INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ

CAMPUS TERESINA ZONA SUL

CURSO LICENCIATURA EM COMPUTAÇÃO

ISLÂNIO PABLO DOS SANTOS LUZ

A EFICÁCIA DO SOFTWARE OPENDNS NO CONTROLE DE ACESSOS INDEVIDOS EM LABORATÓRIOS DE INFORMÁTICA: UMA PESQUISA-AÇÃO NO CETI PROFESSOR MILTON AGUIAR.

TERESINA, PI

2026

ISLÂNIO PABLO DOS SANTOS LUZ

A EFICÁCIA DO SOFTWARE OPENDNS NO CONTROLE DE ACESSOS INDEVIDOS EM LABORATÓRIOS DE INFORMÁTICA: UMA PESQUISA-AÇÃO NO CETI PROFESSOR MILTON AGUIAR.

Trabalho de Conclusão de Curso (artigo científico) apresentado como exigência parcial para obtenção do diploma do Curso de Licenciatura em Computação do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul.

Professor Orientador: Jovennilton Soares de Sousa

TERESINA, PI

2026

A EFICÁCIA DO SOFTWARE OPENDNS NO CONTROLE DE ACESSOS INDEVIDOS EM LABORATÓRIOS DE INFORMÁTICA: UMA PESQUISA-AÇÃO NO CETI PROFESSOR MILTON AGUIAR.

Islânio Pablo dos Santos Luz[1]

Jovennilton Soares de Sousa[2]

RESUMO

A presente pesquisa avaliou o uso do software OpenDNS no controle de acessos indevidos no Laboratório de Informática do CETI Professor Milton Aguiar, em Teresina-PI. O objetivo foi identificar a frequência de acessos a conteúdos impróprios (como redes sociais e sites não educacionais) e avaliar como o bloqueio desses sites melhorou o andamento das aulas e a atenção dos alunos. A metodologia utilizada foi a pesquisa-ação, com abordagem quali-quantitativa. O estudo teve duas fases: uma exploratória (para entender o uso da internet antes dos filtros) e uma descritiva (para avaliar os resultados após o uso da ferramenta). Os dados foram coletados analisando os registros de acesso (logs) do OpenDNS e as respostas do professor aos questionários de diagnóstico e avaliação. Os resultados mostraram que o sistema bloqueou com sucesso conteúdos inadequados (como sites adultos e violentos) e reduziu o acesso a jogos online, mesmo com algumas dificuldades técnicas para bloquear certas redes sociais. Conclui-se que o uso do software facilitou muito o controle da turma, diminuindo a necessidade de o professor vigiar as telas o tempo todo. Isso criou um ambiente de aprendizado mais seguro e focado, sendo recomendada a continuidade do sistema na escola.

Palavras-chave: OpenDNS. Gestão Escolar. Segurança de Redes. Laboratório de Informática. Pesquisa-ação.

ABSTRACT

This research evaluated the use of the OpenDNS software to control inappropriate access in the Computer Laboratory of CETI Professor Milton Aguiar, in Teresina-PI. The objective was to identify the frequency of access to inappropriate content (such as social networks and non-educational websites) and to evaluate how blocking these sites improved class flow and student attention. The methodology used was action research, with a qualitative and quantitative approach. The study had two phases: an exploratory phase (to understand internet usage before the filters) and a descriptive phase (to evaluate the results after using the tool). Data was collected by analyzing the OpenDNS access records (logs) and the teacher's responses to diagnostic and evaluation questionnaires. The results showed that the system successfully blocked inappropriate content (such as adult and violent websites) and reduced access to online games, despite some technical difficulties in blocking certain social networks. It is concluded that the use of the software greatly facilitated class management, reducing the need for the teacher to constantly monitor the screens. This created a safer and more focused learning environment, and the continued use of the system in the school is recommended.

Keywords: OpenDNS. School Management. Network Security. Computer Laboratory. Action Research.

[1] Graduando(a) em Licenciatura em Computação. IFPI - Teresina Zona Sul. E-mail islaniopbl@gmail.com

[2] Professor mestre em Computação do curso de Licenciatura em Computação. Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul. E-mail jovennilton.sousa@ifpi.edu.br

INTRODUÇÃO

A aplicação de ferramentas tecnológicas para o controle de acessos indevidos em ambientes educacionais é um fator determinante para a qualidade do ensino (BAISHYA; KAKOTY, 2019). No Laboratório de Informática do CETI Professor Milton Aguiar, observações empíricas realizadas previamente evidenciaram que a ausência de um ambiente digital seguro e controlado permite, com frequência, a ocorrência de navegação inadequada. O monitoramento e bloqueio desses conteúdos impróprios como sites de violência, pornografia e jogos online apresentam-se como passos essenciais para a construção de um espaço produtivo, sendo a avaliação do software OpenDNS uma alternativa automatizada para essa gestão.

Situações de dispersão durante o horário letivo comprometem o foco dos alunos e prejudicam gravemente os objetivos pedagógicos do espaço. Esses materiais digitais incluem sites de ódio, redes sociais e plataformas de entretenimento que desviam a atenção discente e geram sérias vulnerabilidades.

Tais riscos são detalhadamente destacados por Dantas et al. (2023), que alertam para perigos iminentes, como a exposição a conteúdos prejudiciais, o contato com adultos mal-intencionados, o cyberbullying e a exploração comercial, reforçando a importância de adotar medidas rigorosas de segurança e supervisão para garantir um uso saudável da rede.

