

EXTENSÃO DE NAVEGADOR PARA CONTROLE PARENTAL

Rafael Rodrigues de Oliveira¹, Marcel Campos Inocencio²

Resumo: Este trabalho apresenta o desenvolvimento de uma extensão de navegador voltada ao controle parental, criada para o Google Chrome com base no Manifest V3. O objetivo foi oferecer uma solução local e segura que permita aos responsáveis supervisionar e restringir o acesso de crianças e adolescentes a conteúdos inapropriados, sem depender de servidores externos. A ferramenta foi desenvolvida em HTML, CSS e JavaScript, integrando as APIs oficiais do Chrome para bloquear e liberar sites, registrar histórico local e configurar horários de acesso por meio do modo de estudo. O sistema conta ainda com categorias automáticas, proteção de busca com o *SafeSearch* e autenticação por senha para acesso às configurações. Durante os testes no navegador Google Chrome, a extensão apresentou desempenho estável, bloqueando corretamente os domínios configurados e mantendo as preferências após o encerramento do navegador. Os resultados demonstraram eficiência, facilidade de uso e total preservação da privacidade do usuário. Conclui-se que a ferramenta atingiu os objetivos propostos, destacando-se pela operação autônoma e pela interface intuitiva.

Palavras-chave: controle parental. extensão de navegador. segurança digital. privacidade. manifest v3.

¹Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), rafa.rdo2003@gmail.com

²Orientador. Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), marcel.inocencio@gmail.com

ABSTRACT: This work presents the development of a browser extension for parental control, created for Google Chrome based on Manifest V3. The goal was to provide a local and secure solution that allows guardians to supervise and restrict children's access to inappropriate content without relying on external servers. The extension was developed using HTML, CSS, and JavaScript, integrating official Chrome APIs to block and allow websites, record local browsing history, and schedule access periods through a study mode. It also includes automatic category grouping, a *SafeSearch* filter, and password protection for configuration access. During testing in the Google Chrome browser, the extension performed stably, correctly blocking configured domains and maintaining user preferences after browser closure. The results demonstrated efficiency, ease of use, and full preservation of user privacy. It is concluded that the extension achieved its goals, standing out for its autonomous operation and intuitive interface.

Keywords: parental control. browser extension. digital security. privacy. manifest v3.

1 INTRODUÇÃO

O avanço da tecnologia e o acesso facilitado à internet transformaram profundamente a forma como crianças e adolescentes se relacionaram com o mundo digital. A crescente presença de dispositivos conectados possibilitou novas formas de aprendizado, socialização e entretenimento, mas também expôs os usuários mais jovens a riscos como o acesso a conteúdos impróprios, cyberbullying, dependência digital e violações de privacidade (Kabali, 2015; Livingstone et al., 2019). Esse cenário evidenciou a necessidade de que pais e responsáveis dispusessem de ferramentas tecnológicas capazes de supervisionar, limitar e acompanhar o uso da internet de maneira efetiva e segura (Mascheroni; Ólafsson, 2017; Cortesi; Gasser, 2020).

Diversas soluções de controle parental foram desenvolvidas ao longo dos últimos anos com o objetivo de restringir o acesso a sites inadequados, controlar o tempo de uso e registrar atividades online. Entretanto, muitas dessas aplicações apresentaram limitações, como interfaces pouco intuitivas, dependência de servidores externos e necessidade de conhecimento técnico avançado (Liu; Komlodi; Yesilada, 2021; Paudel; Subedi; Ghimire, 2020). Além disso, algumas ferramentas comerciais coletavam dados sensíveis, armazenando informações de navegação em nuvens corporativas, o que levantou preocupações quanto à segurança e à privacidade dos

usuários (Ali et al., 2020; Wang et al., 2021). Essas restrições reforçaram a importância de soluções locais e transparentes, com execução autônoma e controle direto do usuário final.

Sob a perspectiva teórica, o controle parental digital pode ser entendido como uma forma de *mediação tecnológica* entre crianças e o ambiente virtual, na qual os responsáveis buscam equilibrar liberdade e proteção. Segundo Livingstone et al. (2019), o desafio contemporâneo não se restringe ao bloqueio de conteúdos, mas envolve apoiar o desenvolvimento da autonomia digital de forma segura e consciente. Da mesma forma, Mascheroni e Ólafsson (2017) apontaram que a eficácia das ferramentas está diretamente associada à capacidade de adaptação às necessidades das famílias e à clareza das informações oferecidas, reforçando a importância de soluções flexíveis e de fácil uso.

A literatura sobre segurança digital destacou a relevância de abordagens descentralizadas, baseadas na execução local e em mecanismos de isolamento de contexto, capazes de reduzir vulnerabilidades e riscos de exposição de dados (Alenezi; Alshehri, 2021; Rahman; Baggili; Liu, 2023). De acordo com Grosse e Upadhyay (2020), a execução local e o isolamento de permissões no navegador são fundamentais para minimizar o impacto de falhas em extensões, uma vez que reduzem a superfície de ataque e garantem maior controle sobre o processamento de informações. O Manifest V3, adotado pelo Google Chrome, consolidou esse modelo ao limitar o acesso direto a APIs críticas e adotar a abordagem declarativa *declarativeNetRequest*, que define regras de bloqueio pré-aprovadas pelo navegador, fortalecendo a segurança e o controle de execução (Developers, 2023; Lee; Kwon, 2021). Esses avanços representaram uma mudança significativa em relação às versões anteriores do modelo de extensões, que eram mais suscetíveis a vazamentos e uso indevido de dados.

