UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Jaqueline Gonçalves de Souza

Análise do uso de DNS Seguro como Estratégia de Proteção Digital

Uberlândia, Brasil

2026

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Jaqueline Gonçalves de Souza

Análise do uso de DNS Seguro como Estratégia de Proteção Digital

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, como parte dos requisitos exigidos para a obtenção título de Bacharel em Sistemas de Informação.

Orientador: Thiago Pirola Ribeiro

Universidade Federal de Uberlândia – UFU

Faculdade de Computação

Bacharelado em Sistemas de Informação

Uberlândia, Brasil

2026

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Computação
Av. João Naves de Ávila, 2121, Bloco 1B - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4393 - www.facom.ufu.br - facom@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Sistemas de Informação				
Defesa de:	FACOM31802 - Trabalho de Conclusão de Curso II				
Data:	24/03/2026	Hora de início:	19:00	Hora de encerramento:	20:25
Matrícula do Discente:	12211BSI249				
Nome do Discente:	Jaqueline Gonçalves de Souza				
Título do Trabalho:	Análise do uso de DNS Seguro como Estratégia de Proteção Digital				

A carga horária curricular foi cumprida integralmente?	(X) Sim ( ) Não

Reuniu-se na Sala Virtual, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Sistemas de Informação, assim composta: Prof. Dr. Diego Nunes Molinos; Prof. Dr. Marcelo Zanchetta do Nascimento; Prof. Dr. Thiago Pirola Ribeiro orientador da candidata.

Iniciando os trabalhos, o presidente da mesa, Dr. Thiago Pirola Ribeiro, apresentou a Comissão Examinadora e a candidata, agradeceu a presença do público, e concedeu à discente a palavra, para a exposição do seu trabalho. A duração da apresentação da discente e o tempo de arguição e resposta foram conforme as normas do curso.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir a candidata. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando a candidata:

(X) Aprovada Nota [90]

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Marcelo Zanchetta do Nascimento**, **Professor(a) do Magistério Superior**, em 24/03/2026, às 20:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Diego Nunes Molinos**, **Professor(a) do Magistério Superior**, em 24/03/2026, às 20:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Thiago Pirola Ribeiro**, **Professor(a) do Magistério Superior**, em 24/03/2026, às 20:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7155140** e o código CRC **BAF780D7**.

Agradecimentos

Agradeço ao Senhor Deus por me abençoar durante toda a minha trajetória, concedendo-me força e coragem em todos os momentos.

Aos meus pais, Marta e Admilson, e ao meu irmão, Matheus, que me apoiaram incondicionalmente ao longo de toda essa caminhada. Sou profundamente grata pelo amor, pela confiança, pelos conselhos e pelo incentivo constante aos meus estudos, que foram fundamentais para que eu chegasse até aqui.

Às minhas tias Maria Ivonilda e Maria Alzira, que estiveram comigo durante todo o meu percurso de estudos, oferecendo apoio e carinho. A convivência e as experiências compartilhadas com elas foram fundamentais para despertar em mim a motivação e a inspiração que deram origem à escolha e ao desenvolvimento deste trabalho.

Por fim, agradeço ao professor Thiago, que se dispôs a me orientar e compartilhar seus conhecimentos durante minha trajetória no mundo das Redes.

“Eu via sempre o Senhor comigo, porque Ele está ao meu lado direito, para que nada me abale.”

(Atos 2:25)

Resumo

Este trabalho analisa o uso de serviços de DNS com filtragem como estratégia de proteção digital para usuários com baixa familiaridade tecnológica. Foram avaliados provedores que oferecem mecanismos de bloqueio de domínios maliciosos, considerando critérios como segurança, aplicabilidade, disponibilidade e documentação. Como etapa prática, foi realizado um teste automatizado por meio de um script Bash em ambiente WSL Linux, utilizando amostras de domínios das listas CERT.pl e URLhaus. Nos resultados, observou-se desempenho elevado e homogêneo entre os provedores para os domínios do CERT.pl, com taxas superiores a 95% de bloqueio. Por outro lado, para os domínios do URLhaus, houve maior variação, com destaque para o Quad9, que apresentou taxa significativamente superior em relação aos demais. Os resultados indicam que serviços de DNS com filtragem podem atuar como uma camada adicional de proteção, embora sua eficácia varie conforme a fonte dos domínios maliciosos.

Palavras-chave: DNS Seguro, Proteção digital para usuários com baixa familiaridade tecnológica, Resolvedores.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

CERTs	*Computer Emergency Response Teams*
CSV	*Comma-Separated Values*
DNS	Sistema de Nomes de Domínio
DNSSEC	*Domain Name System Security Extensions*
DoH	*DNS over HTTPS*
DoQ	*DNS over QUIC*
DoT	*DNS over TLS*
FUSD	*Fresno Unified School District*
HTTPS	*Hypertext Transfer Protocol*
IP	*Internet Protocol*
MDHC	Ministério dos Direitos Humanos e da Cidadania
ODoH	*Oblivious DNS over HTTPS*
SNDPI	Secretaria Nacional dos Direitos da Pessoa Idosa
TLS	*Transport Layer Security*
UnB	Universidade de Brasília
WSL	*Windows Subsystem for Linux*

Sumário

1 Introdução

Com a crescente digitalização da sociedade, notícias relacionadas ao entretenimento, saúde, política e demais temas sociais são publicadas de forma contínua e dinâmica em mídias digitais, especialmente por meio de redes sociais, portais de notícias e aplicativos de mensagens. Impulsionadas por essas ferramentas, pessoas de diferentes perfis demonstram crescente interesse em se manter informadas sobre os acontecimentos ao redor do mundo. Entre esses usuários, destacam-se aqueles com pouca experiência ou conhecimento em tecnologias digitais, o que pode dificultar a identificação de riscos no ambiente online, como ocorre com diferentes grupos, incluindo idosos e crianças.

Esse comportamento é evidenciado pelo aumento significativo do uso da Internet, conforme apontam dados que indicam a ampliação do acesso a dispositivos conectados e da frequência de navegação online, inclusive entre pessoas com 60 anos ou mais (IBGE, 2023). No entanto, essa maior inserção digital também expõe esses usuários a riscos associados à navegação desprotegida, como o contato com conteúdos maliciosos, *hiperlinks* fraudulentos, golpes financeiros, notícias falsas e outras formas de manipulação virtual. Diante desse cenário, torna-se essencial a adoção de mecanismos eficazes de proteção digital, que auxiliem na prevenção de ameaças virtuais e na promoção de um ambiente mais seguro para o uso da Internet por usuários leigos.

Com base nessa perspectiva, mecanismos como o Sistema de Nomes de Domínio (*Domain Name System* (DNS)) podem ser utilizados como uma camada adicional de segurança na navegação, ao permitir o bloqueio de acessos a domínios maliciosos por meio de filtros configuráveis (FORTINET, 2026b). Essa abordagem pode ser adotada por meio de serviços que já oferecem esse tipo de proteção de forma integrada ou por meio de configurações realizadas pelo usuário ou administrador da rede.

Nesse contexto, a notícia (FEBRABAN, 2024) indica que um dos golpes mais comuns envolve a falsa venda online, na qual criminosos criam páginas que simulam e-commerces legítimos e divulgam ofertas enganosas por meio de mensagens contendo *hiperlinks* que redirecionam os usuários a websites maliciosos. Esse tipo de ataque afeta especialmente usuários com conhecimento limitado em tecnologias digitais, que podem apresentar maior dificuldade em avaliar a confiabilidade desses endereços. Assim, a configuração de um serviço de DNS com filtros de segurança na rede doméstica pode reduzir significativamente a exposição a esses riscos, limitando o acesso a domínios maliciosos, tanto já conhecidos quanto recentemente identificados, e diminuindo a necessidade de reconhecimento manual de ameaças digitais.

A análise realizada pela Alliance (2021) ressalta que a segurança em camada DNS

atua na prevenção de ciberataques ao bloquear conexões com domínios maliciosos nas etapas iniciais do processo de comunicação, visto que o DNS constitui o primeiro passo no estabelecimento de conexões na Internet. De forma complementar, estudos aprofundam essa perspectiva ao investigar o uso de filtros baseados em zonas de política de resposta e na detecção automatizada de domínios suspeitos (MAGNUSSON, 2024), bem como ao apresentar abordagens para a identificação de domínios maliciosos com base na análise de dados de consultas DNS (ZHAUNIAROVICH et al., 2018).

1.1 Objetivo geral

O objetivo deste trabalho é investigar o uso do DNS seguro como estratégia de proteção digital para usuários com baixa familiaridade tecnológica. Nesse contexto, são examinados os principais serviços com filtros de segurança disponíveis no mercado, como Cloudflare DNS, CleanBrowsing, AdGuard e Quad9, com base nos critérios de segurança, aplicabilidade, disponibilidade e documentação, considerando também sua relevância para públicos com menor familiaridade tecnológica.

1.1.1 Objetivos específicos

- Descrever os resolvedores de DNS analisados, abordando seu funcionamento e os mecanismos utilizados para filtragem de ameaças.
- Avaliar o comportamento desses serviços frente a listas de domínios maliciosos provenientes das fontes: URLhaus e CERT.pl.
- Comparar os resultados obtidos entre os diferentes resolvedores DNS analisados.
- Analisar o potencial dessas soluções como mecanismo de proteção digital para usuários leigos.