A urgência em implementar um controle mais rigoroso sobre a internet escolar tornou-se evidente durante a participação no Programa Institucional de Bolsas de Iniciação à Docência (PIBID), entre os anos de 2022 e 2024. Ao longo desse período, foi possível acompanhar diversos episódios de acessos rotineiros a jogos online e conteúdos pornográficos que, além de serem estritamente impróprios para menores de idade, inviabilizavam o andamento das aulas. A recorrência desses episódios demonstrou a ineficácia das medidas paliativas e a necessidade imediata de uma intervenção técnica e automatizada.

Diante desse cenário de dispersão e risco, a implementação do OpenDNS projeta-se como uma solução capaz de resgatar o alinhamento às necessidades pedagógicas da instituição. A adoção dessa filtragem de rede desponta como uma alternativa viável para interceptar o tráfego não autorizado, trazendo benefícios como a melhoria da segurança digital, a diminuição drástica de distrações e o consequente aumento da produtividade. Simultaneamente, considera-se a

possibilidade de a ferramenta enfrentar a resistência dos estudantes na tentativa de contornar as restrições impostas, fator que ressalta a importância de avaliar as limitações práticas da solução adotada.

Para reverter o quadro de vulnerabilidade do laboratório, o presente trabalho tem como objetivo geral avaliar na prática a eficácia do software OpenDNS no controle de acessos indevidos. Como objetivos específicos, busca-se mapear detalhadamente os tipos de conteúdos impróprios requisitados; instalar e configurar filtros específicos na rede local; medir numericamente a redução do acesso a materiais prejudiciais; e, por fim, analisar as mudanças efetivas no ambiente de aprendizado e o nível de satisfação do professor em relação ao restabelecimento do uso seguro da internet.

2 CONTROLE DE ACESSOS E MEDIAÇÃO TECNOLÓGICA NO AMBIENTE ESCOLAR

O uso da tecnologia em ambientes educacionais tem se tornado cada vez mais essencial, especialmente com a popularização de laboratórios de informática e o acesso à internet nas escolas. No entanto, o acesso indiscriminado à rede pode levar ao uso inadequado dos recursos tecnológicos, como o acesso a conteúdos impróprios, que distraem os alunos e comprometem o ambiente de aprendizado. Conforme destacado por Baishya e Kakoty (2019), a filtragem de conteúdo é uma estratégia fundamental para garantir que a internet seja utilizada de forma produtiva e segura, alinhando-se aos objetivos pedagógicos.

Nesse contexto, ferramentas como o OpenDNS surgem como soluções tecnológicas promissoras para o controle de acessos indevidos. O OpenDNS atua como um serviço de DNS[3] que permite bloquear categorias de sites inadequados, como pornografia, jogos online e conteúdos violentos, conforme descrito em sua documentação oficial OpenDNS (2025). Essa funcionalidade não apenas protege os usuários de conteúdos prejudiciais, mas também contribui para a criação de um ambiente digital mais seguro e focado no aprendizado.

[3] Sistema de nomes de domínios que funciona como uma "lista telefônica" da internet, traduzindo nomes de sites (como www.google.com) em endereços de IP numéricos que os computadores entendem.

2.1 A IMPORTÂNCIA DO CONTROLE DE ACESSO EM AMBIENTES EDUCACIONAIS

A tecnologia tem se tornado cada vez mais presente nos ambientes educacionais, especialmente com o uso de laboratórios de informática (SILVA; SANTOS, 2020). A integração da tecnologia e da internet transformou as práticas de ensino-aprendizagem, consolidando-se como uma ferramenta essencial para o acesso à informação, a realização de pesquisas e o desenvolvimento das habilidades digitais necessárias aos estudantes na sociedade contemporânea. Nesse cenário, o laboratório de informática deixa de ser apenas um espaço técnico para se tornar um ambiente fundamental de construção de conhecimento.

No entanto, a simples disponibilização do acesso à rede não garante o aprendizado. O acesso indiscriminado à internet pode levar ao uso inadequado dos recursos tecnológicos, expondo os alunos a conteúdos impróprios e distrações que fogem ao escopo da aula. Conforme alertam Dantas e Azevedo (2023), a internet expõe crianças e adolescentes a riscos severos, como a exposição a materiais de violência, pornografia, discursos de ódio e a prática de *cyberbullying*. Em um ambiente escolar, a ausência de controle sobre esses fatores não apenas coloca em risco a segurança e o bem-estar dos estudantes, mas também desvia o foco dos objetivos pedagógicos propostos pelos professores.

Além da questão da segurança, o controle de acesso é vital para a produtividade educacional. Baishya e Kakoty (2019) destacam que a filtragem de conteúdo é essencial para garantir que a internet seja utilizada de forma produtiva. Sem ferramentas de mediação, o laboratório de informática corre o risco de se tornar um espaço de entretenimento desordenado (focado em jogos e redes sociais) em vez de um local de estudo. Portanto, a gestão do acesso não deve ser vista apenas como uma medida proibitiva, mas como uma estratégia pedagógica necessária para direcionar a atenção do aluno e otimizar o tempo de aula.

Dessa forma, a implementação de mecanismos de controle visa assegurar que a infraestrutura tecnológica da escola cumpra sua função social e educativa. Ao mitigar riscos de contato com adultos mal-intencionados ou exploração comercial, a escola cria um "cinturão de segurança" digital. Isso permite que os educadores utilizem a web como fonte de pesquisa segura, promovendo o desenvolvimento

crítico dos alunos sem expô-los às vulnerabilidades inerentes à navegação livre e sem supervisão.

2.2 TÉCNICAS DE FILTRAGEM DE CONTEÚDO

A filtragem de conteúdo é essencial para garantir o uso seguro e produtivo da internet, especialmente em ambientes educacionais. Ela consiste em bloquear o acesso a sites ou conteúdos considerados inadequados, como aqueles relacionados a violência, pornografia, discursos de ódio, redes sociais e plataformas de entretenimento que desviam a atenção dos alunos, conforme Baishya e Kakoty (2019). Essa técnica pode ser aplicada por meio de diferentes abordagens, como a análise de palavras-chave, a análise de URLs (*Uniform Resource Locator*) e a análise de pacotes, que permitem identificar e bloquear conteúdos indesejados de forma eficiente.