Além dos aspectos de segurança, estudos sobre usabilidade e design têm apontado que a eficácia de ferramentas de controle parental está fortemente relacionada à sua capacidade de oferecer uma experiência acessível e intuitiva. Mahmood e Maqbool (2021) destacaram que a adoção de interfaces claras e consistentes reduz a carga cognitiva do usuário, tornando a configuração mais eficiente. Já Ferreira, Santos e Carvalho (2022) ressaltaram a importância da acessibilidade digital, argumentando que interfaces adaptáveis ao contexto visual e sensorial dos usuários promovem inclusão e ampliam o alcance das soluções. Assim, a combinação entre segurança local, privacidade e design acessível tem se mostrado essencial

para garantir o uso efetivo de ferramentas de mediação digital (Aslan; Mete; Özel, 2020).

Nesse contexto, extensões de navegador se consolidaram como uma alternativa promissora, pois operaram diretamente no ambiente de navegação, permitindo interceptar e bloquear solicitações de sites em tempo real, sem necessidade de infraestrutura adicional (Sharma; Mehta, 2022; Moghaddam; Samadi; Khonsari, 2022). Segundo o *StatCounter* (StatCounter, 2024), o Google Chrome representou mais de 65% do mercado global de navegadores em 2024, consolidando-se como a principal plataforma de acesso à web. Sua estrutura modular, definida no Manifest V3, proporcionou maior controle sobre permissões e segurança na execução de scripts (Developers, 2023; Grosse; Upadhyay, 2020).

Com base nesse cenário, o presente trabalho teve como objetivo o desenvolvimento de uma extensão de navegador voltada ao controle parental, projetada para o Google Chrome. A solução foi implementada de forma a operar totalmente em ambiente local, utilizando tecnologias web consolidadas como HTML, CSS e JavaScript, integradas à API oficial de extensões do Chrome. A extensão permitiu o bloqueio de sites, a criação de listas de permissão e a configuração de um modo de estudo com horários programáveis, garantindo a privacidade e o controle de uso. A interface foi desenvolvida com foco em responsividade e integração visual, adaptando-se automaticamente ao tema do navegador, claro ou escuro e mantendo consistência estética e conforto durante a navegação (Bhanarkar; Paul; Mehta, 2023; Ferreira; Santos; Carvalho, 2022).

Durante a fase de desenvolvimento, foram analisadas as principais ferramentas de controle parental disponíveis no mercado e em repositórios acadêmicos, buscando compreender suas abordagens e limitações. Essa análise incluiu soluções como o *FilterPlus* (Babu; Kumar, 2014), que realiza bloqueio de conteúdo em tempo real; o *AI Parental Control* (AI Parental Control, 2023), que aplica algoritmos de inteligência artificial para filtragem; e o estudo *Betrayed by the Guardian* (Ali et al., 2020), que revelou falhas de segurança e privacidade em diversas plataformas comerciais. A partir dessa comparação, foram identificadas lacunas quanto à transparência dos dados e à dependência de serviços externos, fatores que nortearam as decisões de design e arquitetura do trabalho aqui desenvolvido.

A extensão criada utilizou armazenamento interno (*localStorage*) para preservar as configurações de bloqueio, permitindo que as informações permanecessem disponíveis mesmo após o encerramento da sessão.

Essa abordagem eliminou a necessidade de cadastros e logins, reforçando a autonomia do usuário e a segurança local. Também foram implementadas boas práticas de segurança e privacidade, conforme recomendações de órgãos como a Mozilla Foundation e o W3C (Foundation, 2024; W3C, 2023). O sistema foi projetado com arquitetura modular, seguindo os princípios do Manifest V3, garantindo isolamento de contexto e execução controlada das funções de bloqueio e monitoramento (Lee; Kwon, 2021).

Os testes realizados confirmaram que a extensão atingiu os objetivos estabelecidos, bloqueando corretamente os sites configurados, registrando os acessos e ativando o modo de estudo nos horários programados. A ferramenta demonstrou estabilidade, operação autônoma e compatibilidade com diferentes versões do navegador, atendendo às expectativas de usabilidade e privacidade definidas no escopo inicial. Dessa forma, foi possível validar a eficácia do trabalho e sua viabilidade como alternativa prática e segura para controle parental em ambiente doméstico.

O trabalho teve como objetivo geral desenvolver uma extensão de navegador para controle parental, possibilitando o bloqueio e a liberação de sites, a configuração de horários de acesso e o registro local de histórico, assegurando a proteção de dados e a personalização das preferências do usuário. Especificamente, buscou-se analisar as principais soluções existentes, identificar suas limitações, definir os requisitos técnicos e funcionais da proposta, implementar a ferramenta com base em tecnologias web modernas e avaliar sua usabilidade em cenários reais de aplicação.

A trabalho desenvolvido contribuiu para o campo da segurança digital e da engenharia de software aplicada, oferecendo uma solução funcional, de baixo custo e de fácil adoção para o contexto familiar. A adoção de uma arquitetura local e independente de servidores externos reforçou o compromisso com a privacidade, enquanto a interface adaptativa e simplificada proporcionou uma experiência positiva para o usuário final. O projeto também serve como base para futuras pesquisas sobre controle parental local e extensões de navegador seguras, ressaltando o potencial das tecnologias web como meio de proteção e mediação digital.

