FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Daniel Dias Alves Ferreira

Matheus Lisbôa Pereira

Vyctor Kawan Destro Machado

CRIANÇAS NA INTERNET

Exposição a riscos cibernéticos

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Daniel Dias Alves Ferreira

Matheus Lisbôa Pereira

Vyctor Kawan Destro Machado

CRIANÇAS NA INTERNET

Exposição a riscos cibernéticos

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Prof. Esp. José William Pinto Gomes

Área de concentração: Segurança da Informação.

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

FERREIRA, Daniel Dias Alves

Crianças na internet: exposição a riscos cibernéticos. / Daniel Dias Alves Ferreira, Matheus Lisbôa Pereira, Vyctor Kawan Destro Machado – Americana, 2025.

56f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. José William Pinto Gomes

1. Redes sem fio 2. Redes virtuais 3. Responsabilidade social. I. FERREIRA, Daniel Dias Alves, II. PEREIRA, Matheus Lisbôa, III. MACHADO, Vyctor Kawan Destro IV. GOMES, José William Pinto V. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681519
681519
316.7

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Daniel Dias Alves Ferreira

Matheus Lisbôa Pereira

Vyctor Kawan Destro Machado

Crianças na internet: exposição a riscos cibernéticos

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da informação.

Americana, 03 de dezembro de 2025.

Banca Examinadora:

José William Pinto Gomes
Especialista
Fatec Americana "Ministro Ralph Biasi"

Wagner Siqueira Cavalcante
Mestre
Fatec Americana "Ministro Ralph Biasi"

Diógenes de Oliveira
Mestre
Fatec Americana "Ministro Ralph Biasi"

AGRADECIMENTOS

Agradecemos aos nossos colegas pela companhia durante o curso, tal qual aos nossos professores, pelos conhecimentos transmitidos.

“Nosso tempo passou, John…”

(Dutch van der Linde em
Red Dead Redemption)

RESUMO

O presente trabalho visa apresentar ao leitor as principais ameaças que as crianças e adolescentes correm ao acessar as redes sociais de maneira irrestrita e não supervisionada, listando-os ao longo dos capítulos e mostrando como tais ameaças podem ser evitadas ou ao menos mitigadas. Em suma, o documento traz uma visão dos efeitos psiquiátricos, das redes sociais, por profissionais da saúde credenciados da área da psicologia. O capítulo introdutório conta com uma contextualização da cena atual, no ano de 2024, sobre como as redes sociais operam e como as crianças e adolescentes fazem seu uso, que servirá como um embasamento teórico ao tema para o leitor. Utiliza-se de um vasto número de artigos e monografias acadêmicas sobre os temas relacionados ao uso de redes sociais, as ameaças que apresentam à segurança digital dos usuários, para uma revisão bibliográfica, e também, a consulta à diversos psicólogos credenciados para o levantamento das consequências dessas plataformas digitais para a saúde dos agentes estudados. A estudo mostra uma clara explanação ao leitor, sobre os perigos que a falta de supervisão no uso de redes sociais apresenta a crianças, com o intuito de conscientizar pais, responsáveis e guardiões de menores de idade sobre a ideia de um uso adequado e seguro de redes sociais por parte das crianças brasileiras.

Palavras-chave: Redes Sociais; Engenharia Social; Riscos Cibernéticos; *Grooming*; *Pedofilia*;

ABSTRACT

This paper aims to present to the reader the main threats that children and adolescents face when having unrestricted and unsupervised access to social media platforms, listing them throughout the chapters and concluding on how these threats can be avoided or at least mitigated. In sum, the document will provide an overview of the psychiatric effects of social media by accredited health professionals in the field of psychology. The introductory chapter provides a contextualization of the current scene (2024) on how social media operate and how children and adolescents use them, which will serve as a theoretical basis for the topic for the reader. It will be used a vast number of articles and academic monographs on topics related to the use of social networks and threats that they present to the digital security of their users as a bibliographic review, such as the consultation of several accredited psychologists to survey the consequences of these digital platforms for the health of the studied agents. It is hoped the success of the project on clearly presenting to the reader of the dangers that the lack of supervision in the use of social networks presents to children, with the objective of raising awareness among parents, guardians and guardians of minors about the idea of appropriate and safe use of social networks by Brazilian children.