Segundo Baishya e Kakoty (2019), a filtragem de conteúdo pode ser implementada utilizando ferramentas como *firewalls*, *proxies* e *softwares* especializados, como o OpenDNS. Essas ferramentas atuam como barreiras que impedem o acesso a sites maliciosos ou inadequados, garantindo que os recursos tecnológicos sejam utilizados de forma alinhada aos objetivos pedagógicos. Além disso, a filtragem de conteúdo contribui para a criação de um ambiente digital mais seguro, protegendo os usuários de ameaças como *malware*, *phishing* e outros riscos associados ao uso indiscriminado da internet.

2.3 O OPENDNS COMO FERRAMENTA DE FILTRAGEM DE CONTEÚDO

De acordo com a documentação oficial do OpenDNS (2025), a ferramenta conta com uma base de dados atualizada constantemente, permitindo que as configurações de segurança sejam aplicadas de maneira dinâmica e eficiente. A administração das configurações é feita online por usuários com privilégios administrativos.

O OpenDNS oferece diferentes formas de configuração, incluindo filtros predefinidos de proteção rápida, como o *FamilyShield*, que automaticamente bloqueia *sites* considerados impróprios. Além disso, soluções mais avançadas, como *OpenDNS VIP* e *Enterprise*, permitem ajustes detalhados de filtragem, oferecendo três níveis padrões de bloqueio (baixo, moderado e alto), bem como a possibilidade

de personalização total, onde administradores podem escolher categorias específicas a serem bloqueadas.

2.4 LOGS DE ACESSO: FUNCIONAMENTO E APLICAÇÃO

Os *logs* de acesso são registros gerados por sistemas computacionais que documentam as atividades realizadas pelos usuários em um ambiente digital. Esses registros são amplamente utilizados para monitorar e analisar o comportamento dos usuários, permitindo identificar padrões de uso, detectar acessos, verificar os conteúdos inadequados presentes e avaliar a eficácia de ferramentas de controle e filtragem de conteúdo. Conforme destacado por Agosti (2012), a metodologia de análise de *logs* inclui a identificação de padrões de uso, a categorização de acessos inadequados e a comparação de dados antes e após a implementação de medidas de controle, como a ativação de filtros de conteúdo.

No contexto da pesquisa, os *logs* de acesso gerados pelo OpenDNS foram utilizados como a principal fonte de dados quantitativos para avaliar a eficácia da ferramenta no controle de acessos inadequados no laboratório de informática do CETI Professor Milton Aguiar. A análise desses logs permitiu mapear os padrões de uso inadequados, identificar os tipos de conteúdos mais acessados e comparar a redução nos acessos inadequados após a implementação dos filtros.

Além disso, a análise de *logs* de acesso deve ser realizada com atenção aos aspectos éticos, garantindo a privacidade dos usuários. Conforme Marconi e Lakatos (1999), a coleta de dados deve ser feita de forma anônima, sem a identificação individual dos usuários, e os resultados devem ser utilizados exclusivamente para fins acadêmicos e de melhoria do ambiente educacional. Essa prática é essencial para manter a confiança dos usuários e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).

2.5 OS RISCOS DA INTERNET E A IMPORTÂNCIA DA SUPERVISÃO

Conforme destacado na cartilha "*Uso de Internet por Crianças e Adolescentes: O que os Pais e Responsáveis Devem Saber?*" Dantas e Azevedo (2023), a internet, embora seja uma ferramenta poderosa para a educação, também expõe crianças e adolescentes a diversos riscos. Entre eles, destacam-se a exposição a conteúdos prejudiciais (como violência, pornografia e discursos de

ódio), o contato com adultos mal-intencionados, o *cyberbullying* e a exploração comercial. Esses riscos podem desviar a atenção dos alunos dos objetivos pedagógicos e comprometer sua segurança e bem-estar.

Existe a necessidade de supervisão e orientação por parte dos educadores e responsáveis, destacando que a tecnologia deve ser utilizada de forma consciente e responsável. Além disso, sugere medidas práticas para garantir um uso seguro da internet, como a configuração de perfis privados em redes sociais, o uso de ferramentas de controle parental e o diálogo aberto sobre os riscos online. Essas práticas não apenas protegem os alunos, mas também promovem a conscientização sobre a importância de um uso responsável da internet.

Nesse contexto de riscos e supervisão, é essencial estabelecer uma distinção clara entre a natureza das diferentes distrações no ambiente escolar. Plataformas de jogos online caracterizam-se por serem ambientes estritamente imersivos e de uso individual, que tendem a isolar o aluno e inviabilizar o acompanhamento das atividades propostas. Por outro lado, as redes sociais apresentam uma dinâmica diferente: embora sejam reconhecidas como potenciais distratores, possuem ferramentas que podem, em tese, ser mediadas e aplicadas ao contexto pedagógico. Diante dessa dualidade, a adoção de políticas de controle não deve se limitar à proibição irrestrita e generalizada. A opção por não aplicar uma filtragem severa imediata às redes sociais serve como um mecanismo para observar o comportamento dos discentes. Essa abordagem transforma a intervenção técnica em uma oportunidade prática para o desenvolvimento da 'Cidadania Digital', incentivando a reflexão e o uso ético, seguro e consciente da rede no espaço escolar.