Por fim, este trabalho foi estruturado de modo a apresentar inicialmente a introdução, que abordou a contextualização, fundamentação teórica, justificativa e objetivos. A Seção 2 apresenta os trabalhos correlatos que embasaram o desenvolvimento da extensão. A Seção 3 descreve os materiais e métodos empregados na implementação, enquanto a Seção 4 expõe os resultados e a discussão das funcionalidades obtidas. Por fim,

a Seção 5 apresenta as conclusões gerais, destacando as contribuições do estudo e as perspectivas de aprimoramento futuro.

2 TRABALHOS CORRELATOS

Os trabalhos correlatos analisados serviram de referência para compreender as abordagens mais utilizadas em ferramentas de controle parental e identificar suas limitações técnicas e de segurança. A comparação entre diferentes soluções permitiu avaliar as estratégias de bloqueio de conteúdo, os mecanismos de configuração e os níveis de dependência de infraestrutura externa, fornecendo subsídios para o desenvolvimento do trabalho apresentado neste estudo.

O *FilterPlus*, proposto por Babu e Kumar (2014), consiste em uma extensão de navegador para o Google Chrome voltada à filtragem de conteúdo em tempo real. A ferramenta permite bloquear elementos como cookies, imagens e scripts, além de possibilitar o controle de domínios específicos. Apesar do baixo consumo de recursos e da integração simples com o navegador, o *FilterPlus* limita-se ao bloqueio estático de conteúdo e não possui funcionalidades relacionadas ao controle de tempo de uso ou à criação de listas de permissão. A ausência de um sistema de armazenamento local das configurações também restringe a personalização e a persistência das preferências do usuário após o encerramento do navegador.

Em contraposição, o *AI Parental Control* (AI Parental Control, 2023) apresenta uma proposta mais sofisticada ao empregar algoritmos de inteligência artificial para classificar e restringir conteúdos com base em análise de texto e imagens. Essa extensão comercial, disponibilizada na Chrome Web Store, amplia a precisão na identificação de material impróprio, porém depende de conexão constante com servidores externos para processar os dados, o que implica riscos à privacidade e maior consumo de rede. Além disso, o modelo fechado e baseado em nuvem reduz a transparência do processo de filtragem, impossibilitando que o usuário verifique ou altere os critérios aplicados pela aplicação.

Em contrapartida, o estudo *Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions*, de Ali et al. (2020), destaca vulnerabilidades e práticas invasivas de coleta de dados presentes em diversas ferramentas de controle parental disponíveis comercialmente. A pesquisa revela que muitas dessas aplicações armazenam informações sensíveis de usuários, como históricos de navegação e credenciais de lo-

gin, em servidores remotos sem criptografia adequada. Essa constatação reforça a importância de desenvolver soluções locais e independentes de infraestrutura externa, priorizando a segurança e a transparência no tratamento de dados.

Além dessas soluções, Liu, Komlodi e Yesilada (2021) discutem aspectos de usabilidade em ferramentas de controle parental, enfatizando que a eficácia dessas aplicações depende diretamente da facilidade de configuração e compreensão por parte dos pais e responsáveis. Interfaces complexas e pouco intuitivas tendem a reduzir o engajamento e a adoção dessas ferramentas, comprometendo sua efetividade. Essa observação é considerada no desenvolvimento da extensão proposta neste trabalho, que busca adotar uma interface adaptável ao tema do navegador e uma organização visual simplificada, reduzindo barreiras de uso e ampliando a acessibilidade.

De modo comparativo, observou-se que o *FilterPlus* (Babu; Kumar, 2014) concentra-se apenas em filtragem estática, sem controle de tempo ou persistência de configurações. Já o *AI Parental Control* (AI Parental Control, 2023) introduz inteligência artificial, mas à custa da dependência de servidores externos e coleta de dados. O estudo de Ali et al. (2020) evidencia vulnerabilidades nessas soluções baseadas em nuvem, destacando o risco à privacidade. Em contrapartida, a extensão desenvolvida neste trabalho opera de forma totalmente local, armazenando as configurações no próprio navegador, sem qualquer comunicação externa, o que reduziu riscos de exposição de dados e garante maior autonomia ao usuário. Além disso, o modo de estudo programável e a interface adaptativa representam diferenciais entre as ferramentas analisadas, aliando segurança, simplicidade e controle personalizado.

A análise dos trabalhos correlatos permitiu identificar as tendências atuais e as lacunas ainda existentes na área de controle parental, destacando a necessidade de soluções mais transparentes e personalizáveis. Esses estudos forneceram a base teórica e comparativa necessária para a definição dos requisitos, da arquitetura e das decisões de implementação que nortearam o desenvolvimento desta pesquisa.

3 MATERIAIS E MÉTODOS

Para guiar o desenvolvimento da extensão, adotou-se um procedimento metodológico composto por três etapas principais: Levantamento de requisitos, baseado na análise dos trabalhos correlatos e na observação

de padrões de navegação de pais e responsáveis; implementação da solução, estruturada conforme o modelo de extensões do Chrome no Manifest V3, utilizando HTML, CSS, JavaScript e APIs nativas como a *declarativeNetRequest*; e verificação funcional, realizada por meio de testes práticos que avaliaram estabilidade, bloqueio de domínios, persistência das configurações e execução do modo de estudo.