1.2 Justificativa

A motivação para o desenvolvimento deste trabalho surgiu a partir da convivência da autora com pessoas da terceira idade, observando com frequência situações em que esse público é alvo de golpes virtuais ou acessa páginas maliciosas sem perceber os riscos envolvidos. Esse cenário reflete o crescimento dessas ameaças no ambiente digital, que atingem usuários de diferentes faixas etárias (ERLICH, 2025).

Diante dessa realidade, torna-se relevante investigar soluções tecnológicas que possam contribuir para aumentar a segurança desse público durante o uso da internet. Entre

as alternativas possíveis, destacam-se os serviços de DNS com filtragem de conteúdo e bloqueio de domínios maliciosos, que podem atuar como uma camada adicional de proteção ao impedir o acesso a sites potencialmente perigosos.

1.3 Organização do trabalho

A estrutura deste trabalho está organizada nos capítulos descritos a seguir:

- **Capítulo 2**: apresenta a fundamentação teórica, abordando os conceitos relacionados ao DNS, ao DNS seguro, à filtragem de conteúdo por meio de serviços de DNS e à proteção digital voltada a usuários com menor familiaridade tecnológica.
- **Capítulo 3**: apresenta os trabalhos relacionados à temática do estudo, destacando pesquisas e abordagens relevantes existentes na literatura, que servem de apoio à análise realizada neste trabalho.
- **Capítulo 4**: descreve a metodologia utilizada no desenvolvimento do estudo, incluindo a abordagem adotada, os critérios de seleção dos resolvedores DNS, a utilização e adaptação do script utilizado e os procedimentos de execução dos testes.
- **Capítulo 5**: apresenta os resultados obtidos a partir da análise dos dados coletados, comparando o desempenho dos resolvedores DNS frente às bases de domínios maliciosos utilizadas.
- **Capítulo 6**: apresenta a conclusão do trabalho, destacando os principais resultados alcançados, as contribuições do estudo e possíveis trabalhos futuros.

2 Fundamentação Teórica

Este capítulo apresenta os fundamentos teóricos que sustentam este trabalho, abordando o Sistema de Nomes de Domínio e seus mecanismos de segurança, a filtragem de conteúdo por meio de serviços de DNS e aspectos relacionados à proteção de usuários com reduzido conhecimento em tecnologias digitais.

2.1 DNS

O Sistema de Nomes de Domínio é um dos componentes fundamentais da Internet, responsável por permitir que usuários acessem serviços online por meio de nomes de fácil compreensão, em vez de endereços numéricos (IBM, 2026). Na prática, o DNS atua como um mecanismo de tradução, convertendo nomes de domínio, como www.exemplo.com, em endereços IP que identificam os servidores na rede.

Para viabilizar esse processo, o DNS utiliza uma arquitetura composta por diferentes tipos de servidores que atuam de forma hierárquica. Quando uma consulta é realizada, ela é inicialmente direcionada a um resolvedor DNS recursivo, responsável por intermediar a requisição e buscar a resposta apropriada. Caso a informação não esteja disponível em cache, o resolvedor realiza consultas sequenciais a outros servidores do sistema, incluindo os servidores raiz, os servidores de domínio de topo e, por fim, os servidores autoritativos. Estes últimos armazenam os registros oficiais dos domínios e fornecem as respostas definitivas às consultas. Essa organização distribuída permite que o DNS opere de forma escalável e eficiente, atendendo a um grande volume de requisições (SERVICES, 2026).

Nesse contexto, o processo de resolução de nomes ocorre de forma transparente para o usuário. Ao acessar um endereço na Internet, o dispositivo envia uma solicitação ao resolvedor DNS, que inicialmente verifica a existência de uma resposta armazenada em cache. Caso contrário, inicia-se uma sequência de consultas na hierarquia do DNS até que o endereço IP correspondente ao domínio solicitado seja localizado. A partir dessa informação, torna-se possível estabelecer a conexão com o servidor de destino e acessar o conteúdo desejado. Esse mecanismo permite que os usuários naveguem utilizando nomes de domínio, sem a necessidade de memorizar endereços IP (FORTINET, 2026a).

Além de sua função essencial na resolução de nomes, o DNS também exerce influência direta no desempenho das aplicações. Isso ocorre porque mecanismos de cache permitem o armazenamento temporário de respostas previamente obtidas, reduzindo a necessidade de novas consultas à hierarquia de servidores (AKAMAI, 2026). Como consequência, há diminuição no tempo de resposta e melhoria na eficiência do acesso aos

serviços.

2.2 DNS Seguro

O DNS não foi originalmente projetado com foco em segurança, de modo que suas limitações de design, aliadas aos avanços tecnológicos, o tornam vulnerável a um amplo espectro de ataques (CLOUDFLARE, 2026b). Em 2008, Dan Kaminsky demonstrou uma falha crítica no sistema que permitia a injeção de informações falsas nos caches de servidores DNS (SIDN, 2026). Esse cenário mobilizou a comunidade técnica e órgãos de padronização a desenvolver soluções voltadas à proteção e privacidade.

Diversas tecnologias foram então propostas para fortalecer a infraestrutura do DNS. Entre elas, destaca-se o DNSSEC (*Domain Name System Security Extensions*), que utiliza assinaturas digitais criptografadas para validar a integridade e as respostas do DNS (PRESTON, 2026). Outra solução é o DNS sobre TLS (DoT), que criptografa consultas e respostas DNS para proteger a privacidade do usuário, operando na porta 853 [1] (DNS.SB, 2026). De modo semelhante, o DNS sobre HTTPS (DoH) encapsula as consultas DNS dentro do tráfego HTTPS, dificultando sua identificação e interceptação (CLOUDFLARE, 2025).

Além dessas abordagens já consolidadas, pesquisas recentes têm buscado aprimorar ainda mais a privacidade e o desempenho do DNS. O *Oblivious DNS over HTTPS* (ODoH) impede que um único servidor tenha acesso simultâneo à identidade do solicitante e ao conteúdo da consulta, utilizando um modelo de proxy com criptografia avançada (SINGANAMALLA et al., 2020). Já o *DNS over QUIC* (DoQ) explora os benefícios do protocolo de transporte QUIC, oferecendo menor latência e conexões mais ágeis (KOSEK et al., 2023).

A adoção de protocolos de DNS seguro já pode ser observada em soluções práticas disponíveis ao usuário final. Fabricantes como a TP-Link incorporaram suporte a DoH e DoT em roteadores domésticos da linha Archer, permitindo que a resolução de nomes seja feita de forma criptografada diretamente pela interface de administração (COMMUNITY, 2023). De modo semelhante, navegadores como o Mozilla Firefox possibilitam a ativação do DoH em suas configurações (SUPPORT, 2025), ampliando a proteção da navegação contra monitoramento por terceiros.

[1] Uma porta é um identificador numérico utilizado para direcionar a comunicação a serviços, a porta 853 é a porta padrão do protocolo DNS sobre TLS utilizada para a transmissão segura de consultas DNS por meio de criptografia.

2.3 Filtragem de conteúdo via serviço de DNS

A filtragem de domínio por meio de serviços de DNS é uma estratégia de segurança que controla o acesso a domínios da Internet com base em políticas pré-estabelecidas. O mecanismo atua no momento da consulta DNS, aplicando regras que impedem ou permitem a resolução de nomes considerados inadequados ou fora do escopo permitido (CLOUDFLARE, 2026a). Para isso, os serviços de nomes de domínio utilizam conjuntos de domínios organizados, geralmente estruturados em listas de bloqueio ou de permissão. As listas de bloqueio incluem domínios já reconhecidos por hospedar *phishing*, *malware*, conteúdo adulto, jogos de azar e outras categorias nocivas, sendo mantidas atualizadas conforme novas ameaças emergem (LUMIUN, 2026). Já as listas de permissão permitem apenas a resolução de domínios previamente autorizados (SECURITY, 2024).

Com o crescimento da Internet e o aumento das ameaças digitais, surgiram serviços de DNS que incorporaram políticas de segurança diretamente na infraestrutura (DN.ORG, 2024). Um dos pioneiros nesse modelo foi o OpenDNS, lançado em 2006, que já em 2007 passou a oferecer recursos de filtragem de conteúdo personalizada (*custom content filtering*), permitindo aos usuários configurar o bloqueio de determinadas categorias de sites OpenDNS (2025).

Desse modo, a filtragem de conteúdo evoluiu significativamente, incorporando mecanismos adaptáveis e baseados em inteligência artificial. Serviços modernos utilizam algoritmos de *machine learning* para classificar domínios, permitindo detectar padrões maliciosos mesmo quando os domínios não estão presentes em uma lista de bloqueio (DNSFILTER, 2025). Além disso, esses serviços passaram a empregar gerenciamento de tráfego baseado em políticas personalizadas, podendo responder de forma diferente a uma mesma solicitação conforme critérios como localização geográfica, tornando a filtragem mais precisa e contextualizada (TECHNOLOGIES, 2026).

Exemplos práticos da adoção de DNS seguro com filtragem incluem o Quad9, que bloqueia automaticamente domínios associados a atividades maliciosas a partir de fontes atualizadas (FOUNDATION, 2026). O funcionamento básico desse tipo de solução pode ser observado na Figura 1.

Em ambientes escolares, o *Fresno Unified School District* (FUSD) utiliza o DNSFilter para proteger cerca de 35 mil dispositivos estudantis, bloqueando em média mais de 700 mil domínios maliciosos por mês e restringindo o acesso a conteúdos inadequados (RAYMOND, 2021). Esses casos demonstram a eficácia e aplicabilidade da filtragem de domínio via DNS em diferentes contextos.