Keywords: *Social Media*; *Social Engineering*; *Cyber Risks; Grooming; Pedophilia*

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

Na sociedade moderna a necessidade de uso da tecnologia junto a internet tornou-se indispensável para a vida diária das pessoas, desde as ações mais simples como criar uma lista de compras ou ler notícias, até tarefas mais complexas como pagar contas, ter conversas a longa distância ou também saber se amanhã chove ou não. Quase tudo pode ser feito de maneira digital, e o que ainda não é possível, logo será. Nesse contexto de dependência, certos grupos são mais suscetíveis a ataques digitais, como pessoas menos instruídas, idosos e crianças, as quais vêm se tornando alvos cada vez mais fáceis para cibercriminosos que procuram nesses ambientes potenciais vítimas.

Bozzola et al. (2022) afirmam que, durante o "*lockdown*" da pandemia de Covid-19, a internet permitiu que muitas crianças e adolescentes mantivessem a comunicação e atividades acadêmicas de dentro de casa, o que foi uma excelente adaptação às condições adversas do isolamento social. Entretanto, esse acesso, muitas vezes irrestrito e não supervisionado por pais ou responsáveis, trouxe diversas adversidades que, até a data de publicação deste trabalho, ainda não são amplamente reconhecidas por pais e profissionais da educação.

Este trabalho visa demonstrar quais são essas adversidades, focadas em segurança da informação, a fim de conscientizar os mentores, dos riscos do acesso irrestrito de redes sociais por crianças.

Considera-se o projeto viável, visto a quantidade de trabalhos acadêmicos, artigos e monografias sobre o tema disponíveis para a revisão bibliográfica. Contamos também com as indicações do professor orientador, que possui um vasto contato com um público de pais e acadêmicos da área, que permitiu estudar e levantar dados sobre qual o conhecimento e preocupação dos mesmos em relação aos riscos sofridos por crianças na internet.

O objetivo geral do trabalho é demonstrar os possíveis riscos e nocividades que crianças estão correndo ao acessar de maneira irrestrita a internet.

As hipóteses são de que possíveis riscos como o *Cyberbullying* (uso da internet para efetuar assédios digitais com menores); Pedofilia digital (utilização da internet junto a *chats* digitais visando obter conteúdo de cunho erótico da menoridade); Publicação de informações privadas, trazendo a falta de conscientização e

monitoramento dos menores sobre quais tipos de informações podem ser publicadas e expostas a rede; Golpes digitais (quando criminosos manipulam crianças a entregar informações sigilosas ou dinheiro com técnicas de engenharia social simples). Esses possíveis riscos são os mais comuns e principais quando se trata das crianças no âmbito digital.

O percurso metodológico deste trabalho é uma pesquisa exploratória junto a revisões bibliográficas sobre redes sociais, cyber segurança e acesso digital precoce, trazendo dados de maneira quantitativa.

O trabalho está estruturado da seguinte forma: o Capítulo 1 apresenta o referencial teórico que fundamenta o estudo, abordando conceitos de segurança da informação, riscos digitais e comportamentos online. O Capítulo 2 traz a metodologia adotada e a análise dos dados obtidos pelo questionário aplicado a 131 participantes, permitindo compreender a percepção social sobre os riscos digitais enfrentados por crianças e adolescentes. Por fim, o Capítulo 3 trata sobre as considerações finais, sintetizando os principais achados e deixando clara a importância de ações coletivas e educativas voltadas à segurança digital infantil.

1 FUNDAMENTAÇÃO TEÓRICA

1.1 Riscos Cibernéticos.

Na sociedade atual pessoas de todas as faixas etárias estão constantemente conectadas à internet, seja utilizando celulares, computadores ou outros dispositivos. Esses acessos ocorrem diariamente, e cerca de 94,6% da população brasileira acessa a internet todos os dias da semana (CETIC.br, 2023). Por conta disso, existe um enorme tráfego de informações da população sendo constantemente acessadas, manipuladas, armazenadas e compartilhadas.

Levando esse tráfego de informações em consideração, dados, que muitas vezes podem vir a ser sigilosos, estão expostas as vulnerabilidades presentes nesse ambiente. De acordo com Santos (2019), vulnerabilidades são fraquezas que, quando exploradas, trazem algum prejuízo, dano ou perturbação. A exploração dessas falhas é definida como uma ameaça, e o risco seria a possibilidade dessa ameaça se tornar real.