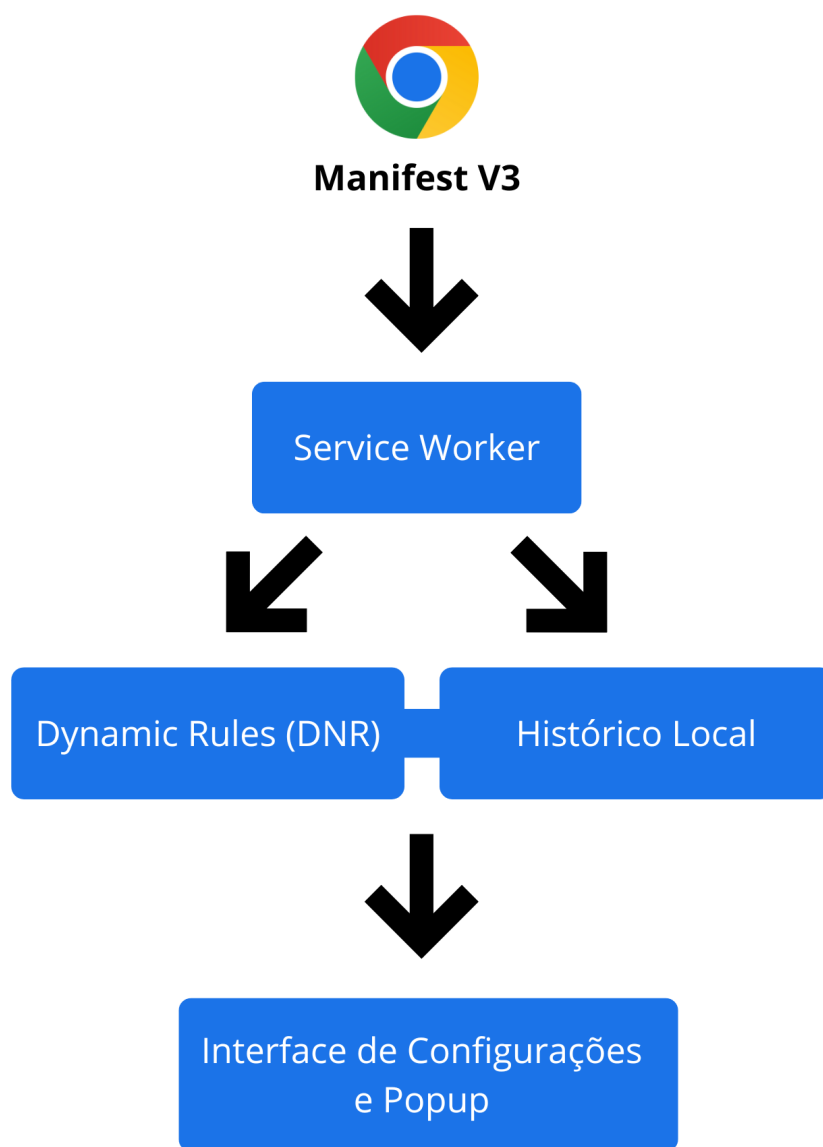
O presente trabalho adota uma abordagem aplicada e experimental, direcionada ao desenvolvimento de uma extensão de navegador para controle parental voltada ao ambiente doméstico. O processo metodológico envolve três etapas complementares: levantamento e análise de requisitos, implementação da ferramenta e verificação funcional. Todo o procedimento fundamenta-se em princípios de engenharia de software e design centrado no usuário, priorizando segurança, privacidade e usabilidade.

A etapa de levantamento de requisitos fundamenta-se na análise dos trabalhos correlatos e em observações sobre o comportamento de navegação de pais e responsáveis. Foram definidos como requisitos funcionais principais: o bloqueio de sites por domínio, a configuração de listas de permissão, o registro local de histórico de navegação e a definição de horários de uso por meio do modo de estudo. Entre os requisitos não funcionais, destacam-se a operação totalmente local, a independência de servidores externos e a adaptação da interface ao tema do navegador, de modo responsivo e acessível.

A arquitetura da extensão estrutura-se no modelo de extensões do Google Chrome conforme o Manifest V3, que define scripts isolados e o uso do *service worker* como componente responsável por executar tarefas em segundo plano de forma eficiente e segura (Developers, 2023; Grosse; Upadhyay, 2020; Upadhyay; Grosse, 2020). Nesse modelo, as regras de bloqueio são aplicadas pelo próprio navegador por meio da API *declarativeNetRequest*, reduzindo a necessidade de scripts ativos e aumentando o desempenho.

A Figura 1 apresenta a arquitetura geral da extensão, destacando a interação entre o Manifest V3, o *service worker*, as regras dinâmicas, o armazenamento local e a interface composta pela página de configurações e pelo *popup*. Enquanto o Manifest define permissões e componentes, o *service worker* atualiza as regras de bloqueio e processa eventos, e o *localStorage* mantém as configurações do usuário de forma persistente no dispositivo.

Figura 1 - Arquitetura da extensão



Fonte: Do autor.

Essa configuração possibilita o controle de permissões e a utilização de APIs nativas, com destaque para a *declarativeNetRequest*, responsável pelo bloqueio de solicitações HTTP de domínios listados. A adoção desse modelo contribui para a segurança e previsibilidade na execução das regras de bloqueio, reduzindo a exposição a falhas e a dependência de componentes externos. O armazenamento das configurações é implementado com a API *localStorage*, permitindo a persistência das listas, histórico

e horários após o encerramento da sessão.

Ao acessar a extensão pela primeira vez, o usuário é solicitado a registrar uma senha de acesso. Essa senha é armazenada de forma criptografada e utilizada em todas as futuras alterações das configurações, impedindo que terceiros, como crianças ou outros usuários do computador modifiquem ou desativem a proteção sem autorização. O mecanismo de autenticação reforça a segurança da ferramenta, restringindo o acesso ao painel administrativo apenas ao responsável cadastrado.