Figura 1 – Filtragem das requisições através do servidor de DNS seguro.

Fonte: Da Autora com o uso da IA.

2.4 Proteção digital para usuários com pouca familiaridade tecnológica

Com a ampliação do uso da Internet em atividades cotidianas, a segurança no ambiente digital tornou-se uma preocupação relevante para diferentes grupos da população. Embora pessoas idosas frequentemente sejam apontadas como mais vulneráveis, estudos e reportagens recentes indicam que golpes virtuais não fazem distinção de idade, afetando também adolescentes, adultos e idosos (SENADO, 2025). Diante desse cenário, torna-se necessário adotar medidas que promovam o uso seguro da Internet, envolvendo tanto o emprego de tecnologias quanto ações de educação digital (VEJA.ORG, 2025). Nesse sentido, observa-se o desenvolvimento de diferentes iniciativas voltadas à mitigação desses riscos.

No âmbito tecnológico, observa-se o desenvolvimento de soluções voltadas a tornar a experiência digital mais acessível e segura para usuários com pouca familiaridade tecnológica. Nesse contexto, o design de interfaces passou a incorporar práticas mais inclusivas, como contrastes elevados, fontes ampliadas, linguagem clara e navegação simplificada, que contribuem para reduzir dificuldades de uso e facilitar a compreensão das informações apresentadas (CHUNG, 2024). Tais adaptações auxiliam os usuários na identificação de elementos relevantes da interface e na tomada de decisões mais seguras durante a navegação.

Ademais, destaca-se o surgimento de aplicações como Be My Eyes (2026), voltadas especialmente a usuários com baixa visão ou pouca experiência digital. Essas ferramentas oferecem suporte direto na utilização de dispositivos e serviços online, seja por meio de chamadas de vídeo com voluntários, seja com o auxílio de inteligência artificial, permitindo orientar os usuários em situações que envolvem possíveis riscos, como a verificação de conteúdos suspeitos ou a realização de ações sensíveis.

No campo educacional, destacam-se iniciativas como o Projeto Viva Mais Cidadania Digital, lançado no campus da Universidade de Brasília (UnB), fruto de parceria entre a Secretaria Nacional dos Direitos da Pessoa Idosa (SNDPI) e o Ministério dos Direitos Humanos e da Cidadania (MDHC). O programa busca capacitar pessoas idosas para a prevenção de golpes em ambientes virtuais, por meio de encontros presenciais e materiais educativos (CIDADANIA, 2025).

Como complemento, no contexto de soluções tecnológicas, destacam-se os serviços de DNS com filtragem de conteúdo, que atuam como uma camada adicional de proteção ao bloquear automaticamente o acesso a domínios maliciosos ou inadequados. Um exemplo é o serviço *Cloudflare 1.1.1.1 for Families*, que permite configurar a rede para restringir o acesso a páginas com *malware* ou conteúdo impróprio, contribuindo para uma navegação mais segura, especialmente em ambientes domésticos (CLOUDFLARE, 2020).

3 Trabalhos relacionados

Esta seção apresenta trabalhos relacionados que contribuíram como base para este estudo, oferecendo direcionamento quanto às metodologias e abordagens utilizadas na análise de resolvedores DNS.

3.1 Análise de resolvedores DNS públicos na literatura

A pesquisa de Silva et al. (2023) apresenta uma análise sobre resolvedores de DNS públicos, reunindo e sistematizando os principais estudos acadêmicos publicados entre 2019 e 2023, a partir de buscas em bases, como ACM Digital Library, IEEE Xplore e Google Scholar. O estudo discute métricas e metodologias aplicadas na avaliação desses resolvedores e evidencia tendências relacionadas ao desempenho e resiliência de provedores amplamente utilizados.

A contribuição desse trabalho para a presente pesquisa é fornecer uma visão consolidada que auxilia na compreensão dos critérios adotados em avaliações anteriores, servindo de base para identificar mecanismos relevantes de desempenho e segurança.

3.2 Avaliação de desempenho de resolvedores DNS com a ferramenta PerfResolv

O trabalho de Silva et al. (2024) apresenta a ferramenta PerfResolv, desenvolvida para avaliar o desempenho de resolvedores DNS públicos selecionados, sendo eles: Google, Cloudflare, OpenDNS, Quad9 e ComodoDNS. Além de mensurar tempos de resposta, o estudo contribui ao evidenciar como variáveis, como a geolocalização dos usuários, a popularidade dos domínios consultados, influenciam no desempenho percebido.

Essa abordagem se conecta diretamente à presente pesquisa, pois fornece informações sobre o comportamento dos resolvedores em diferentes condições, contribuindo para decisões mais informadas na escolha de cada um deles.

3.3 Eficácia de serviços DNS no controle de conteúdo e segurança

A investigação de Liberato et al. (2025), por sua vez, analisou a eficácia de sistemas de controle parental em diferentes plataformas, incluindo roteadores, serviços de DNS e softwares especializados. A metodologia envolveu testes práticos com listas de domínios categorizados, medindo taxas de bloqueio e identificando falhas. Os resultados indicaram

que serviços de DNS, OpenDNS e DNS0.eu, tiveram bom desempenho no bloqueio de conteúdos inadequados.

Essa análise se conecta diretamente a este trabalho porque evidencia que mecanismos de filtragem via DNS podem ser aproveitados para oferecer uma boa camada de segurança online.

As principais características dos trabalhos relacionados discutidos nesta seção são sintetizadas na Tabela 1. Nela são apresentados os objetivos, metodologias empregadas, resolvedores de DNS analisados e os principais resultados obtidos por cada estudo, incluindo também o presente trabalho, permitindo uma visão comparativa das abordagens utilizadas na literatura.

Tabela 1 – Comparação das principais características dos trabalhos relacionados

Trabalho	**Objetivo**	**Metodologia**	**Resolvedores analisados**	**Resultados**
Silva et al. (2023)	Analisar trabalhos sobre resolvedores de DNS públicos, sistematizando métricas e metodologias	Revisão e consolidação de estudos anteriores	Resolvedores de DNS públicos	Visão consolidada das métricas de avaliação, destacando desempenho e cenários
Silva et al. (2024)	Avaliar desempenho de resolvedores DNS públicos através da ferramenta PerfResolv	Testes de tempos de resposta considerando variáveis, como popularidade de domínios	Google, Cloudflare, OpenDNS, Quad9, ComodoDNS	Evidenciou influência de fatores contextuais no desempenho percebido; útil para escolha de provedores em cenários diferentes
Liberato et al. (2025)	Investigar eficácia de sistemas de controle parental em diferentes plataformas	Testes práticos com listas de domínios categorizados, medindo taxas de bloqueio	OpenDNS, DNS0.eu	Serviços de DNS mostraram bom desempenho no bloqueio de conteúdos inadequados
Este trabalho	Avaliar o uso de DNS com filtragem de segurança como mecanismo de proteção digital para usuários com baixa familiaridade tecnológica	Teste automatizado com script em ambiente WSL, utilizando 300 domínios da lista CERT.pl e 300 domínios da URLhaus	Cloudflare DNS, CleanBrowsing, AdGuard e Quad9	Os resolvedores apresentaram diferentes taxas de bloqueio, com destaque para maior eficácia em listas com maior concentração de ameaças conhecidas

4 Desenvolvimento

Para o desenvolvimento deste trabalho, buscou-se analisar o uso de resolvedores de DNS seguro como estratégia de proteção digital, com foco na aplicabilidade para usuários com menor domínio de tecnologias digitais. Para atingir esse objetivo, a pesquisa adota uma abordagem baseada na execução de um teste prático de resolução de domínio malicioso.

4.1 Metodologia

Como base metodológica, foi utilizado o script em bash disponibilizado no artigo de (LOWET, 2025), publicado no blog técnico da Nexxwave em setembro de 2024. Esse script foi empregado como referência para a execução dos testes, mantendo-se a mesma lógica experimental, porém com a substituição e adaptação de alguns pontos do código, sendo um deles, os resolvedores de DNS analisados neste trabalho: Cloudflare DNS, CleanBrowsing, AdGuard e Quad9.

A seguir, são descritos os tópicos que integram cada etapa do estudo:

- Etapa 1 - Definição dos critérios dos resolvedores
- Etapa 2 - Descrição dos resolvedores selecionados
- Etapa 3 - Estruturação e adaptações do script
- Etapa 4 - Procedimentos de execução dos testes
- Etapa 5 - Coleta e organização dos dados
- Etapa 6 - Visualização dos resultados

4.1.1 Etapa 1 - Definição dos critérios dos resolvedores

A seleção dos resolvedores de DNS utilizados neste estudo foi orientada por critérios técnicos específicos, com o objetivo de analisar a eficácia na mitigação de ameaças, especialmente no contexto de proteção de usuários com pouco conhecimento tecnológico contra conteúdos maliciosos e interceptação de dados.