Um exemplo de ameaça a essas informações seria a exposição de dados pessoais ou sigilosos, como por exemplo o vazamento de chaves PIX relatado pelo Banco Central em 2022, quando 137.285 chaves PIX atreladas à empresa Abastece Aí foram vazadas.

Roubos ou golpes realizados online são outro exemplo, sendo que, de acordo com pesquisas feitas pela empresa Kaspersky (2022), o Brasil foi o país que mais sofreu ataques *phishing* (Phishing é uma fraude online onde criminosos usam engenharia social para enganar vítimas e roubar dados sensíveis, como senhas, números de cartão de crédito e informações bancárias) através do Whatsapp, e ficou na quarta posição do *ranking* mundial desse mesmo tipo de ataque nas plataformas de e-mail.

Além desses exemplos, outras ameaças como *Ransomware*, roubo de identidade digital, entre outros estão presentes no ambiente virtual, fazendo com que todos seus usuários sejam vulneráveis. Esses ataques muitas vezes são imprevisíveis, e podem ter variadas motivações, como vingança, tentativa de obter um retorno monetário, ataques coordenados em massa ou até mesmo por prazer do

indivíduo por trás dos ataques. Seja qual for a motivação essas ameaças trazem consequências negativas e não devem ser ignoradas (Cannon, 2008).

1.2 Redes Sociais.

Redes sociais são estruturas sociais composta por um coletivo de pessoas que compartilham um interesse, valor, objetivo ou visão e se relacionam de maneira horizontal e de maneira hierárquica e não hierárquica, ou seja, onde qualquer pessoa interage com qualquer outra da rede de maneira independente, podendo ou não existir alguma figura de autoridade ou liderança.

Embora muito associada a plataformas digitais, as redes sociais, podem, sim ser off-line; uma igreja católica, por exemplo, pode ser considerada uma rede social, por se tratar de um conglomerado de pessoas que compartilham dos valores e ideais do cristianismo e interagem entre si sobre o assunto. Porém, o presente trabalho se refere apenas às redes sociais digitais, que surgiram no final do século XX e se popularizaram no começo dos anos 2000, e que hoje, são a forma de entretenimento e comunicação mais acessada do mundo. Em dado levantado por da Cruz (2020), plataformas como Facebook, WhatsApp, YouTube, Instagram, LinkedIn, X (anteriormente conhecido como Twitter) e Pinterest, são as mais utilizadas no Brasil, onde o habitante médio passa cerca de cinco horas por dia conectado à internet, e grande parte do tempo é gasto nesses canais. Somente o Facebook, a rede social mais usada no mundo, possui 129 milhões de contas ativas em solo brasileiro.

As redes sociais digitais não são somente um ambiente para divertimento e descontração dos usuários, como também uma ferramenta de trabalho, sendo usada principalmente para a divulgação de produtos ou serviços:

> “Em tempos mais recentes, o Marketing Digital está sendo cada vez mais utilizado por empreendedores. Acompanhando a internet, traz como objetivo principal aumentar a lucratividade e a popularidade da empresa (...) A vantagem em fazer Marketing Digital, é obviamente pelo grande número de pessoas que pode ser alcançado, se trabalhado de maneira correta tanto em sites, como em redes sociais. No Brasil, o número de *smartphones* que estão sendo usados já passam dos 76,1 milhões desde o terceiro trimestre de 2015.” (Nielsen, 2015). “Esses dados facilitam a percepção de que há uma grande possibilidade de se ter um serviço eficaz.” (Gomes, 2015, p.56).

1.3 Engenharia Social.

O termo “engenharia social” se refere à técnica utilizada por criminosos para enganar vítimas, buscando obter vantagens como informações confidenciais ou manipulando as mesmas a realizar ações que podem prejudicar o próximo, sempre alterando seus métodos de ataque conforme compreende mais o alvo e chega mais próximo ao objetivo:

> “A engenharia social é um método muito eficaz, resume em basicamente enganar a vítima, criar uma familiaridade, abusando da sua inocência e da confiança, o atacante consegue explorar várias áreas do sentimento humano para fazer o ataque, como por exemplo, a curiosidade, onde a vítima recebe um link e por curiosidade e inocência acaba entrando no link sem saber que se trata de um link malicioso, muitas vezes em uma empresa, o atacante escolhe como alvo algum funcionário que tem acesso ao sistema, através de várias ferramentas e métodos, conseguindo assim adquirir informações que podem dar acesso ao sistema.” (Tieso e Santo, 2020).