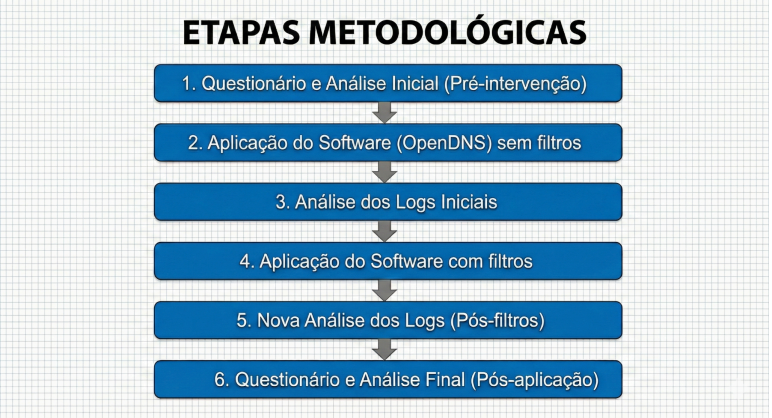
3 METODOLOGIA

A metodologia desta pesquisa é definida como uma pesquisa-ação. Conforme conceitua Thiollent (2011), essa abordagem se caracteriza por ser uma forma de investigação na qual o pesquisador tem uma participação ativa e intervém em um problema prático, buscando não apenas produzir conhecimento, mas também gerar uma transformação na situação estudada. Essa modalidade é ideal para o presente estudo, pois o pesquisador atua diretamente no Laboratório de Informática ao

implementar o OpenDNS para solucionar um problema real — o acesso a conteúdo inadequado — e, ao mesmo tempo, analisar os resultados dessa intervenção.

Quanto ao propósito, a pesquisa se classifica como exploratória na fase inicial de coleta de dados sem filtros, buscando compreender os padrões de uso da internet, e descritiva na fase posterior, ao descrever os resultados e a eficácia da ferramenta após a aplicação dos filtros. A abordagem utiliza métodos quali-quantitativos. A análise quantitativa foi realizada a partir dos dados numéricos gerados pelos logs de acesso do OpenDNS, que medem a frequência dos acessos. A análise qualitativa foi feita com base nas percepções do professor sobre as mudanças no ambiente de aprendizado, coletadas por meio de instrumentos como questionários. Por não se limitar apenas à observação, mas envolver uma intervenção direta no ambiente escolar para solucionar um problema prático, a pesquisa é classificada como uma pesquisa-ação. A imagem 1 apresenta as etapas do procedimento metodológico adotado, sintetizando o cronograma de ações para a pesquisa-ação.Por ser realizada diretamente no ambiente escolar, a pesquisa é classificada como de campo.

A imagem 1: etapas do procedimento metodológico adotado, sintetizando o cronograma de ações para a pesquisa-ação.



Fonte: Luz e Sousa (2025)

Para fundamentar a metodologia desta pesquisa, foi realizada uma revisão bibliográfica que abrangeu conceitos como a fundamentação teórica sobre métodos de pesquisa, análise de *logs* e segurança da internet, com ênfase na filtragem de conteúdo. Essa revisão utilizou métodos sistemáticos de busca, priorizando artigos científicos, teses, dissertações e documentação técnica em bases de dados como

Google acadêmico e Scielo, utilizando palavras-chave como '*OpenDNS*', 'filtragem de conteúdo', 'controle de acesso em escolas' e 'segurança na internet'.

No que se refere aos métodos de pesquisa, Marconi e Lakatos (1999) foram utilizados como referência para a elaboração do questionário, que foi aplicado ao professor responsável pelo laboratório de informática. Segundo os autores, o questionário é uma ferramenta eficaz para coletar dados, permitindo compreender a percepção dos envolvidos sobre o problema e as possíveis soluções. Além disso, os conceitos apresentados por Agosti (2012), sobre a análise de *logs* foram fundamentais para destacar uma técnica que permite identificar padrões de acesso, comportamentos dos usuários e possíveis vulnerabilidades no sistema. Essa abordagem foi essencial para avaliar a eficácia do *OpenDNS* como solução de segurança.

Para compreender os aspectos técnicos relacionados à segurança da internet e à filtragem de conteúdo, a documentação oficial do *OpenDNS* (2025) foi consultada. Esse material fornece informações detalhadas sobre o funcionamento do *software*, suas funcionalidades de bloqueio de conteúdos inadequados e a geração de *logs* de acesso, que foram analisados durante a pesquisa.

Com base nessa revisão bibliográfica, as etapas da pesquisa foram definidas da seguinte forma:

Questionário e Análise Inicial (Pré-intervenção): Foi aplicado um questionário ao professor responsável pelo laboratório para compreender o cenário antes da implementação do *OpenDNS,* identificando os desafios enfrentados no controle dos acessos indevidos.

Aplicação do Software (OpenDNS) sem filtros: O *OpenDN*S foi configurado sem restrições para monitorar os acessos dos alunos e coletar dados iniciais sobre os padrões de navegação.

Análise dos Logs Iniciais: Os registros de acesso foram analisados para identificar a frequência e os tipos de conteúdos impróprios acessados.

Aplicação do software com filtros: Com base na análise inicial dos logs, os filtros do OpenDNS foram configurados especificamente para bloquear a categoria de 'Games' (jogos online), identificada como o distrator mais crítico, preservando temporariamente as redes sociais para avaliar a precisão granular da ferramenta no contexto educacional.

Nova Análise dos Logs (Pós-filtros): Após a ativação dos filtros, os registros de acesso foram novamente analisados para verificar a efetividade dos bloqueios e a redução das tentativas de acesso.

Questionário e Análise Final (Pós-aplicação): Uma nova aplicação do questionário foi realizada com o professor para avaliar suas percepções sobre o impacto da implementação do *OpenDNS* e as mudanças no ambiente de aprendizado.