Os critérios estabelecidos foram definidos a partir de subcritérios objetivos, visando garantir maior consistência e comparabilidade entre os serviços analisados:

- **Segurança**: avaliada com base na origem e diversidade das fontes de inteligência de ameaças, frequência de atualização das listas de bloqueio e suporte a protocolos seguros de resolução DNS, como DoH e DoT, visando prevenir interceptação, espionagem ou manipulação das consultas DNS;
- **Aplicabilidade**: considerada a facilidade de configuração do serviço, analisando a simplicidade do processo de instalação e a necessidade de conhecimento técnico;
- **Disponibilidade**: analisou-se a utilização da arquitetura *anycast*, técnica de endereçamento e roteamento na qual múltiplos servidores compartilham o mesmo endereço IP, direcionando a consulta do usuário ao nó da rede geograficamente mais próximo ou com menor latência;
- **Documentação**: avaliada quanto à clareza, organização e acessibilidade das instruções fornecidas ao usuário final.

Foram escolhidos os seguintes resolvedores para essa análise: Cloudflare DNS, CleanBrowsing, AdGuard e Quad9.

4.1.2 Etapa 2 - Descrição dos resolvedores selecionados

4.1.2.1 Cloudflare

O Cloudflare foi selecionado devido à sua infraestrutura global distribuída e elevada disponibilidade, características que garantem estabilidade e confiabilidade no serviço. O resolvedor padrão 1.1.1.1 é voltado para desempenho e privacidade, e a empresa também disponibiliza variantes com filtragem de segurança, como o 1.1.1.2, destinado ao bloqueio de malware e conteúdos potencialmente indesejados.

Além disso, o Cloudflare DNS utiliza inteligência de ameaças baseada em sua própria infraestrutura global, com coleta e análise contínua de dados em larga escala, apoiada por iniciativas como o Cloudflare Radar.

O resolvedor também oferece suporte a tecnologias modernas de segurança e privacidade, como DNSSEC, DoH e DoT, contribuindo para a proteção contra interceptação e manipulação de consultas DNS.

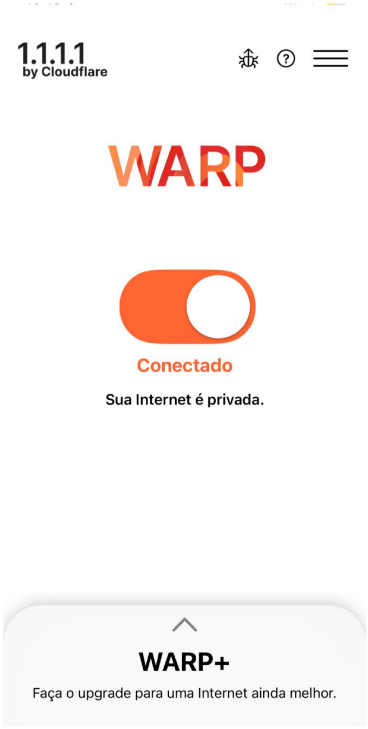
A configuração pode ser realizada diretamente no roteador ou no sistema operacional, sem necessidade de cadastro. Alternativamente, é possível configurar via aplicativo oficial do Cloudflare, ativando o recurso WARP e realizando as definições na seção de configuração avançada, dentro das opções de conexão em configurações de DNS, como ilustrado nas Figuras 3 e 4. Embora o processo seja relativamente simples, pode exigir conhecimento básico por parte do usuário. Ainda assim, a documentação técnica é clara,

bem estruturada e acessível, facilitando a adoção por diferentes perfis de usuários, como se pode observar na Figura 2.

Figura 2 – Instruções via website do Cloudflare DNS.

Fonte: Cloudflare (2026c).

Figura 3 – Aplicativo do Cloudflare DNS.



Fonte: Da Autora.

Figura 4 – Página de configuração via aplicativo do Cloudflare DNS.

Fonte: Da Autora.

.

4.1.2.2 CleanBrowsing

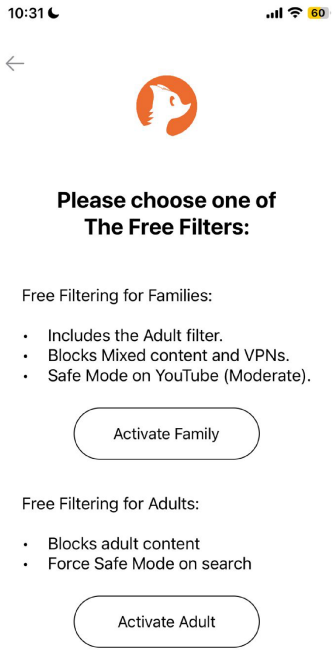
O CleanBrowsing destaca-se por oferecer diferentes perfis de filtragem, como segurança, familiar e adulto, permitindo maior controle sobre o tipo de conteúdo bloqueado. O serviço disponibiliza opções gratuitas acessíveis por meio de aplicativo próprio, como os modos *Free Filtering for Families* e *Free Filtering for Adults*, que podem ser utilizados sem necessidade de cadastro.

No que se refere às listas de bloqueio, o CleanBrowsing utiliza uma combinação de bases próprias e fontes externas, com curadoria voltada tanto à segurança quanto ao controle de conteúdo. As atualizações são realizadas continuamente. O serviço também oferece suporte a protocolos seguros como DoH e DoT, contribuindo para a proteção das consultas DNS contra interceptação.

A configuração pode ser realizada tanto por aplicativo quanto manualmente, por meio da alteração dos servidores DNS em dispositivos ou roteadores, como se pode notar nas Figuras 5 e 6. Essa flexibilidade torna o serviço altamente acessível, inclusive para usuários com pouca familiaridade técnica.

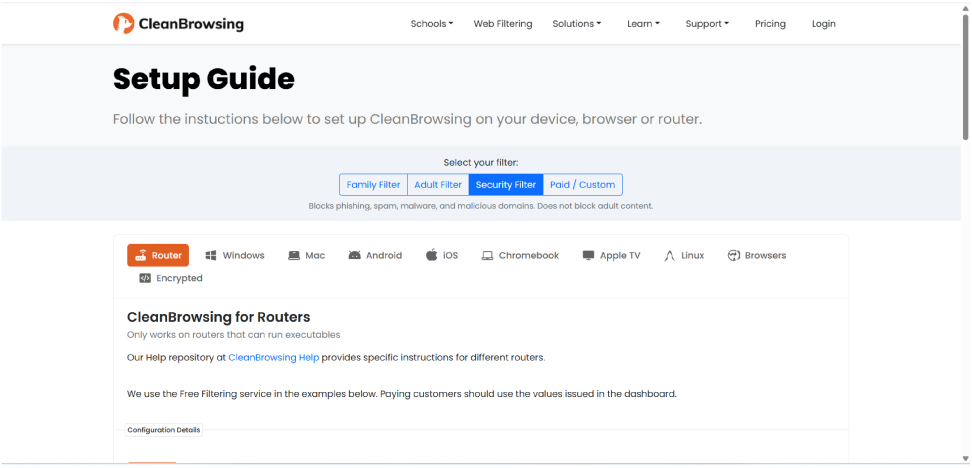
A infraestrutura utiliza arquitetura *anycast* com presença global, contribuindo para uma operação estável e consistente do serviço. A documentação é abrangente, com guias claros, objetivos e orientados ao usuário final, facilitando a implementação em diferentes ambientes.

Figura 5 – Aplicativo do CleanBrowsing.



Fonte: Da Autora.

Figura 6 – Instruções via website do CleanBrowsing.



Fonte: CleanBrowsing (2025).

4.1.2.3 AdGuard

O AdGuard DNS foi selecionado por sua abordagem voltada à filtragem de domínio indesejado e proteção contra ameaças online. O serviço possui versões gratuita e paga, sendo a versão paga voltada a recursos adicionais e maior nível de personalização.

O serviço baseia suas listas de bloqueio em bases mantidas pela própria AdGuard,

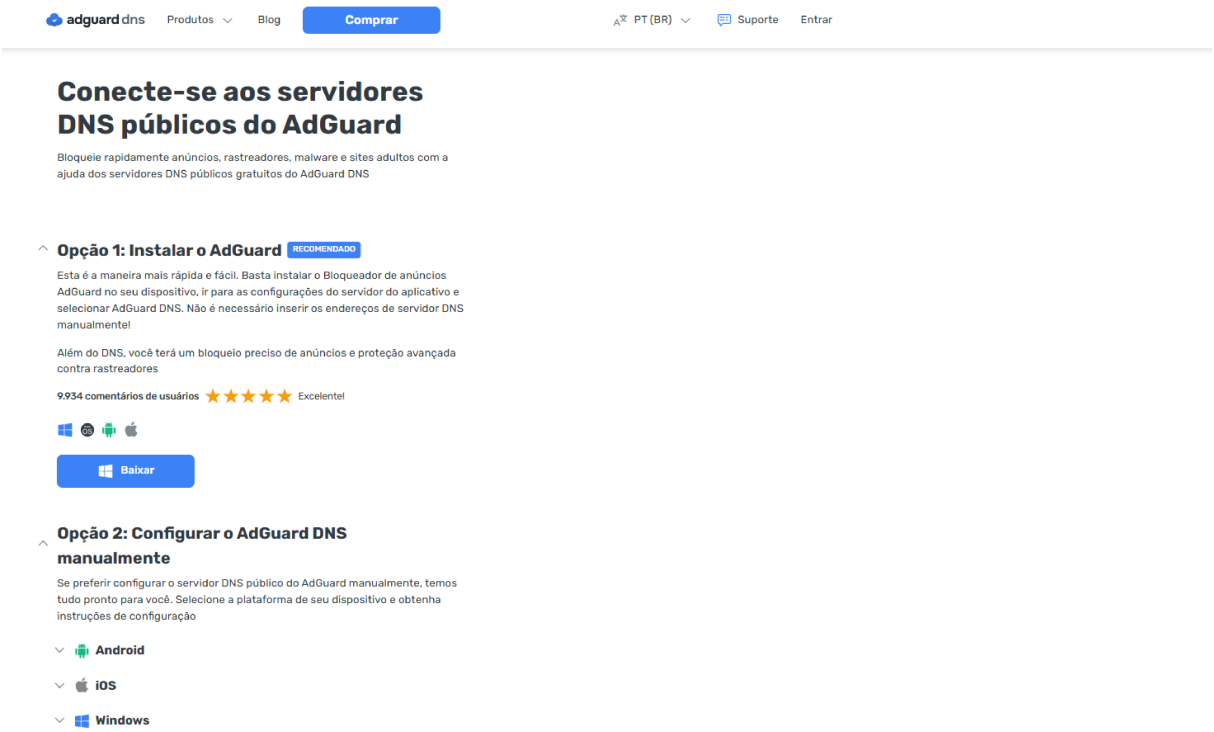
permitindo ainda a personalização por meio da inserção manual de domínios em listas de bloqueio ou de permissão (*blocklist*/*allowlist*). Essas listas são organizadas por categorias e consolidadas em bases aplicadas ao resolvedor, sendo atualizadas continuamente por meio de mecanismos de monitoramento. Esse processo possibilita adaptação constante a novas ameaças.