De acordo com a empresa Kaspersky (2022), o Brasil é o principal país atacado na América Latina por métodos de *phishing*, seja com mensagens enviadas por e-mail ou SMS e principalmente por redes sociais ou Whatsapp. Quando a atenção é totalmente direcionada para o quesito tecnológico, o principal pilar, que é o ser humano, acaba sendo deixado de lado, mesmo sendo o maior fruto de exposição de dados e o lado mais fácil de ceder por conta de falta de treinamento ou conscientização.

Mesmo sendo um termo de extrema importância, visando ambientes corporativos com *whaling* (Whaling (ou "pesca de baleias") é um tipo altamente direcionado de phishing que ataca exclusivamente executivos de alto nível), até para ambientes cotidianos com golpes de *phishing.* Até mesmo profissionais de TI não possuem completo conhecimento desta arte antiga ou negligenciam pensando que nunca passarão por um ataque desse, porém, a falta de preparo traz perdas enormes. A empresa CERT.br publicou uma estatística em seu site com o título Páginas Falsas Utilizadas em Tentativas de *Phishing* (2023), onde são retiradas estatísticas de um sistema de acompanhamento monitorado por analistas onde se nota que em 2023, o número de páginas falsas que foram notificadas para os analistas da CERT.br é de 10.923, sendo 7422 dessas afetando empresas no Brasil.

1.4 Definição legal de “criança”.

Segundo a Lei Federal Nº 8.069, de 13 de julho de 1990, popularmente conhecida como ECA, (Estatuto da Criança e do Adolescente), uma criança é definida como qualquer pessoa de até 12 anos de idade incompletos, o que gera o entendimento de que, no Brasil, qualquer ser humano que possua até 11 anos, 11 meses e 29 dias de idade é considerado para todos os fins judiciais uma “criança”, independentemente de qualquer outro fator. A lei também diz que qualquer pessoa de idade entre 12 e 18 anos incompletos é considerado um “adolescente”.

A ONU (Organização das Nações Unidas), também possui uma definição clara do que é considerado uma “criança”, que, segundo a Convenção sobre os Direitos da Criança, ocorrida na Assembleia Geral da ONU em 20 de novembro de 1989, destaca como “criança” qualquer ser humano com menos de 18 anos de idade completos, em exceção de quando em conformidade com a lei aplicável à criança, a maioridade seja alcançada antes.

Embora a definição de “criança” do órgão mundial seja divergente da lei nacional, para os devidos fins, o presente trabalho considerará a definição existente na lei brasileira.

2 ANÁLISE E DISCUSSÃO DOS DADOS

2.1 Levantamento de Dados

A coleta de dados foi realizada entre os meses de setembro e outubro de 2025 por meio de um questionário on-line elaborado na plataforma Google *Forms*, aplicado a 131 participantes de diferentes faixas etárias, gêneros, níveis de escolaridade e condições parentais (pais e não pais). O objetivo da pesquisa foi analisar o nível de conhecimento e a percepção dos adultos quanto aos riscos que as crianças enfrentam ao utilizar a internet de maneira irrestrita.

Os participantes residem predominantemente na Região Metropolitana de Campinas (incluindo cidades como Americana, Limeira e Piracicaba), bem como em outros estados brasileiros. A divulgação do formulário foi feita pelos meios digitais e presenciais, principalmente por redes sociais e contatos diretos com colegas, alunos e conhecidos. Esse formato misto de divulgação foi utilizado com a intenção de ampliar o alcance geral da pesquisa e garantir maior diversidade dentro da amostra.

O questionário foi elaborado de forma a preservar o anonimato dos respondentes, pontuando que todos participaram de maneira voluntária e consentida. O objetivo é coletar dados sobre a percepção e o conhecimento dos participantes quanto aos riscos digitais enfrentados por crianças. Nele havia perguntas fechadas e de múltipla escolha, organizadas em quatro pilares principais:

1. Perfil sociodemográfico, abordando gênero, faixa etária, escolaridade e localidade;
2. Condição parental, investigando se o participante possui filhos e quantos;
3. Percepção individual de conhecimento e relevância sobre riscos digitais infantis;
4. Hierarquia de ameaças percebidas, contemplando aspectos sociais, psicológicos, técnicos e financeiros do ambiente on-line.