A análise detalhada de cada etapa acima será apresentada na seção de resultados, permitindo uma avaliação objetiva da eficácia do OpenDNS no controle de acessos indevidos no laboratório de informática.

Quanto ao ambiente de realização, a pesquisa foi desenvolvida diretamente no laboratório de informática do CETI Professor Milton Aguiar, local onde o problema investigado ocorreu e onde foram realizadas as etapas de coleta e análise de dados.

Para a coleta de dados, foram utilizados dois instrumentos principais: a análise dos logs de acesso gerados pelo sistema de filtragem e a aplicação de questionários ao professor responsável pelo laboratório. Os logs de acesso constituíram a principal fonte de dados quantitativos da pesquisa, pois registram as solicitações de acesso realizadas pelos dispositivos conectados à rede, permitindo identificar os tipos de sites acessados e a frequência de tentativas de acesso a conteúdos considerados inadequados no contexto educacional.

Além disso, foi aplicado um questionário ao professor responsável pelo laboratório de informática com o objetivo de obter informações qualitativas sobre o uso da internet no ambiente escolar e sobre as mudanças percebidas após a implementação do sistema de filtragem. O questionário foi aplicado em dois momentos: antes da implementação dos filtros, para identificar os desafios enfrentados no controle de acessos indevidos, e após a intervenção, para avaliar os impactos da solução adotada no cotidiano do laboratório. O instrumento continha perguntas abertas e fechadas permitindo que o professor apresentasse suas percepções e experiências de maneira mais detalhada, ao mesmo tempo em que seguia um roteiro previamente definido para orientar a coleta das informações.

3.1 PARTICIPANTES DA PESQUISA

Os participantes deste estudo abrangeram o professor responsável e os alunos de todas as turmas que utilizaram o Laboratório de Informática do CETI Professor Milton Aguiar. Em cumprimento aos preceitos éticos, o professor responsável, ciente da intervenção, assinou o Termo de Consentimento Livre e Esclarecido (TCLE).

Em relação aos alunos, o monitoramento via OpenDNS registrou apenas dados quantitativos gerais de tráfego de rede, sendo tecnicamente impossível a identificação individual dos usuários ou dos terminais específicos. Devido a essa inviabilidade de identificação e para não comprometer a validade da pesquisa (evitando que o conhecimento prévio alterasse o comportamento e as tentativas de acesso), os discentes não foram avisados previamente sobre a ativação dos filtros. Todo o monitoramento foi realizado de forma totalmente anônima, garantindo que o foco da investigação permanecesse exclusivamente na segurança institucional da infraestrutura.

4 RESULTADOS E DISCUSSÃO

Os resultados obtidos após a implementação do *software OpenDNS* no Laboratório de Informática do CETI Professor Milton Aguiar buscaram avaliar a eficácia da ferramenta no controle de acessos indevidos. A análise restringe-se aos usuários desse laboratório, considerando estritamente os conteúdos desviantes do contexto pedagógico, e mede o sucesso da intervenção com base na redução do número de requisições a esses materiais. Contudo, a avaliação não se limitou apenas aos aspectos técnicos, mas buscou também uma compreensão do impacto gerado no ambiente educacional como um todo.

Dessa forma, os dados e as discussões a seguir foram estruturados a partir de três frentes principais:

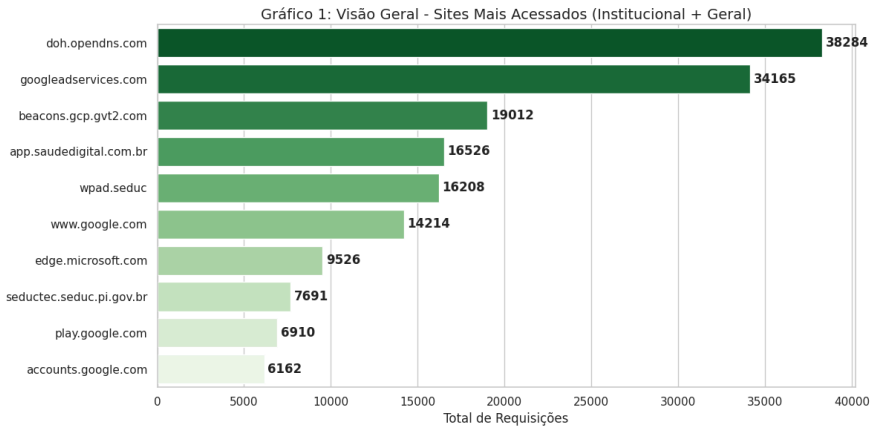
- **Logs de Acesso Pós-Filtros:** Análise quantitativa técnica evidenciada pelos registros da rede após a ativação das políticas de bloqueio.

- **Feedback do Docente:** Avaliação da percepção pedagógica, coletada por meio do questionário de pós-aplicação respondido pelo professor responsável, focando nas mudanças na gestão e no andamento das aulas.
- **Feedback e Comportamento dos Alunos:** Embora não estivesse previsto na metodologia inicial do trabalho, as reações e os relatos informais dos discentes durante e após as aulas surgiram de forma espontânea. Essa observação qualitativa não planejada tornou-se um indicador empírico valioso para compreender como a intervenção impactou diretamente a dinâmica e a postura dos estudantes no laboratório.

4.1 Mapeamento Inicial: O Perfil de Navegação e a Identificação de Acessos Indevidos

A Fase 1 (Diagnóstico) dedicou-se a registrar o tráfego da rede sem a aplicação de restrições, com o intuito de mapear o perfil real de utilização do laboratório. Como demonstra o Gráfico da imagem 2, a infraestrutura cumpria parcialmente o seu papel institucional, registrando um alto volume de acessos a domínios legítimos, como o sistema de saúde digital (`app.saudedigital.com.br` com 16.526 requisições) e sistemas internos da Secretaria de Educação (`wpad.seduc` com 16.208 requisições), além de ferramentas de pesquisa.