O AdGuard DNS também oferece suporte a diferentes protocolos de segurança, DoH, DoT e DoQ, ampliando a proteção das consultas DNS contra interceptação.

A configuração pode ser realizada tanto de forma manual quanto por meio de aplicativo próprio, demonstrada na Figura 8, que simplifica o processo e amplia a acessibilidade para usuários não técnicos.

A infraestrutura utiliza arquitetura distribuída com *anycast* [1], contribuindo para estabilidade operacional e bom desempenho nas consultas DNS. A documentação oficial é detalhada, clara e orientada à implementação prática, como ilustrado na Figura 7.

Figura 7 – Instruções via website do AdGuard DNS.



Fonte: AdGuard (2026).

[1] Anycast é uma técnica de roteamento em que múltiplos servidores compartilham o mesmo endereço IP, sendo a requisição direcionada automaticamente ao servidor mais próximo ou com melhor desempenho.

Figura 8 – Aplicativo do AdGuard DNS.

Fonte: Da Autora.

4.1.2.4 Quad9

O Quad9 foi incluído por sua abordagem voltada exclusivamente à segurança. O resolvedor realiza bloqueios automáticos com base em múltiplas fontes de inteligência de ameaças, incluindo feeds provenientes de organizações especializadas em segurança cibernética, como a IBM X-Force e outros parceiros.

Essas informações são integradas e atualizadas de forma contínua, permitindo rápida resposta a novas ameaças e maior eficiência na identificação de domínios maliciosos.

O serviço também oferece suporte a DoT, DoH e DNSCrypt, reforçando a proteção das consultas contra interceptação e adulteração.

Sua implementação é direta, sendo realizada por meio da configuração manual de DNS em dispositivos ou roteadores, como demonstrado na Figura 9. Apesar de simples, essa abordagem pode exigir conhecimento técnico básico por parte do usuário.

A infraestrutura do Quad9 utiliza a arquitetura *anycast*, distribuída em centenas de pontos de presença (PoPs) globalmente. A documentação é bem estruturada, clara e

adequada para diferentes níveis de conhecimento.

Figura 9 – Instruções via website do Quad9.

Fonte: Quad9 (2026).

4.1.3 Etapa 3 - Estruturação e adaptações do script

O script em Bash utilizado neste estudo tem como finalidade automatizar a verificação do comportamento de diferentes resolvedores DNS diante de domínios classificados como maliciosos. Sua execução ocorre de forma padronizada, garantindo condições uniformes durante os testes.

O código-base utilizado foi adaptado a partir de um script público disponibilizado por Kris Lowet na plataforma GitHub, em seu repositório (LOWET, 2023). Originalmente foi desenvolvido no contexto de uma análise comparativa de resolvedores DNS com foco em filtragem de malware.

4.1.3.1 Estrutura do script

Os resolvedores de DNS avaliados são definidos diretamente no código por meio de seus respectivos endereços IP. Entre eles, incluiu-se um resolvedor sem mecanismos de filtragem (Cloudflare 1.1.1.1), utilizado como referência para validação dos domínios e como base de comparação com os serviços que implementam filtragem.

O script realiza automaticamente a coleta de domínios suspeitos a partir de duas fontes públicas: a lista disponibilizada pelo CERT.pl e a lista URLhaus. Inicialmente, são selecionados os primeiros 1.000 domínios de cada fonte, os quais passam por um processo de pré-processamento para remoção de comentários, entradas inválidas e formatações inconsistentes.

Após a etapa de limpeza e unificação das listas, é realizada a remoção de duplicatas, preservando a ordem de inserção. Em seguida, os domínios são validados por meio do

resolvedor de referência, sendo descartados aqueles que não retornam um endereço IP válido, caracterizando domínios inativos ou não resolvíveis.

Para os domínios selecionados, são realizadas consultas DNS nos demais resolvedores configurados. As respostas são classificadas como resolução válida ou bloqueio, considerando tanto a ausência de resposta quanto a presença de endereços IP associados a mecanismos de bloqueio.

As consultas aos resolvedores com filtragem são executadas em paralelo por meio da ferramenta *GNU Parallel*, reduzindo o tempo total de execução do experimento.

4.1.3.2 Adaptações realizadas

O script original foi modificado com o objetivo de melhorar a consistência dos resultados e garantir maior precisão na identificação de bloqueios DNS. As principais adaptações realizadas são descritas a seguir e o script adaptado está disponível no repositório (SOUZA, 2026):

- **Atualização dos resolvedores avaliados:** A lista de servidores foi reorganizada para incluir explicitamente serviços com filtragem ativa, como Cloudflare (1.1.1.2), CleanBrowsing, AdGuard e Quad9.
- **Ampliação do conjunto de IPs de bloqueio:** Foram adicionados endereços IP associados a mecanismos de bloqueio utilizados por diferentes provedores, como os IPs do AdGuard (`94.140.14.33`, `94.140.14.35` e `94.140.14.15`), evitando que respostas de *sinkhole* [2] fossem interpretadas como resoluções válidas.
- **Limitação controlada da amostra:** Diferentemente da versão original, que utilizava listas completas, o script limitou a coleta às 1.000 primeiras entradas de cada fonte. Em seguida, foi realizada validação por resolução DNS utilizando o resolvedor Cloudflare 1.1.1.1, sendo descartados os domínios sem resposta válida. Embora tenham sido obtidos 955 domínios válidos, observou-se desequilíbrio entre as bases, com 345 do CERT.pl e 610 do URLhaus. Para análise comparativa, foi aplicado balanceamento da amostra, com seleção de 300 domínios válidos por fonte, garantindo consistência e comparabilidade dos dados.
- **Processamento independente das fontes:** As listas passaram a ser tratadas separadamente antes da unificação, assegurando maior consistência na limpeza dos dados.

[2] Sinkhole é uma técnica de segurança em que domínios maliciosos ou indesejados são redirecionados para endereços IP controlados, impedindo a comunicação com o destino original.

- **Remoção de duplicatas com preservação de ordem:** Foi adotada a abordagem `awk '!seen[$1]++'` para eliminar entradas repetidas sem alterar a ordem original dos domínios, garantindo reprodutibilidade.
- **Identificação da origem dos domínios:** Cada entrada passou a incluir um rótulo indicando sua lista de origem, permitindo rastreabilidade nos resultados.
- **Adequação do formato CSV:** O delimitador foi alterado para ponto e vírgula (`;`), garantindo compatibilidade com o padrão regional brasileiro.

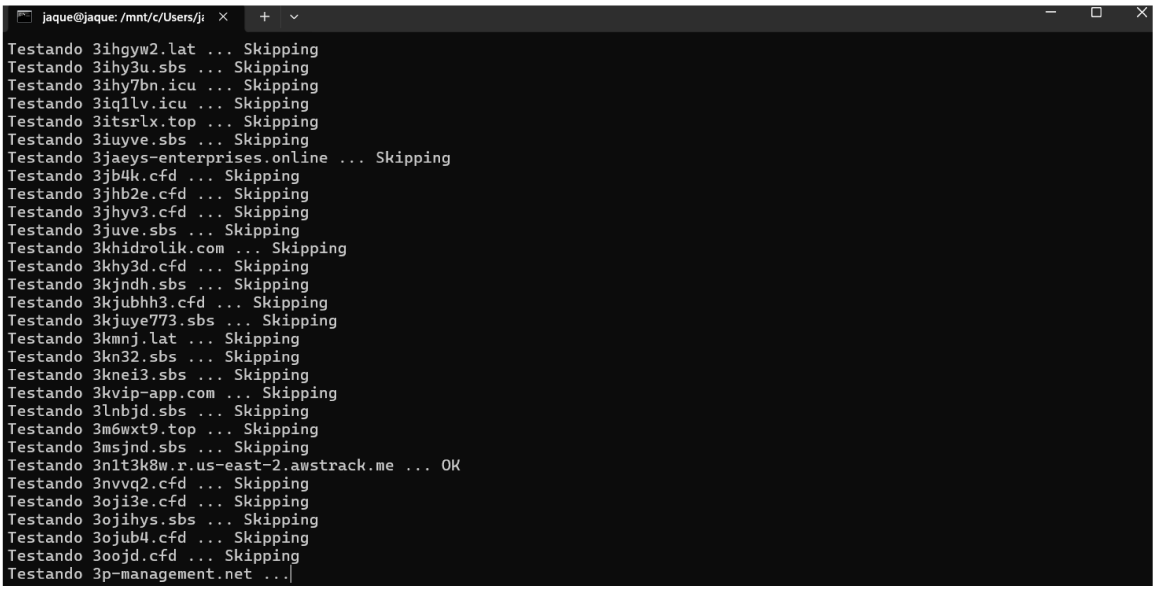
4.1.4 Etapa 4 - Procedimentos de execução dos testes

Os testes experimentais foram executados de forma automatizada por meio de um script em bash, utilizando o ambiente Linux provido pelo *Windows Subsystem for Linux* (WSL) no Windows 11, o que garantiu compatibilidade com as ferramentas empregadas.