Os dados levantados foram analisados de forma quantitativa e descritiva, buscando identificar padrões de comportamento e percepção entre os participantes. Para complementar a análise, foi utilizada a interpretação qualitativa, relacionando respostas às teorias apresentadas na fundamentação teórica.

A utilização do Google *Forms* possibilitou abrangência e facilidade de acesso para os participantes, além de reduzir erros de transcrição, automatizar a consolidação das respostas e agilizar a tabulação dos dados. Embora a amostra não represente a população como um todo, ela fornece indicativos relevantes sobre o comportamento digital de adultos e jovens instruídos.

2.2 Dados Levantados no questionário

O questionário contou com onze questões, que visam reconhecer o perfil demográfico dos participantes e especialmente, o que eles consideram nocivos as crianças na internet, e em que grau.

2.2.1 Reconhecimento de riscos específicos

A questão mais importante do questionário, a décima primeira questão do formulário visa analisar e classificar a grande escala quais são os riscos que os entrevistados consideram mais nocivos e perigosos no ambiente virtual. Cada entrevistado poderia escolher até cinco opções dentre as seguintes:

1. Pedofilia - Ameaças, humilhações e violência de cunho sexual contra crianças.
2. Compras não autorizadas - Uso de cartões cadastrados para compras em jogos ou aplicativos sem permissão dos pais.
3. Contatos com desconhecidos - Risco de interação com predadores virtuais, golpistas ou pessoas mal-intencionadas.
4. Sexualização precoce - Exposição de crianças a conteúdos, estímulos ou comportamentos sexuais antes da idade adequada.
5. Exposição a conteúdo impróprio - Acesso a imagens, vídeos ou textos inadequados para a idade, como violência ou pornografia.
6. *Ciberbullying* - Ameaças, humilhações e ofensas feitas online por outras crianças ou adolescentes
7. Vazamento de dados pessoais - Crianças podem compartilhar informações privadas sem perceber os riscos.

8. Dependência de telas - Uso excessivo da internet pode prejudicar o desenvolvimento social e emocional.
9. *Phishing* (sites falsos que imitam um site real) e golpes online - Crianças podem ser enganadas a fornecer dados ou clicar em links maliciosos.
10. Desafios perigosos e tendências virais - Participação em brincadeiras ou desafios que colocam a segurança em risco.
11. *Grooming* (Aliciamento Online) – Quando adultos mal-intencionados se passam por crianças para ganhar a confiança delas e manipulá-las.
12. Exposição à desinformação – Crianças podem acreditar em fake news, teorias da conspiração e informações falsas.
13. Desafios psicológicos – Comparação excessiva com influenciadores pode causar baixa autoestima e ansiedade.
14. Pressão para exposição – Influência para postar fotos e vídeos para ganhar curtidas e aceitação social.
15. Apostas e jogos de azar – Publicidade ou acesso fácil a sites de apostas pode incentivar comportamentos compulsivos.
16. Conteúdo extremista – Crianças podem ser expostas a discursos de ódio, ideologias radicais ou grupos extremistas.
17. Exploração financeira – Golpes que fazem crianças gastarem dinheiro em jogos ou assinaturas sem entender as consequências.
18. Roubo de identidade – Hackers podem roubar informações e usá-las para fraudes.
19. *Doxxing* (Exposição de Dados) – Vazamento de informações pessoais que podem levar a perseguições ou ameaças.
20. *Deepfake* e manipulação de imagens – Crianças podem ser vítimas de vídeos e fotos falsas que as envolvem.
21. *FOMO* (*Fear of Missing Out*) – Ansiedade causada pelo medo de estar perdendo algo que os outros estão fazendo online.
22. Exploração infantil – Risco de exploração sexual e tráfico infantil em plataformas online.
23. Influência de comportamentos autodestrutivos – Sites e fóruns que incentivam distúrbios alimentares, automutilação e até suicídio.
24. Desafios e brincadeiras perigosas – Algumas tendências virais incentivam atitudes arriscadas ou prejudiciais.

25. Ataques hackers – Crianças podem baixar vírus ou malwares sem perceber, colocando dispositivos e redes em risco.
26. Falsa sensação de anonimato – Pode levar a comportamentos inadequados, como cyberbullying e discurso de ódio.
27. Exposição a publicidade abusiva – Anúncios enganosos ou direcionados que podem influenciar decisões de consumo indevidas.