Imagem 2: *Visão geral dos sites mais acessados no laboratório (incluindo uso institucional) antes do bloqueio.*



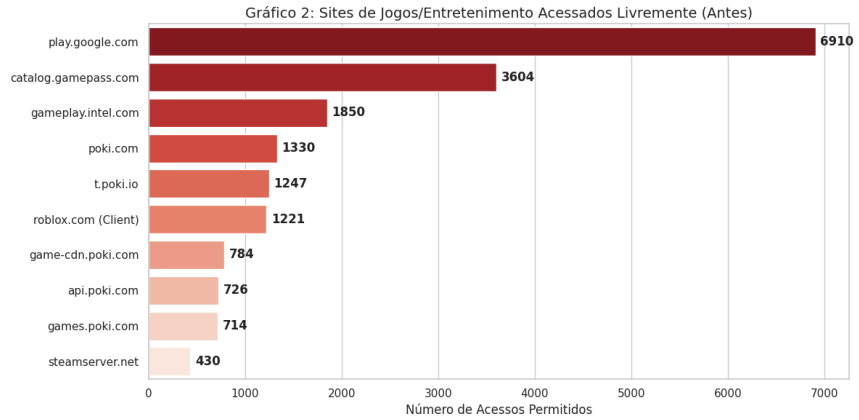
Fonte: Gráficos gerados pelo Google Forms. 2026

No entanto, misturado a esse tráfego legítimo, identificou-se um grave desvio de finalidade. No questionário pré-aplicação (20/08), o professor relatou que a

frequência de acessos indevidos ocorria “*toda aula”*, citando especificamente *"Jogos Online"* como o maior distrator.

Ao filtrar os dados apenas para as categorias de entretenimento, os logs confirmaram a percepção do docente. Conforme o gráfico da imagem 3, a loja de aplicativos *play.google.com* (6.910 acessos) e o serviço *Xbox Game Pass* (3.604 acessos) competiam diretamente pela banda da escola, evidenciando que o laboratório estava sendo subutilizado como uma "lan house" pelos alunos.

Imagem 3: *Detalhamento dos sites de jogos e entretenimento acessados livremente antes do bloqueio*



Fonte: Gráficos gerados pelo Google Forms. 2026

Para proporcionar uma compreensão mais detalhada sobre a natureza do tráfego interceptado no laboratório, o quadro da imagem 3 detalha os principais domínios indevidos registrados nos logs da rede, conforme evidenciado nos gráficos anteriores. O quadro 1 descreve a funcionalidade de cada plataforma e indica a qual categoria de filtro os domínios pertencem dentro do sistema do *OpenDNS*, justificando tecnicamente a ação de bloqueio.

Quadro 1: Domínios mais interceptados

Domínio Registrado nos Logs	**Descrição da Plataforma ou Serviço**	**Categoria de Bloqueio**
play.google.com	Loja oficial de aplicações da Google. No ambiente do laboratório, é utilizada pelos alunos para tentar descarregar jogos *mobile*, emuladores ou	*Games* (Jogos) e *Software/Technology*

	aplicações de entretenimento não educacionais.	
catalog.gamepass.com device.auth.xboxlive.com title.mgt.xboxlive.com www.xboxab.com	Domínios pertencentes ao ecossistema da Xbox e da Microsoft. São acedidos para visualização de catálogos de jogos, autenticação de contas Xbox Live e tentativas de jogar via nuvem (*Cloud Gaming*).	*Games* (Jogos)
poki.com *(e subdomínios como t.poki.io, api.poki.com, games.poki.com)*	Plataforma *online* altamente popular de *browser games* (jogos de navegador). É um dos maiores focos de distração por não exigir a instalação prévia de ficheiros, correndo diretamente no navegador *web*.	*Games* (Jogos)
roblox.com e roblox.com (Client)	Plataforma interativa de criação e exploração de jogos *online*. Consome banda significativa e exige comunicação constante com os servidores do jogo (*Client*).	*Games* (Jogos)
gameplay.intel.com	Plataforma da Intel focada em configurações, otimizações e perfis para correr jogos eletrônicos no computador.	*Games* (Jogos)
steamserver.net	Servidores de infraestrutura da Steam, a maior plataforma digital de distribuição de jogos para PC do mundo. Indica tentativas de conexão ou transferência de jogos pesados.	*Games* (Jogos)

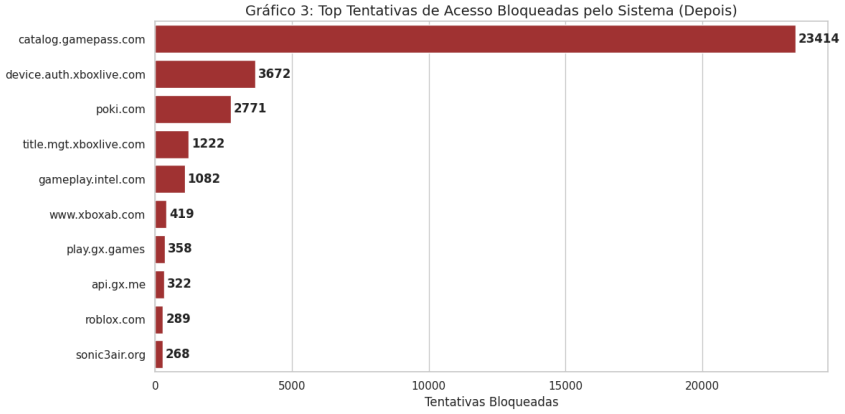
play.gx.games e api.gx.me	Domínios associados ao Opera GX, um navegador com foco em público *gamer*, contendo uma plataforma integrada de jogos *online*.	*Games* (Jogos)
sonic3air.org	*Site* específico dedicado a um jogo criado por fãs da franquia Sonic.	*Games* (Jogos)