A execução seguiu a lógica definida no programa adotado como base metodológica, sem necessidade de intervenção manual durante a realização das consultas DNS. Esse processo é ilustrado na Figura 10.

Durante os testes, o script efetuou consultas DNS a partir de duas listas de domínios previamente definidas, direcionando as requisições aos resolvedores configurados no código. As listas de domínios foram percorridas de forma ordenada, assegurando a coleta consistente e padronizada dos resultados.

Figura 10 – Execução do script.



Fonte: Da Autora.

4.1.5 Etapa 5 - Coleta e organização dos dados

Durante a execução dos testes, o script registra automaticamente os resultados das consultas DNS em um arquivo no formato CSV (*Comma-Separated Values*). Cada linha corresponde a um domínio consultado, e cada coluna representa o resultado retornado por um resolvedor específico.

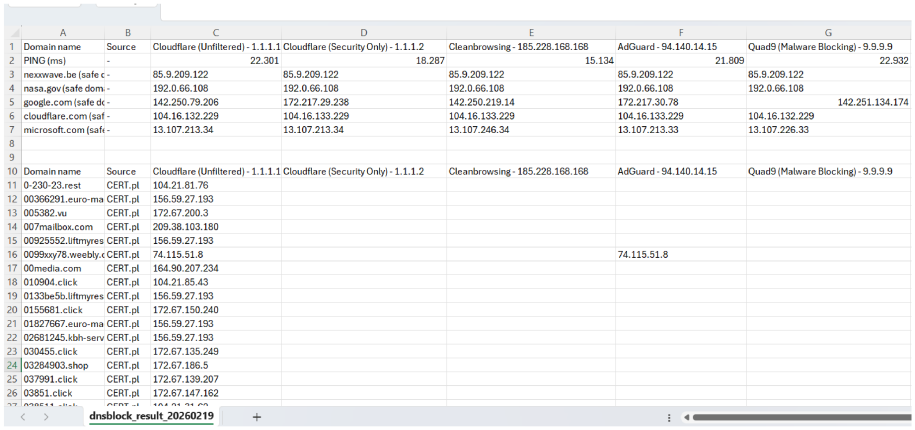
A planilha está organizada em duas seções distintas, conforme evidenciado na Figura 11.

1. Na primeira seção, as linhas iniciais apresentam domínios legítimos utilizados como referência para validar o correto funcionamento dos resolvedores DNS. Nessa etapa,

a presença de um endereço IP nas colunas correspondentes indica que o resolvedor está operacional e realizando a resolução corretamente.

2. Após uma linha em branco, iniciou-se a segunda seção, correspondente aos testes propriamente ditos. Nessa parte, são listados os domínios acompanhados da identificação de sua fonte de origem (CERT.pl ou URLhaus), permitindo a rastreabilidade dos dados. As colunas subsequentes representam os resultados retornados por cada resolvedor configurado no script, identificados pelo nome do serviço e seu respectivo endereço IP: Cloudflare (Unfiltered) – 1.1.1.1; Cloudflare – 1.1.1.2; CleanBrowsing – 185.228.168.9; AdGuard – 94.140.14.15; e Quad9 (Malware Blocking) – 9.9.9.9.

Figura 11 – Organização dos dados na planilha em formato CSV.



	A	B	C	D	E	F	G
1	Domain name	Source	Cloudflare (Unfiltered) - 1.1.1.1	Cloudflare (Security Only) - 1.1.1.2	Cleanbrowsing - 185.228.168.168	AdGuard - 94.140.14.15	Quad9 (Malware Blocking) - 9.9.9.9
2	PING (ms)	-	22.301	18.287	15.134	21.809	22.932
3	nexxwave.be (safe c	-	85.9.209.122	85.9.209.122	85.9.209.122	85.9.209.122	85.9.209.122
4	nasa.gov (safe dom	-	192.0.66.108	192.0.66.108	192.0.66.108	192.0.66.108	192.0.66.108
5	google.com (safe dc	-	142.250.79.206	172.217.29.238	142.250.219.14	172.217.30.78	142.251.134.174
6	cloudflare.com (saf	-	104.16.132.229	104.16.133.229	104.16.133.229	104.16.133.229	104.16.132.229
7	microsoft.com (safe	-	13.107.213.34	13.107.213.34	13.107.246.34	13.107.213.33	13.107.226.33
8							
9							
10	Domain name	Source	Cloudflare (Unfiltered) - 1.1.1.1	Cloudflare (Security Only) - 1.1.1.2	Cleanbrowsing - 185.228.168.168	AdGuard - 94.140.14.15	Quad9 (Malware Blocking) - 9.9.9.9
11	0-230-23.rest	CERT.pl	104.21.81.76				
12	00366291.euro-ma	CERT.pl	156.59.27.193				
13	005382.vu	CERT.pl	172.67.200.3				
14	007mailbox.com	CERT.pl	209.38.103.180				
15	00925552.liftmyres	CERT.pl	156.59.27.193				
16	0099xxy78.weebly.c	CERT.pl	74.115.51.8			74.115.51.8	
17	00media.com	CERT.pl	164.90.207.234				
18	010904.click	CERT.pl	104.21.85.43				
19	0133be5b.liftmyres	CERT.pl	156.59.27.193				
20	0155681.click	CERT.pl	172.67.150.240				
21	01827667.euro-ma	CERT.pl	156.59.27.193				
22	02681245.kbh-serv	CERT.pl	156.59.27.193				
23	030455.click	CERT.pl	172.67.135.249				
24	03284903.shop	CERT.pl	172.67.186.5				
25	037991.click	CERT.pl	172.67.139.207				
26	03851.click	CERT.pl	172.67.147.162				

dnsblock_result_20260219

Fonte: Da Autora.

Na seção de testes, a presença de um endereço IP indica que o domínio foi resolvido normalmente, ou seja, não foi bloqueado pelo resolvedor. Por outro lado, quando o domínio é bloqueado, o script registra a célula correspondente em branco no arquivo CSV.

4.1.6 Etapa 6 - Visualização dos resultados

Inicialmente, foram analisados os dados obtidos durante a execução dos testes, considerando, de forma separada para cada lista, o número absoluto de domínios bloqueados por cada resolvedor, obtido a partir da diferença entre o total de amostras por lista e os domínios não bloqueados identificados nas consultas. Os resultados foram apresentados por meio de gráficos comparativos, permitindo observar o desempenho individual de cada serviço dentro de cada conjunto analisado.

Em seguida, os percentuais de bloqueio apurados experimentalmente foram comparados com as métricas previamente estabelecidas na metodologia para cada resolvedor. Essa comparação foi realizada considerando separadamente os resultados obtidos em cada lista, possibilitando verificar o grau de alinhamento entre a avaliação teórica e o desempenho prático observado em diferentes contextos de ameaça.

5 Resultados

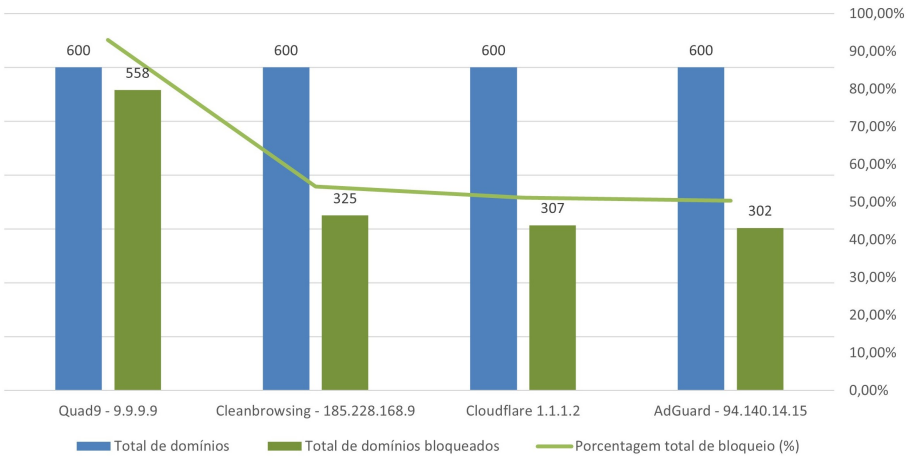
5.1 Análise dos dados obtidos

Inicialmente, apresentou-se uma visão geral dos resultados considerando o total de domínios analisados. Em seguida, os dados são detalhados por fonte, possibilitando uma compreensão mais aprofundada do desempenho dos resolvedores em diferentes cenários.