O histórico local da extensão registra três categorias distintas de eventos: “permitido”, “bloqueado” e “suspeito”. A categoria “permitido” registra os domínios acessados que foram previamente autorizados na lista de sites permitidos, além dos acessos a domínios que não estão associados a nenhuma regra de bloqueio; a categoria “bloqueado” registra tentativas de acesso a domínios restritos; e a categoria “suspeito” inclui pesquisas realizadas no Google que contêm termos ou nomes de sites presentes na lista de bloqueio.

Além da categorização, o histórico possui recursos que tornam a visualização e a análise dos registros mais claras e eficientes. Entre elas, destacam-se os filtros dinâmicos que permitem ao responsável selecionar visualmente apenas os registros de um tipo específico, como “bloqueado”, “permitido” ou “suspeito”, facilitando a navegação em grandes volumes de dados. Ao clicar em um registro, é exibida uma descrição detalhando o motivo da classificação, informando, por exemplo, se o domínio foi bloqueado por estar em uma categoria restrita ou se foi considerado suspeito por conter termos relacionados a sites proibidos.

O carregamento do histórico utiliza o mecanismo de *lazy load*, que exibe os registros de forma gradual conforme o usuário rola a página. Essa abordagem melhora o desempenho e reduz o consumo de memória, permitindo que a interface permaneça fluida mesmo com longos períodos de uso. Esse conjunto de melhorias reforça o caráter analítico e transparente do sistema, proporcionando ao responsável um controle mais detalhado e eficiente sobre as atividades de navegação, sem recorrer a servidores externos ou à coleta de dados sensíveis.

A extensão incorpora ainda um módulo de proteção de busca. Essa funcionalidade permite bloquear o acesso direto ao Google Vídeos e Google Imagens, além de aplicar o modo de pesquisa segura (*SafeSearch*). O *SafeSearch* é um recurso nativo de mecanismos de busca que filtra automaticamente resultados com conteúdo sexual explícito, violência

ou linguagem imprópria, ajustando a exibição dos resultados de pesquisa para um contexto mais adequado ao público infantil. A integração desse modo diretamente no navegador garante uma camada adicional de segurança durante o uso de motores de busca.

O modo de estudo possibilita configurar períodos em que apenas os sites previamente autorizados permanecem acessíveis. Durante os horários definidos pelo responsável, os demais domínios são automaticamente bloqueados, direcionando o uso do navegador para fins educacionais ou de pesquisa. Essa funcionalidade auxilia no controle de tempo e na criação de hábitos digitais mais equilibrados, operando de forma automatizada e sem depender de servidores externos.

A implementação da interface foi realizada utilizando HTML, CSS e JavaScript, empregando princípios de design responsivo (Bhanarkar; Paul; Mehta, 2023). A interface principal de configurações é estruturada em seções independentes, permitindo ao usuário habilitar ou desabilitar a proteção, gerenciar listas e categorias, configurar o modo de estudo e visualizar o histórico de navegação. O design adapta-se automaticamente ao tema definido no navegador Chrome, claro ou escuro, garantindo consistência estética e conforto visual durante o uso. O layout utiliza tipografia legível, espaçamento uniforme e botões de ação destacados, favorecendo a compreensão mesmo por usuários com pouca experiência técnica.

Durante a fase de testes, a extensão foi executada no ambiente Windows 10 com o navegador Google Chrome, sendo avaliados aspectos de estabilidade, tempo de resposta, consistência do bloqueio e persistência dos dados locais. Os testes demonstraram que a extensão bloqueou corretamente os domínios configurados, registrou o histórico de acessos e executou o modo de estudo conforme os horários programados, sem apresentar travamentos ou falhas de sincronização. O funcionamento local da ferramenta reduziu o tempo de carregamento e eliminou a necessidade de autenticação externa, comprovando a eficiência da abordagem descentralizada (Alenezi; Alshehri, 2021; Rahman; Baggili; Liu, 2023).

O desenvolvimento foi documentado por meio de versionamento de código e anotações das etapas, garantindo rastreabilidade das alterações e integridade do processo. Ao final, os resultados obtidos demonstraram que a extensão atendeu aos requisitos definidos, validando a proposta e estabelecendo base para futuras evoluções, como a implementação de alteração de senha, proteção contra desativação e integração de mecanismos de bloqueio avançado de conteúdo.

4 RESULTADOS E DISCUSSÃO

Com base nos estudos analisados, foi elaborado um comparativo entre as principais soluções identificadas na literatura e a proposta desenvolvida neste trabalho. A Tabela 1 apresenta a síntese das características de cada abordagem, destacando a arquitetura empregada, as principais funcionalidades e as limitações identificadas.

Tabela 1 - Comparativo entre os trabalhos correlatos e o trabalho desenvolvido

Trabalho	Arquitetura	Funcionalidades	Limitações
FilterPlus (Babu; Kumar, 2014)	Local (extensão Chrome)	Bloqueio de conteúdo, cookies e scripts por domínio	Sem controle de tempo; sem persistência de dados
AI Parental Control (AI Parental Control, 2023)	Baseado em nuvem	Filtragem por IA; relatórios online	Requer conexão externa; coleta/processamento em servidores
<i>Betrayed by the Guardian</i> (Ali et al., 2020)	Diversas (comerciais)	Avaliação de segurança e privacidade de apps de controle parental	Falhas e vazamento de dados sensíveis em múltiplas soluções
Trabalho desenvolvido	Local (Manifest V3)	Bloqueio por listas, lista de sites permitidos, modo de estudo e histórico local	Foco no Chrome; não utiliza IA/filtragem semântica

Fonte: Do autor.