Fonte: construído pelo autor.2026

4.2 Fase de Intervenção: A Eficácia Técnica e a Percepção de Melhora

Com a ativação dos filtros em 10 de setembro, o cenário mudou drasticamente. O OpenDNS passou a atuar ativamente, e o tráfego que antes era permitido tornou-se alvo de bloqueio. O serviço Xbox, que fluía livremente na fase anterior, registrou ***23.414 tentativas de conexão bloqueadas*** *em apenas duas semanas (Gráfico 3).*

Imagem 3:*Tentativas de acesso bloqueadas pelo sistema durante a fase de intervenção.*



Fonte: Gráficos gerados pelo Google Forms. 2026

Esses números comprovam a robustez da solução técnica: o filtro atuou cirurgicamente nos domínios de jogos (poki.com, roblox.com), preservando o acesso aos sites educacionais mostrados no Gráfico 1.

4.3 Análise das Categorias: Onde o Filtro Acertou

No que tange ao acesso às redes sociais (como Facebook e Instagram), a investigação revelou uma importante distinção entre a fundamentação teórica e a execução técnica. Embora a literatura aponte as plataformas sociais como fontes de dispersão, a configuração inicial dos filtros priorizou a categoria de Games. Esta foi uma escolha metodológica ("precisão cirúrgica") para testar a eficácia da ferramenta no distrator mais crítico relatado pelo professor, resultando na manutenção de aproximadamente 19.000 acessos permitidos ao Facebook na Fase 2.

Esta escolha metodológica não invalida a eficácia do software, mas sim demonstra sua precisão granular. O OpenDNS permite que a gestão escolar decida quais categorias interceptar sem gerar bloqueios generalizados. Dessa forma, a percepção do docente de que 'não houve mudança' no acesso às redes sociais confirma que a ferramenta operou exatamente conforme os parâmetros técnicos definidos. Para implementações futuras mais restritivas, a ferramenta permite um controle granular, como:

- **Ativação de Categorias Específicas:** A seleção explícita da categoria 'Social Networking' no painel para interceptar esses domínios.
- **Criação de Whitelists/Blacklists:** A configuração de listas de exceção, bloqueando o acesso geral, mas permitindo domínios específicos em horários determinados para fins educativos.
- **Mediação Pedagógica:** A integração do bloqueio a planos de aula sobre etiqueta digital.

4.4 Análise Comparativa: O Ambiente do Laboratório Antes e Após a Intervenção

Para avaliar a real eficácia do s*oftware OpenDNS*, procedeu-se ao cruzamento dos dados recolhidos na fase de diagnóstico (Pré-Aplicação) com os resultados obtidos após o período de bloqueio (Após-Aplicação). Esta triangulação de dados foi fundamental para compreender não apenas a eficiência técnica da ferramenta, mas sobretudo o seu impacto na dinâmica pedagógica do laboratório de informática.

A fim de ilustrar a transformação no ambiente de ensino, o Quadro 1 apresenta um paralelo entre os principais desafios relatados pelo docente por meio de formulários antes da intervenção e o cenário observado após a implementação das políticas de filtragem.

Quadro 2: Comparativo da Percepção Docente (Pré e Pós-Intervenção)

Categoria de Análise	Fase de Diagnóstico (Antes da Intervenção)	Resultados Alcançados (Depois da Intervenção)
Frequência e Perfil das Distrações	O professor relatou que os acessos indevidos ocorriam **"muito frequentemente"**, sendo a categoria de "Jogos Online" a principal fonte de dispersão.	O sistema assumiu o controle. As tentativas de acesso a categorias como jogos e conteúdo adulto foram **interceptadas automaticamente**, resultando na redução drástica do uso indevido dos computadores.
Impacto no Foco e Aprendizado	Havia a percepção clara de que os alunos **perdiam o foco** das explicações e deixavam de concluir as atividades pedagógicas devido à navegação livre.	O professor avaliou que **"o acesso aos conteúdos de aula fluiu normalmente"**. Sem os distratores, observou-se um redirecionamento forçado do foco para a conclusão das tarefas acadêmicas.
Gestão e Controle da Turma	O docente dependia de **medidas manuais de contenção** (como advertências e vigilância constante das telas), o que gerava desgaste e tomava tempo da aula.	O *software* automatizou a restrição. O professor foi liberto da função de "vigilante tecnológico", podendo dedicar **100% do seu tempo ao suporte pedagógico**.

Comportamento dos Alunos	Os alunos utilizavam a infraestrutura livremente, criando um **hábito consolidado de uso dos computadores para entretenimento** durante o horário letivo.	Houve **insatisfação e frustração** explícitas por não possuírem conhecimento técnico para burlar os bloqueios do *OpenDNS*, comprovando a eficácia e a segurança da barreira imposta.
Eficácia da Ferramenta	Havia apenas a **expectativa** (hipótese) de que uma ferramenta automática de bloqueio facilitaria o trabalho no laboratório.	A hipótese foi **confirmada**. O professor não relatou falsos positivos (bloqueios errados de sites úteis) e recomendou **"com certeza"** a manutenção definitiva do *OpenDNS*.

Fonte: construído pelo autor.2026

A análise comparativa evidencia uma mudança substancial no perfil de utilização do laboratório. O diagnóstico inicial revelava um ambiente onde a distração digital, impulsionada predominantemente por jogos online, comprometia o andamento das aulas. As medidas de contenção aplicadas manualmente pelo professor mostravam-se insuficientes para evitar a dispersão dos estudantes.