5.1.1 Visão geral dos resultados

Na Figura 12 está ilustrado o desempenho agregado dos resolvedores, considerando o total de 600 domínios avaliados, sendo 300 provenientes do CERT.pl e 300 do URLhaus.

Figura 12 – Total de domínios bloqueados por resolvedor



Fonte: Da Autora.

Observou-se que o Quad9 apresentou o melhor desempenho geral, com 558 domínios maliciosos bloqueados (93,00%), destacando-se de forma significativa em relação aos demais resolvedores.

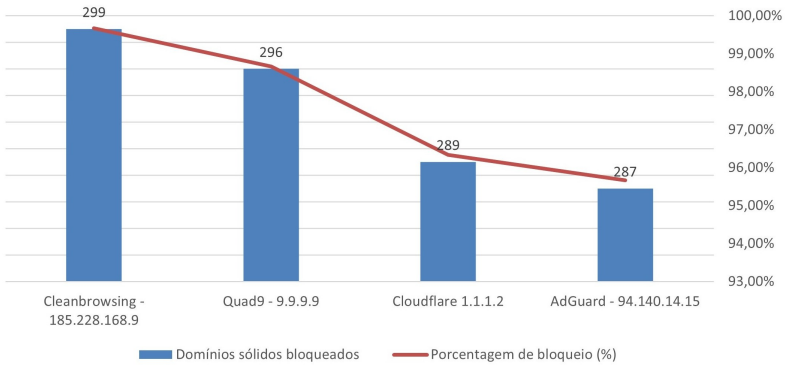
O CleanBrowsing totalizou 325 domínios bloqueados (54,17%), enquanto o Cloudflare e o AdGuard apresentaram resultados próximos, com 307 (51,17%) e 302 (50,33%) domínios bloqueados, respectivamente.

Essa análise inicial evidencia diferenças relevantes no desempenho agregado dos resolvedores, indicando a necessidade de uma avaliação segmentada por fonte de dados para melhor compreensão dos resultados.

5.1.2 Resultados para domínios do CERT.pl

Na análise dos 300 domínios provenientes do CERT.pl, cujos resultados são apresentados na Figura 13, observou-se que todos os resolvedores apresentaram elevadas taxas de bloqueio, com desempenho relativamente homogêneo entre si.

Figura 13 – Taxa de bloqueio para domínios provenientes do CERT.pl



Fonte: Da Autora.

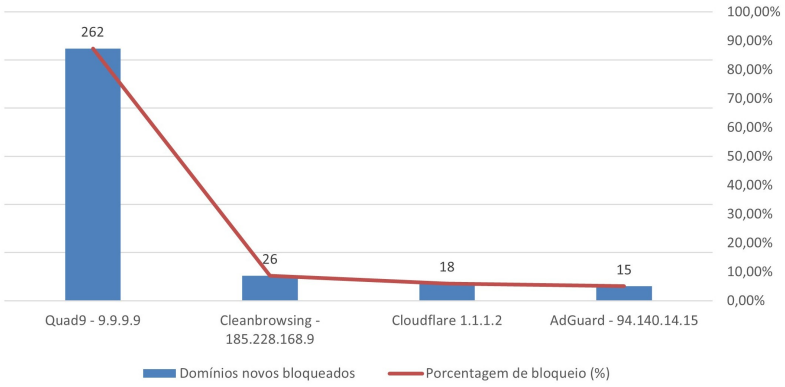
O CleanBrowsing apresentou o melhor resultado, com 299 domínios bloqueados (aproximadamente 99,67%), seguido pelo Quad9 com 296 bloqueios (cerca de 98,67%). O Cloudflare registrou 289 bloqueios (aproximadamente 96,33%), enquanto o AdGuard bloqueou 287 domínios (cerca de 95,67%).

5.1.3 Resultados para domínios do URLhaus

Para os outros 300 domínios oriundos do URLhaus, evidenciados na Figura 14, observou-se diferença significativa no desempenho dos resolvedores avaliados.

O Quad9 destacou-se de forma expressiva, bloqueando 262 domínios (aproximadamente 87%). Em contraste, os demais resolvedores apresentaram taxas substancialmente inferiores: o CleanBrowsing bloqueou 26 domínios (cerca de 8%), o Cloudflare bloqueou 18 domínios (aproximadamente 6%) e o AdGuard bloqueou 15 domínios (cerca de 5%).

Figura 14 – Taxa de bloqueio para domínios provenientes do URLhaus



Fonte: Da Autora.

5.2 Comparação entre os conjuntos de dados analisados

A análise comparativa dos resultados obtidos a partir das bases do CERT.pl e do URLhaus mostra diferenças claras no comportamento dos resolvedores DNS frente a diferentes tipos de ameaças e tempos de atualização.

O conjunto de dados do CERT.pl é composto por domínios associados a campanhas maliciosas, incluindo phishing, fraudes online e conteúdos enganosos. Trata-se de uma iniciativa vinculada ao CERT da Polônia, com caráter institucional e nacional, na qual os domínios passam por análise técnica e validação antes de serem incluídos na lista. O rigor técnico da instituição é evidenciado pelo desenvolvimento de ferramentas próprias de defesa cibernética, como o *Artemis*, um scanner de segurança criado para identificar vulnerabilidades em serviços web CERT.pl (2026). Esse mesmo processo estruturado de análise é aplicado na triagem de ameaças. Como resultado, os domínios incluídos na lista de bloqueio apresentam maior grau de validação quanto à sua natureza maliciosa, o que tende a resultar em bloqueios mais consistentes entre os resolvedores DNS. Esse cenário evidencia que processos institucionais de validação contribuem para maior uniformidade na mitigação das ameaças.

Em contrapartida, a base do URLhaus, mantida pela Abuse.ch, é um repositório comunitário aberto voltado à coleta e ao compartilhamento de URLs associados à distribuição de malware URLhaus (2026). Diferentemente de listas institucionais, trata-se de uma plataforma colaborativa, alimentada por pesquisadores e sistemas automatizados, permitindo a inclusão rápida de URLs recentemente identificadas como maliciosas. Essa base caracteriza-se por sua alta dinamicidade, refletindo a rápida evolução das campanhas maliciosas na Internet. O caráter aberto e continuamente atualizado tende a gerar maior variabilidade na resposta dos serviços analisados: no experimento realizado, o Quad9 apresentou taxa de bloqueio de 87%, enquanto os demais resolvedores registraram valores entre 5% e 8%, o que dificulta sua detecção por mecanismos de filtragem baseados

exclusivamente em DNS, que operam no nível de domínio.

Isso demonstra que a eficácia de um resolvedor DNS não depende apenas da capacidade de bloqueio, mas também da natureza e do processo de curadoria das fontes de inteligência de ameaças utilizadas. Essa distinção torna-se relevante quando se observa o contraste entre listas institucionais e bases colaborativas, uma vez que cada uma apresenta características distintas em termos de confiabilidade, granularidade e atualização.

No contexto analisado, a robustez de um sistema de proteção DNS está diretamente associada ao perfil dessas fontes: enquanto listas institucionais como a do CERT.pl, submetidas a processos formais de validação e análise técnica, tendem a fornecer bloqueios mais consistentes e abrangentes contra domínios fraudulentos, bases colaborativas e altamente dinâmicas como o URLhaus apresentam desafios operacionais para a filtragem via DNS, devido à sua maior granularidade e à rápida atualização das ameaças.

6 Conclusão

Este trabalho investigou a utilização de serviços de resolução de nomes de domínio com mecanismos de filtragem de segurança como estratégia de proteção digital para usuários com experiência reduzida no uso de tecnologias. Foram avaliados provedores amplamente utilizados: Cloudflare DNS, CleanBrowsing, AdGuard e Quad9, considerando critérios técnicos e práticos.

Considerando o público-alvo, observou-se que o desempenho técnico, de forma isolada, não é suficiente para determinar a adequação de uma solução. Embora métricas como tempo de resposta e taxa de bloqueio sejam relevantes, a análise demonstrou que outros fatores exercem papel igualmente importante na prática. Critérios como nível de segurança oferecido, aplicabilidade, disponibilidade do serviço e documentação influenciam diretamente a viabilidade de adoção, especialmente para usuários com menor familiaridade com tecnologia, que tendem a enfrentar dificuldades na configuração e compreensão dessas ferramentas.

Os resultados experimentais evidenciaram diferenças relevantes entre os serviços avaliados, demonstrando que a escolha do resolvedor impacta diretamente o nível de proteção oferecido. Observou-se desempenho semelhante no bloqueio de domínios associados a *phishing*, porém variações significativas no tratamento de infraestruturas ligadas à distribuição de malware. Nesse contexto, o Quad9 manteve desempenho elevado em ambas as bases de teste, enquanto os demais apresentaram redução expressiva no conjunto relacionado à base dinâmica da URLhaus.

Entre as limitações deste estudo, destacam-se a ausência de análise longitudinal para avaliar a variação do desempenho dos provedores ao longo do tempo e a não avaliação de arquiteturas de proteção em múltiplas camadas que integrem diferentes soluções.

Como perspectivas para trabalhos futuros, destacam-se:

- Realização de estudos longitudinais para avaliar a estabilidade e a evolução do desempenho dos provedores ao longo do tempo;
- Investigação da integração de soluções de proteção em múltiplas camadas, combinando mecanismos de filtragem local, como o Pi-hole, com resolvedores DNS seguros.