Após o desenvolvimento e a implementação da extensão de navegador proposta, foram realizados testes técnicos no Google Chrome, visando avaliar sua estabilidade, desempenho e conformidade com os requisitos definidos. A análise dos resultados permitiu discutir o funcionamento da ferramenta à luz da literatura, bem como compará-la com outras soluções de controle parental.

Os testes funcionais verificaram o bloqueio por listas, a aplicação das regras dinâmicas (DNR), o funcionamento do histórico local e a execução do modo de estudo nos horários programados. Os testes de usabilidade foram realizados de forma exploratória por três participantes, que avaliaram clareza, navegabilidade e coerência visual da interface, considerando a adaptação automática ao tema do navegador. Já os testes de comportamento acompanharam o uso da extensão ao longo de cinco dias, observando a persistência das configurações, a estabilidade do service worker e a consistência de bloqueio das regras dinâmicas.

No que diz respeito à interface, observou-se que a adaptação automática ao tema do navegador proporcionou uma experiência visual coerente e confortável, integrando-se de forma natural ao ambiente de navegação. A organização dos elementos na página principal, dividida em seções de “Listas de bloqueio”, “Listas de permissão” e “Modo de estudo”, favore-

ceu a compreensão e a navegação. O design responsivo e os contrastes adequados atenderam às diretrizes de acessibilidade e usabilidade descritas por Ferreira, Santos e Carvalho (2022) e Mahmood e Maqbool (2021), reforçando a importância da clareza e da simplicidade em ferramentas de mediação digital.

A análise funcional indicou que o modo de estudo representou um diferencial relevante da proposta. Esse recurso permitiu configurar períodos específicos em que apenas sites previamente autorizados permaneceram acessíveis, bloqueando automaticamente os demais, fora dos intervalos definidos. Essa abordagem não foi observada em soluções correlatas como o *FilterPlus* (Babu; Kumar, 2014) ou o *AI Parental Control* (AI Parental Control, 2023), que dependiam de conexão com servidores externos. A execução totalmente local, sem necessidade de login ou autenticação, reforçou o compromisso com a privacidade do usuário, em conformidade com as boas práticas destacadas por Rahman, Baggili e Liu (2023) e Alenezi e Alshehri (2021).

Durante as medições de desempenho, verificou-se que o tempo médio de resposta entre a detecção de uma regra de bloqueio e a interrupção do carregamento da página foi inferior a 100 milissegundos, garantindo uma experiência fluida e sem atrasos perceptíveis. Esse resultado confirmou a eficiência do processamento declarativo adotado pelo Manifest V3, que executa as regras diretamente no navegador sem dependência de scripts externos (Developers, 2023). Avaliou-se ainda a persistência dos dados armazenados localmente, confirmando que as configurações de listas, histórico e modo de estudo foram mantidas após o encerramento e reabertura do navegador, validando a confiabilidade do uso do *localStorage*.

A Figura 2 apresenta a página principal de configurações da extensão, onde o responsável pode habilitar ou desabilitar a proteção, definir o modo de filtragem e gerenciar as listas de sites bloqueados e sites permitidos. Essa interface centraliza as principais opções de controle, com destaque para a organização visual e a clareza das instruções exibidas ao usuário.

Figura 2 - Interface principal da extensão – Página de configurações

The image shows the main configuration page of the extension, divided into four panels:

- Lista de Bloqueados** (Em uso): Sites bloqueados (usado no modo Bloquear lista). Input field: ex: youtube.com. Button: Adicionar. List: chatgpt.com, youtube.com (each with a red X icon).
- Lista de Permitidos**: Sites permitidos (usado no modo Permitir lista). Input field: ex: escola.gov.br. Button: Adicionar. List: escola.gov.br, unesc.net (each with a red X icon).
- Categorias** (Em uso): Ative categorias para incluir listas prontas de domínios na sua lista de bloqueados. List of categories with checkboxes and 'Ver' buttons: Redes Sociais (10 domínios • 1 permitido), Plataformas de jogos (10 domínios), Conteúdo Adulto e Violência (10 domínios), Inteligência Artificial (10 domínios • 1 permitido), Video & Streaming (10 domínios).
- Proteções de busca (Google)** (Em uso): Essas proteções valem para qualquer pesquisa no Google. List of search protections with checkboxes: Bloquear Imagens (Google Imagens), Bloquear Vídeos (Google Vídeos e Vídeos curtos), Forçar SafeSearch (checked).

Fonte: Do autor.

A Figura 3 apresenta o popup da extensão, acessado diretamente pelo ícone do navegador. O usuário pode adicionar o site atual à lista de bloqueados de forma rápida, sem precisar abrir a página completa de configurações. Antes de aplicar qualquer modificação, o sistema solicita a senha de autenticação cadastrada, garantindo que apenas o responsável autorizado possa alterar ou desabilitar as proteções. A ilustração apresenta o popup nas versões de tema claro e escuro, demonstrando a adaptação automática da interface ao modo definido no navegador. Essa abordagem reforça a integração visual e a consistência estética da ferramenta.