Esse dado é fundamental para reconhecer qual é o nível é a percepção dos entrevistados sobre o tema de segurança da informação para crianças, pois consegue ranquear quais são as maiores preocupações sobre o tema. A escolha de limitar a quantidade de itens que podem ser escolhidos é estratégica, pois visa limitar o pânico moral que alguns participantes podem ter sobre o tema, e evita que ele selecione todos os riscos que ele considera minimamente relevante, mantendo somente as principais ameaças

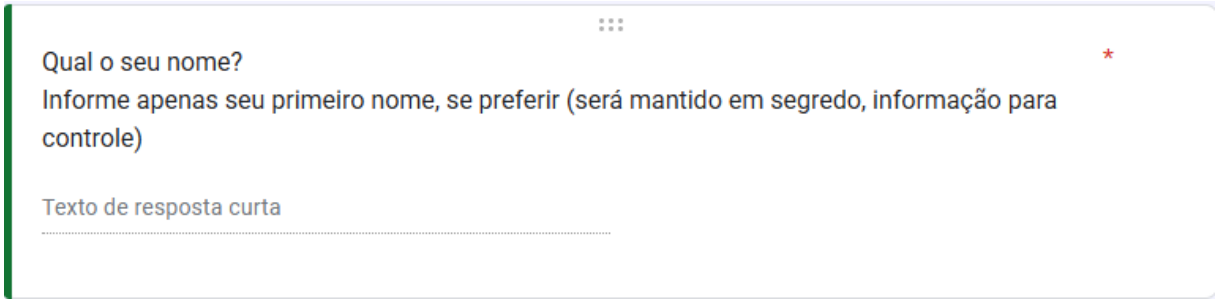
2.3 Perfil Sociodemográfico dos Respondentes

Antes de analisar as respostas, percepções e opiniões dos participantes é necessário compreender qual o perfil sociodemográfico do público que compõe a amostra da pesquisa. Essa caracterização dos participantes permite contextualizar os resultados e trazer uma interpretação mais precisa das informações coletadas.

A amostra total foi composta por 131 respondentes, cujo perfis variam entre gênero, faixa etária, nível de escolaridade e cidade onde residem.

A primeira pergunta da pesquisa, mostrada na Figura 1, solicita o nome do respondente, com o único e exclusivo intuito de manter o controle das informações. O questionário deixa claro que, o entrevistado pode, se quiser, fornecer apenas o primeiro nome, e que será mantido em total sigilo.

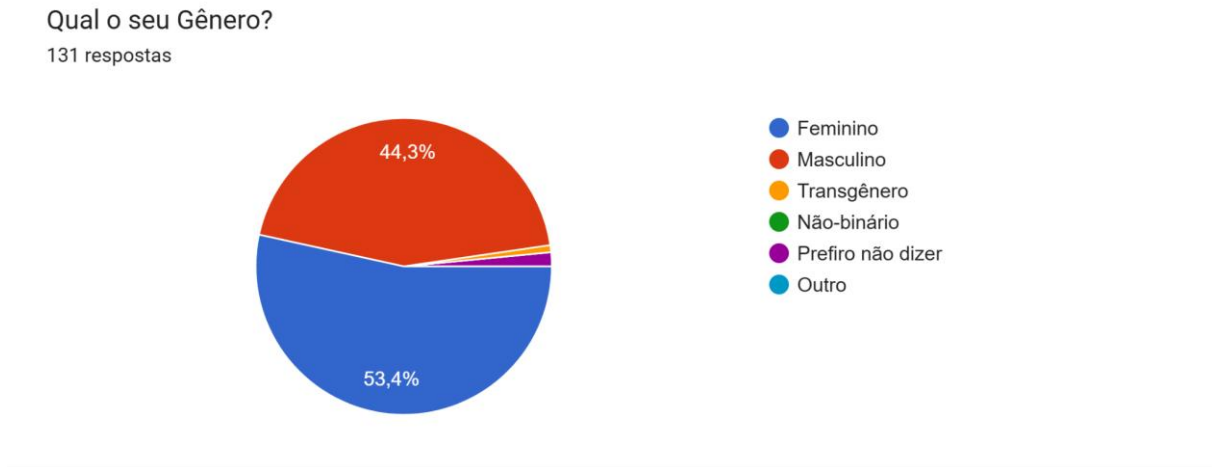
Figura 1 - Pergunta sobre o nome do entrevistado.



Fonte: Elaborado pelos autores (2025).

