um protótipo funcional, apoiado em princípios de pesquisa aplicada, e integrou diversas tecnologias de código aberto para criar uma plataforma completa de filtragem e monitoramento.

Por meio da utilização de uma *Raspberry Pi* como núcleo da infraestrutura, a solução combinou múltiplas camadas de proteção — incluindo filtragem *DNS*, *proxy*, *firewall* com redirecionamento de tráfego e forçamento de mecanismos como o *SafeSearch*. A plataforma desenvolvida permite o bloqueio de conteúdos inadequados, a geração de relatórios de acesso e a aplicação de políticas de restrição por meio de uma interface gráfica intuitiva.

A etapa de validação com participantes reais possibilitou observar como o sistema se comporta em um ambiente doméstico. Os dados coletados indicaram boa aceitação da proposta, destacando-se a facilidade de uso, a clareza da interface e a percepção de segurança promovida pelos recursos de bloqueio e supervisão. As respostas também revelaram sugestões relevantes, que apontam caminhos para aprimoramentos futuros.

Dessa forma, a implementação atendeu aos objetivos inicialmente propostos, demonstrando viabilidade técnica e funcionalidade adequada dentro do escopo da pesquisa. Embora se trate de um protótipo, os resultados obtidos reforçam o potencial da solução como ferramenta complementar de controle parental, especialmente em contextos com limitação de recursos técnicos ou financeiros.

7.1 Trabalhos Futuros

Como desdobramento deste projeto, propõem-se os seguintes aprimoramentos:

- Implementação de mecanismos de alerta em tempo real, com envio de notificações por *email* ou outros canais quando tentativas de acesso a conteúdos bloqueados forem detectadas;
- Expansão do painel administrativo com novas funcionalidades, como geração automática de relatórios periódicos, gráficos estatísticos e agrupamento por perfil de usuário;
- Criação de múltiplos perfis de acesso com políticas diferenciadas por faixa etária ou horário, tornando o sistema aplicável também a ambientes escolares ou redes com múltiplos responsáveis;

- Adaptação da solução para operar em modo híbrido (manual/transparente), facilitando a integração com redes já existentes e ampliando o alcance da proteção mesmo em dispositivos com menor suporte a configurações manuais.
- Exportação de relatórios em múltiplos formatos (CSV e PDF), com suporte a gráficos em tempo real para monitoramento dinâmico da rede.

Essas melhorias visam ampliar a escalabilidade e a eficiência da solução, mantendo seu caráter acessível, configurável e centrado na promoção de um ambiente digital mais seguro e consciente.

Referências

ARTA, Y.; SURYANI, D.; SYAFITRI, N.; HANAFIAH, A.; ELVIRA, D. Workshop aplikasi parental control windows 10. **Buletin Pembangunan Berkelanjutan**, v. 5, n. 2, p. 1–6, Sep. 2021. <https://journal.uir.ac.id/index.php/buletinpembangunan/article/view/7343>.

BARROS, E. D. S.; SILVA, M. A. L. Segurança rede de computadores: Controle parental. **Revista Tecnológica da Fatec Americana**, v. 7, n. 01, p. 70–83, 2019. <https://www.fatec.edu.br/revista/index.php/RTecFatecAM/article/view/211>.

BOUSNANE, R. Safe search engines to protect children and negative digital content reality and rationalization mechanisms. , v. 7, n. 2, p. 827–845, jul 2022. Disponível em: <https://asjp.cerist.dz/en/article/196331>. Disponível em: <https://asjp.cerist.dz/en/article/196331>.

CETIC. **TIC KIDS ONLINE BRASIL 2022**. 2022. <https://cetic.br/media/analises/tic_kids_online_brasil_2022_principais_resultados.pdf>.

CloudFlare. **O que é DNS? | Como o DNS funciona**. s.d. Disponível em: <https://www.cloudflare.com/pt-br/learning/dns/what-is-dns/>. Acesso em: 10 dez. 2025.

Câmara dos Deputados. **Os crimes cibernéticos contra crianças e adolescentes na internet**. 2024. <https://www.camara.leg.br/radio/programas/1155446-os-crimes-ciberneticos-contra-criancas-e-adolescentes-na-internet-reprise/>. Acesso em: 16 jul. 2025.

FANTASTICO. **Rede sem lei: no Discord, criminosos violentam e humilham meninas menores de idade**. 2023. <https://g1.globo.com/fantastico/noticia/2023/06/25/rede-sem-lei-no-discord-criminosos-violentam-e-humilham-meninas-menores-de-idade.ghtml>, Acessado em: 10 abr. 2025.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores: Uma Abordagem Top Down**. 1. ed. Porto Alegre: AMGH, 2013. Citação utilizada: p. 457.

KIMBALL, H. G.; FERNANDEZ, F.; MOSKOWITZ, K. A.; KANG, M.; ALEXANDER, L. M.; CONWAY, K. P.; MERIKANGAS, K. R.; SALUM, G. A.; MILHAM, M. P. Parent-perceived benefits and harms associated with internet use by adolescent offspring. **JAMA network open**, American Medical Association, v. 6, n. 10, p. e2339851–e2339851, 2023.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de redes em ambientes cooperativos**. [S.l.]: Novatec Editora, 2007.

NORTON. **2022 Norton Cyber Safety Insights Report: Special Release – Home & Family | NortonLifeLock**. 2022. <https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safety-insights-report-special-release-home-and-family/>. Acessado em 26 de junho de 2023.

PERES, F. **Monitoramento dos pais na internet X invasão de privacidade**. 2016. <https://www.jusbrasil.com.br/artigos/monitoramento-dos-pais-na-internet-x-invasao-de-privacidade/308216203>.

RICCI, B.; MENDONçA, N. **SQUID Solução Definitiva**. [S.l.]: CIENCIA MODERNA, 2006.

TARTUCE, F. **Abandono digital: negligência dos pais no mundo virtual**. 2017. Disponível em: https://www.jusbrasil.com.br/artigos/abandono-digital-negligencia-dos-pais-no-mundo-virtual-expoe-crianca-a-efeitos-nocivos-da-rede/418887019.

Veja. **O que é o 'desafio do desodorante' que causou a morte de menina em Pernambuco**. 2025. Acesso em: 18 jul. 2025. Disponível em: <https://veja.abril.com.br/coluna/maquiavel/o-que-e-desafio-do-desodorante-que-causou-morte-de-menina-em-pernambuco/>.

YAMAN, N. D.; KARADEMIR, A.; YAMAN, F. An investigation of the parental mediation situations of preschool children's parents. **Anadolu Journal of Educational Sciences International**, Anadolu University, v. 13, n. 2, p. 218–245, 2023.