Figura 3 - *Popup* de acesso rápido à configuração de bloqueio

The image shows the quick access popup of the extension, presented in two versions: light theme (left) and dark theme (right).

Controle Parental (Habilitado):

Modo de filtragem: Bloquear lista (padrão)

Bloqueia os sites que você adicionar à lista de bloqueados. O restante abre normalmente.

Adicionar site atual à lista de BLOQUEADOS

Abrir página de Configurações

Fonte: Do autor.

A Figura 4 demonstra tela de configuração do modo de estudo, responsável por definir os horários em que apenas sites permitidos podem ser acessados. Esse recurso possibilita o controle do tempo de uso, auxiliando na criação de hábitos digitais equilibrados durante os períodos de estudo.

Figura 4 - Configuração do modo de estudo com horários programáveis

Modo Estudo

Em uso

Durante o horário programado, tudo é bloqueado, exceto os sites que você colocar em permitidos durante o estudo.

☒

Ativar Modo Estudo

Início

18:00

Fim

20:00

☐ Dom

☒ Seg

☒ Ter

☒ Qua

☒ Qui

☒ Sex

☐ Sáb

Sites permitidos durante o estudo:

ex: escola.gov.br, unesc.net

Adicionar

unesc.net

Fonte: Do autor.

Por fim, a Figura 5 apresenta o módulo de histórico local, que registra os acessos classificados como “permitido”, “bloqueado” e “suspeito”. O histórico inclui filtros dinâmicos e descrições informativas sobre o motivo de cada registro, oferecendo uma visão detalhada da navegação monitorada, sem recorrer a servidores externos.

Figura 5 - Histórico local com filtros e registros categorizados

Histórico local

Pesquisar...

Todos

Limpar histórico

10/11/2025, 01:25:01	Bloqueado	www.midjourney.com/	Bloqueado: Tentou acessar o site bloqueado (Midjourney).
10/11/2025, 01:24:55	Suspeito	www.google.com/search?q=midjourney&gs_lcrp=EgZigHJybwUyDagAEEUYORixAxiABDIHCAEQABiABDIHCAIQABiABDIHCAMQABiABDIKCAQQAB_	
10/11/2025, 01:24:36	Bloqueado	www.netflix.com/watch/80194276?trackId=155573560	
10/11/2025, 00:00:56	Permitido	term.ooo/?f=I1NDMzMD	
09/11/2025, 14:39:25	Permitido	ava.unesc.net/course/view.php?id=30222	
09/11/2025, 14:39:24	Permitido	ava.unesc.net/my/	
09/11/2025, 14:39:18	Permitido	ava.unesc.net/course/view.php?id=30222	
09/11/2025, 14:39:09	Permitido	ava.unesc.net/my/	
09/11/2025, 14:39:06	Permitido	ava.unesc.net/login/index.php	
09/11/2025, 14:39:03	Permitido	www.unesc.net/ava	

Fonte: Do autor.

De forma geral, os resultados comprovaram que a extensão atendeu plenamente aos requisitos definidos. O sistema operou com estabilidade, bloqueou corretamente os sites configurados, registrou o histórico local e executou o modo de estudo de acordo com os horários programados. Além disso, a comparação com os trabalhos correlatos evidenciou que a solução proposta superou limitações comuns, como dependência de servidores externos e complexidade de configuração. Desta forma, a ferramenta demonstrou viabilidade técnica e segurança para uso doméstico, consolidando-se como uma alternativa eficaz e acessível para o controle parental baseado em execução local.

5 CONCLUSÃO

O desenvolvimento da extensão de navegador para controle parental alcançou os objetivos propostos, apresentando uma solução funcional, local e segura para o gerenciamento do uso da internet por crianças e adolescentes. A ferramenta demonstrou a implementação de um sistema de controle eficiente diretamente no navegador, sem a necessidade de servidores externos, garantindo a privacidade dos dados e a autonomia do usuário.

A arquitetura baseada no Manifest V3 do Google Chrome proporcionou um ambiente seguro e previsível para execução das regras de bloqueio, utilizando a API *declarativeNetRequest* para interceptar solicitações de rede de forma eficiente. O armazenamento local das configurações (*localStorage*) assegurou a persistência das preferências, listas e histórico, mesmo após o encerramento do navegador, eliminando a necessidade de autenticação remota ou sincronização com serviços externos.

Durante a validação técnica, a extensão apresentou desempenho estável, tempo de resposta rápido e funcionamento consistente nas funcionalidades principais, bloqueio de sites, registro de histórico, gerenciamento de listas, categorias e modo de estudo. A autenticação por senha mostrou-se eficaz para restringir o acesso às configurações, reforçando a segurança do sistema. O histórico local, dividido em categorias de sites “permitidos”, “bloqueados” e “suspeitos”, permitiu ao responsável acompanhar de forma clara os acessos e tentativas de navegação a conteúdos restritos, sem expor informações a terceiros. As categorias automáticas e o módulo de proteção de busca, com bloqueio de Google Vídeos, Google Imagens e aplicação do *SafeSearch*, ampliaram o nível de controle e adequação do ambiente de navegação, tornando a ferramenta robusta e

confiável.

Os resultados confirmaram a viabilidade técnica e a usabilidade da extensão, que cumpriu os requisitos de segurança, acessibilidade e operação local. A interface adaptável, desenvolvida em HTML, CSS e JavaScript, proporcionou uma experiência coerente e confortável, ajustando-se automaticamente ao tema claro ou escuro do navegador e facilitando o uso por diferentes perfis de usuários.