Ressalta-se que a realização deste estudo foi viabilizada pelos conhecimentos adquiridos ao longo da formação acadêmica, em especial nas disciplinas de Sistemas Operacionais, Arquitetura e Organização de Computadores e Redes de Computadores. Tais áreas forneceram o embasamento teórico necessário para a compreensão dos aspectos

estruturais e operacionais dos sistemas computacionais, bem como dos protocolos e mecanismos envolvidos na comunicação em redes, fundamentais para a análise desenvolvida neste trabalho.

Concluiu-se que os serviços de DNS com filtragem de segurança constituem uma solução acessível para o fortalecimento da proteção digital de usuários com menor conhecimento tecnológico, desde que selecionados de forma criteriosa e alinhada às suas necessidades.

Referências

ADGUARD. **Conecte-se aos servidores DNS públicos do AdGuard**. 2026. <https://adguard-dns.io/pt_br/public-dns.html>.

AKAMAI. **O que é armazenamento de DNS em cache?** 2026. <https://www.akamai.com/pt/glossary/what-is-dns-caching>.

ALLIANCE, C. S. **DNS Layer Security: The Ultimate Guide to What It Is and Why You Need It**. 2021. <https://cloudsecurityalliance.org/blog/2021/12/09/dns-layer-security-the-ultimate-guide-to-what-it-is-and-why-you-need-it>.

Be My Eyes. **Let's see the world together**. 2026. <https://www.bemyeyes.com/>.

CERT.PL. **The Artemis security scanner**. 2026. <http://cert.pl/en/posts/2024/01/artemis-security-scanner/>.

CHUNG, E. **Age-inclusive design for web interfaces**. 2024. <https://blog.logrocket.com/ux-design/age-inclusive-design-web-interfaces/>.

CIDADANIA, M. dos Direitos Humanos e. **Com apoio do MDHC, projeto capacita pessoas idosas para se protegerem de golpes em âmbito virtual**. 2025. <https://www.gov.br/mdh/resolveuid/217cdab74bb1491f990fba5f2d5766d8>.

CLEANBROWSING. **Setup Guide**. 2025. <https://cleanbrowsing.org/setup>.

CLOUDFLARE. **Introducing 1.1.1.1 for Families**. 2020. <https://blog.cloudflare.com/introducing-1-1-1-1-for-families/>.

_____. **DNS over HTTPS**. 2025. <https://developers.cloudflare.com/1.1.1.1/encryption/dns-over-https/>.

_____. **O que é filtragem de DNS? Servidores de DNS seguros**. 2026. <https://www.cloudflare.com/pt-br/learning/access-management/what-is-dns-filtering/>.

_____. **O que é segurança de DNS?** 2026. <https://www.cloudflare.com/pt-br/learning/dns/dns-security/>.

_____. **Set up**. 2026. <https://developers.cloudflare.com/1.1.1.1/setup/>.

COMMUNITY, T.-L. **Wi-Fi Routers Support DoH and DoT Network**. 2023. <https://community.tp-link.com/en/home/forum/topic/617138>.

DN.ORG. **The Evolution of DNS: From Simple Name Resolution to a Secure Internet Backbone**. 2024. <https://dn.org/the-evolution-of-dns-from-simple-name-resolution-to-a-secure-internet-backbone/>.

DNSFILTER. **How AI Powers DNS Threat Detection in Real Time**. 2025. <https://www.dnsfilter.com/blog/ai-threat-detection-in-dns-filtering>.

DNS.SB. **Using DNS over TLS at DNS.SB**. 2026. <https://dns.sb/dot/>.

ERLICH, F. **Quase 60% dos brasileiros já foram alvos de golpes online, aponta pesquisa**. 2025. <https://veja.abril.com.br/coluna/radar-economico/quase-60-dos-brasileiros-ja-foram-alvos-de-golpes-online-aponta-pesquisa/>.

FEBRABAN. **Veja os 10 golpes mais comuns aplicados contra idosos e saiba como evitá-los**. 2024. <https://portal.febraban.org.br/noticia/4177/pt-br>.

FORTINET. **O que é DNS: Domain Name System**. 2026. <https://www.fortinet.com/br/resources/cyberglossary/what-is-dns>.

_____. **O que é proteção DNS?** 2026. <https://www.fortinet.com/br/resources/cyberglossary/dns-protection>.

FOUNDATION, Q. **An open DNS recursive service for free security and high privacy**. 2026. Disponível em: <https://quad9.net/>.

IBGE, A. **Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet**. 2023. <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet>.

IBM. **O que é DNS (Domain Name System)?** 2026. <https://www.ibm.com/br-pt/think/topics/dns>.

KOSEK, M. et al. **DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance**. 2023. <https://arxiv.org/pdf/2305.00790>.

LIBERATO, M.; AFFINITO, A.; MEIJERINK, B.; JONKER, M.; BOTTA, A.; SPEROTTO, A. To block or not to block? evaluating parental controls across routers, dns services, and software. In: **2025 9th Network Traffic Measurement and Analysis Conference (TMA)**. [S.l.: s.n.], 2025. p. 1–10.

LOWET, K. **dnsblock.sh**. 2023. <https://gist.github.com/KrisLowet/675ba34e682c6d2afbc53fc317b41e85>.

_____. **Public DNS malware filters to be tested in 2025**. 2025. <https://techblog.nexxwave.eu/public-dns-malware-filters-to-be-tested-in-2025/>.

LUMIUN, E. **Bloqueio e filtragem DNS: como proteger os usuários sem se tornar um vigilante abusivo**. 2026. <https://www.lumiun.com/blog/bloqueio-e-filtragem-dns-como-proteger-os-usuarios-sem-se-tornar-um-vigilante-abusivo>.

MAGNUSSON, J. **Survey and Analysis of DNS Filtering Components**. 2024. <https://arxiv.org/pdf/2401.03864>.

OPENDNS. **WHO IS OpenDNS?** 2025. <https://www.opendns.com/about/company-history/>.

PRESTON, S. **O que é DNSSEC e como funciona?** 2026. <https://www.akamai.com/pt/blog/trends/dnssec-how-it-works-key-considerations>.

QUAD9. **Endereços e Caraterísticas do Serviço**. 2026. <https://quad9.net/pt/service/service-addresses-and-features/>.

RAYMOND, S. **Fresno Unified School District Deployed DNSFilter to 35,000 Android Devices**. 2021. <https://www.dnsfilter.com/blog/fresno-unified-school-district-deployed-dnsfilter-to-35-000-android-devices>.

SECURITY, H. **What Is DNS Filtering and Why Does Your Business Need It?** 2024. <https://heimdalsecurity.com/blog/dns-filtering>.

SENADO, A. **Golpes virtuais aumentam e não fazem distinção de idade**. 2025. <https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade>.

SERVICES, A. W. **O que é DNS?** 2026. <https://aws.amazon.com/pt/route53/what-is-dns/>.

SIDN. **A cryptographic security extension to the DNS protocol**. 2026. <https://www.sidn.nl/en/modern-internet-standards/dnssec>.

SILVA, M.; FRANCO, M.; SCHEID, E.; ZEMBRUZKI, L.; GRANVILLE, L. Desempenho de resolvedores de dns públicos: Uma análise do estado da arte. In: **Anais da XX Escola Regional de Redes de Computadores**. Porto Alegre, RS, Brasil: SBC, 2023. p. 43–48. ISSN 2595-5911. Disponível em: <https://sol.sbc.org.br/index.php/errc/article/view/26003>.

SILVA, M. A. d.; FRANCO, M. F.; SCHEID, E. J.; ZEMBRUZKI, L.; GRANVILLE, L. Z. Perfresolv: A geo-distributed approach for performance analysis of public dns resolvers based on domain popularity. In: **International Conference on Advanced Information Networking and Applications (AINA 2024)**. Cham, Switzerland: Springer, 2024. (Lecture Notes on Data Engineering and Communications Technologies, v. 200), p. 35–47. Disponível em: <https://link.springer.com/chapter/10.1007/978-3-031-57853-3_4>.

SINGANAMALLA, S.; CHUNHAPANYA, S.; VAVRUšA, M.; VERMA, T.; WU, P.; FAYED, M.; HEIMERL, K.; SULLIVAN, N.; WOOD, C. **Oblivious DNS over HTTPS (ODoH): A Practical Privacy Enhancement to DNS**. 2020. <https://arxiv.org/pdf/2011.10121>.

SOUZA, J. G. de. **Resolvers-performance**. 2026. <https://github.com/jaquelinegon/Resolvers-performance.git>.

SUPPORT, M. **Configure DNS over HTTPS protection levels in Firefox**. 2025. <https://support.mozilla.org/en-US/kb/dns-over-https>.

TECHNOLOGIES, A. **What Is DNS Traffic Management?** 2026. <https://www.akamai.com/glossary/what-is-dns-traffic-management>.

URLHAUS. **URLhaus data**. 2026. <https://urlhaus.abuse.ch/>.

VEJA.ORG. **Como Proteger os Mais Velhos de Golpes e Riscos Online**. 2025. <https://www.veja.org/blog/2025/03/18/como-proteger-os-mais-velhos-de-golpes-e-riscos-online/>.

ZHAUNIAROVICH, Y.; KHALIL, I.; YU, T.; DACIER, M. **A Survey on Malicious Domains Detection through DNS Data Analysis**. 2018. <https://www.researchgate.net/publication/325311352_A_Survey_on_Malicious_Domains_Detection_through_DNS_Data_Analysis>.