Com a implementação do *OpenDNS*, o cenário de vulnerabilidade pedagógica foi revertido. Os dados quantitativos extraídos dos logs da rede corroboram a percepção final do docente: as dezenas de milhares de tentativas de acesso a categorias de entretenimento (como catalog.gamepass.com, poki.com e roblox.com) foram interceptadas com sucesso, sem gerar falsos positivos que prejudicaram o acesso a conteúdos legítimos. A ferramenta provou ser uma solução de mediação tecnológica eficaz, confirmando a hipótese de que o bloqueio automatizado facilita o trabalho docente.

Adicionalmente, embora não estivesse previsto na metodologia inicial, o feedback direto dos alunos repassado ao professor revelou-se um indicador empírico valioso. O docente relatou que os discentes expressaram forte insatisfação com a intervenção, manifestando frustração pelo fato de não possuírem o conhecimento técnico necessário para burlar a implementação do software nos computadores do laboratório. Paradoxalmente, essa insatisfação confirmou a

robustez e a eficácia da ferramenta: sem a possibilidade de contornar as restrições para acessar as plataformas de entretenimento, observou-se um redirecionamento forçado do foco para a conclusão das atividades acadêmicas, validando o impacto positivo da solução na dinâmica de ensino.

CONSIDERAÇÕES FINAIS

O presente estudo analisou a eficácia do *software OpenDNS* como ferramenta de mediação tecnológica no Laboratório de Informática do CETI Professor Milton Aguiar. A investigação demonstrou que, antes da intervenção, a infraestrutura institucional era subutilizada como espaço de entretenimento, com plataformas de jogos e lojas de aplicativos competindo diretamente pela banda da escola. A hipótese inicial de que o bloqueio automatizado traria benefícios significativos foi confirmada tanto pelos dados técnicos quanto pela percepção docente.

Os resultados revelaram que a implementação do OpenDNS melhorou o cenário de vulnerabilidade pedagógica ao interceptar dezenas de milhares de tentativas de acesso indevido. Tecnicamente, a ferramenta mostrou-se robusta ao atuar cirurgicamente em domínios de distração sem gerar falsos positivos em sites de cunho educativo ou institucional. Pedagogicamente, a automação do bloqueio libertou o professor da função de "vigilante tecnológico", permitindo que a totalidade do tempo de aula fosse dedicada ao suporte instrucional e à conclusão das atividades acadêmicas.

A frustração manifestada pelos alunos diante da impossibilidade de burlar os filtros serviu como um indicador empírico da segurança da solução adotada. Paradoxalmente, essa resistência comprovou que, na ausência de distratores digitais, ocorre um redirecionamento forçado do foco discente para os objetivos pedagógicos.

Em face do exposto, este artigo conclui que o *OpenDNS* é uma alternativa viável, de baixo custo e alta eficiência para a gestão de redes em escolas públicas. Como recomendações para trabalhos futuros, sugere-se:

- **Manutenção Definitiva:** A institucionalização do uso do software para garantir a sustentabilidade do ambiente de aprendizado seguro.

- **Proposta de Fase 3 (Ampliação do Escopo):** A expansão do filtro para as redes sociais (ativando a categoria 'Social Networking'), avaliando se o impacto no foco das aulas seria tão drástico quanto o observado com o bloqueio dos jogos, alinhando a prática à lei do ECA digital na proteção de menores na rede.
- **Formação Continuada e Cidadania Digital:** A integração dessa ferramenta a planos de aula que promovam a cidadania digital, utilizando listas de exceção (Whitelists) para permitir o uso pedagógico das redes sociais quando necessário, transformando a restrição técnica em consciência crítica sobre o uso da internet.

REFERÊNCIAS

AGOSTI, Maristella; CRIVELLARI, Franco; DI NUNZIO, Giorgio Maria. *Web log analysis: a review of a decade of studies about information acquisition, inspection and interpretation of user interaction.* Data Mining and Knowledge Discovery, v. 24, p. 663-696, 2012.

BAISHYA, Ankur; KAKOTY, Sangeeta. *A review on web content filtering, its technique and prospects.* International Journal of Computer Science Trends and Technology (IJCST), v. 7, n. 3, p. 37-40, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 abr. 2026.

DANTAS, Juliana Evangelista. *Uso de Internet por Crianças e Adolescentes: O que os Pais e Responsáveis Devem Saber?* Campinas: Universidade Estadual de Campinas (UNICAMP), 2023.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Técnicas de pesquisa.* 6. ed. São Paulo: Atlas, 1999.

OPENDNS. *OpenDNS Knowledge Base.* Disponível em: https://support.opendns.com/hc/en-us/categories/204012807-OpenDNS-KnowledgeBase. Acesso em: 2025.

SILVA, A. B.; SANTOS, C. D. *Monitoramento de navegação na internet: uso de logs de dados para análise de comportamento online.* Revista de Tecnologia da Informação, v. 15, n. 2, p. 45-60, 2020.

THIOLLENT, Michel. *Metodologia da pesquisa-ação.* 18. ed. São Paulo: Cortez, 2011.

APÊNDICE:

Questionário 1: Avaliação (PRÉ-Aplicação) https://docs.google.com/forms/d/e/1FAIpQLScPETAh_MRfZ1xtK_C5ZQtr79-YMHoUxeZEEDXErRD07sccaw/viewform?usp=dialog

Questionário 2: Avaliação (PÓS-Aplicação) https://docs.google.com/forms/d/e/1FAIpQLScCqAvIGhrKzXOPqQqNknibGn4KRSIbSYkxq64fYuh_TF_a6g/viewform?usp=dialog