Embora os resultados sejam satisfatórios, algumas limitações foram identificadas e serão consideradas em trabalhos futuros. Entre elas, destacam-se a ausência de um mecanismo para alteração de senha, a possibilidade de desativação manual da extensão pelo próprio navegador e o fato de o modo de estudo não encerrar automaticamente as guias abertas quando inicia o período de bloqueio.

Além dessas melhorias, propõe-se a integração de mecanismos de verificação de certificados digitais (SSL/TLS), com o objetivo de identificar e bloquear automaticamente domínios que utilizem certificados inválidos, expirados ou não confiáveis. Essa funcionalidade poderá reforçar a proteção contra sites maliciosos e ataques de *phishing*, ampliando o nível de segurança da navegação.

Outra possibilidade de evolução consiste na implementação de um painel analítico para visualização de estatísticas do histórico local, como número de bloqueios, acessos permitidos e ocorrências suspeitas, a fim de fornecer ao responsável uma visão mais abrangente do uso da ferramenta. Também se sugere a criação de um sistema de classificação dinâmica de risco, capaz de gerar alertas preventivos com base em padrões de navegação.

Por fim, futuras versões poderão explorar mecanismos de sincronização segura entre dispositivos mediante criptografia local, permitindo o gerenciamento unificado de múltiplos navegadores em diferentes máquinas, sem comprometer a privacidade ou depender de servidores externos.

REFERÊNCIAS

AI Parental Control. **AI Parental Control: Harness the Power of AI for Safer Browsing**. 2023. Chrome Web Store.

ALENEZI, M.; ALSHEHRI, M. **Security and privacy concerns in browser extensions: A systematic literature review**. IEEE Access, 2021, v. 9, p. 124680–124695.

- ALI, S. et al. **Betrayed by the guardian: Security and privacy risks of parental control solutions.** arXiv preprint arXiv:2012.06502, 2020.
- ASLAN, S.; METE, S.; ÖZEL, **A review of parental control technologies and children's online safety.** Security and Privacy, 2020, v. 3, n. 1.
- BABU, B.; KUMAR, M. **Filterplus: A real-time content filtering extension for google chrome.** arXiv preprint arXiv:1407.3820, 2014.
- BHANARKAR, N.; PAUL, A.; MEHTA, A. **Responsive web design and its impact on user experience.** International Journal of Advanced Research in Science, Communication and Technology, 2023, v. 3, n. 4.
- CORTESI, S.; GASSER, U. **Youth and digital citizenship in a data-driven world.** Youth and Media, Berkman Klein Center, 2020.
- DEVELOPERS, G. **Chrome Extensions Documentation.** 2023.
- FERREIRA, L.; SANTOS, M.; CARVALHO, T. **Acessibilidade digital em interfaces web: Práticas, desafios e oportunidades.** Revista Brasileira de Informática na Educação, 2022, v. 30, n. 2, p. 1–15.
- FOUNDATION, M. **Security practices for firefox extensions.** 2024.
- GROSSE, E.; UPADHYAY, U. **Security and privacy in the chrome browser.** IEEE Internet Computing, 2020, v. 24, n. 1, p. 64–71.
- KABALI, H. K. e. a. **Exposure and use of mobile media devices by young children.** Pediatrics, 2015, v. 136, n. 6, p. 1044–1050.
- LEE, K.; KWON, D.-H. **Controlled access to web resources using declarative netrequest api in chrome extensions.** Software: Practice and Experience, 2021, v. 51, n. 4, p. 895–909.
- LIU, W.; KOMLODI, A.; YESILADA, Y. **Design considerations for parental control tools: A case study.** International Journal of Human-Computer Studies, 2021, v. 150, p. 102610.
- LIVINGSTONE, S. et al. **In the digital home, how do parents support children and who supports them?** London School of Economics and Political Science, 2019.
- MAHMOOD, A.; MAQBOOL, N. **Usability assessment of browser-based security tools: A framework proposal.** International Journal of Human–Computer Interaction, 2021, v. 37, n. 6, p. 570–582.
- MASCHERONI, G.; ÓLAFSSON, K. **Parental mediation of children's internet use in Europe: A review of the evidence.** In: Global Kids Online Working Paper. [S.l.: s.n.], 2017.
- MOGHADDAM, M.; SAMADI, P.; KHONSARI, A. **Secure content filtering using browser extension-based sandboxing.** Computer Standards Interfaces, 2022, v. 82, p. 103626.

PAUDEL, P.; SUBEDI, M.; GHIMIRE, B. **An enhanced parental control system based on time and content filtering**. International Journal of Computer Applications, 2020, v. 176, n. 25, p. 1–6.

RAHMAN, M. T. H.; BAGGILI, I.; LIU, Q. **A large-scale empirical analysis of browser extension permissions and security risks**. Digital Investigation, 2023, v. 44, p. 301413.

SHARMA, K.; MEHTA, D. **Dynamic web content filtering using browser-based solutions**. International Journal of Web Semantic Technology, 2022, v. 13, n. 1, p. 1–14.

STATCOUNTER. **Browser Market Share Worldwide - April 2024**. 2024.

UPADHYAY, U.; GROSSE, E. **Overview of the chrome extensions platform: Manifest v3 and security improvements**. Google Security Blog, 2020.

W3C. **WebExtensions Community Group**. 2023.

WANG, G. et al. **Protection or punishment? relating the design space of parental control apps and perceptions about them to support parenting for online safety**. arXiv preprint arXiv:2109.05347, 2021.