Em relação ao gênero dos participantes houve uma pequena diferença para a predominância feminina, observada na Figura 2, sendo 70 participantes, representando 53,4% dos respondentes. Tal proporção evidencia uma participação equilibrada entre os gêneros, embora com uma presença feminina levemente superior.

Figura 2 - Distribuição dos respondentes segundo o gênero.

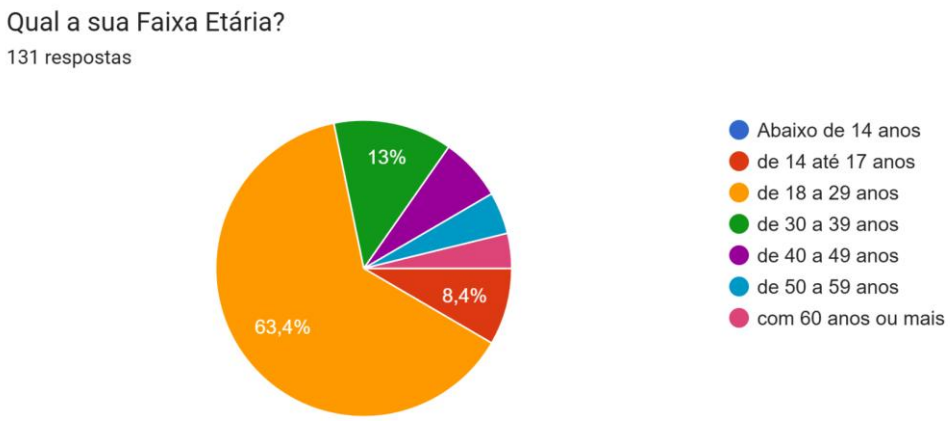


Fonte: Elaborado pelos autores (2025).

No que se refere a faixa etária, constatou-se uma grande concentração nos indivíduos entre 18 à 29 anos de idade, mostrado na Figura 3, correspondendo a 63,4% do total de respondentes. Essa diferença muito se dá por conta dos locais onde a pesquisa foi aplicada, pois grande parte dos respondentes são alunos da FATEC Americana.

O restante dos respondentes está dividido em pequenas parcelas nas demais faixas etárias apresentadas no formulário, totalizando nos 36,6% restantes.

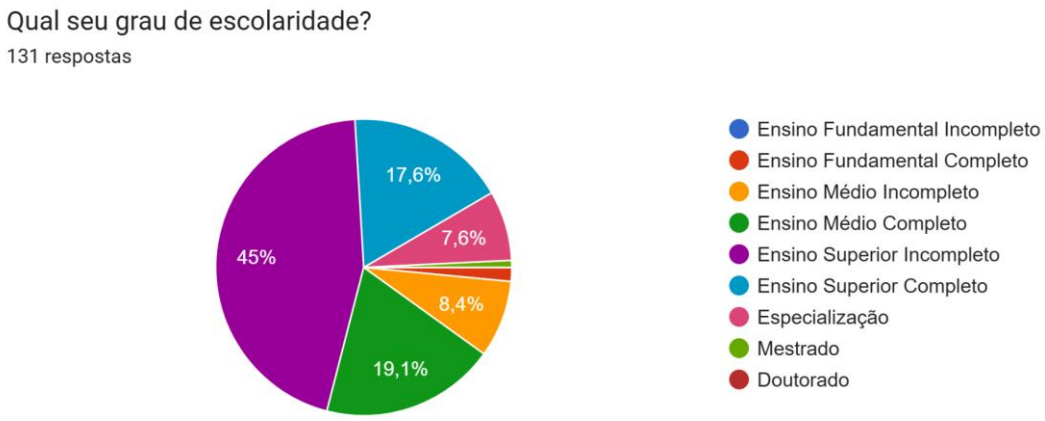
Figura 3 - Faixa etária dos respondentes.



Fonte: Elaborado pelos autores (2025).

Referente ao grau de escolaridade foi possível analisar uma predominância em participantes que estão cursando ou já concluíram o ensino superior, sendo que 45% dos respondentes têm o ensino superior incompleto ou cursando, enquanto 17,6% já concluiu o ensino superior, como visto na Figura 4. Assim como o resultado anterior, isso se dá por conta dos locais onde a pesquisa foi aplicada. Essa distribuição indica que grande parte dos respondentes está em um nível educacional elevado dentro da amostra analisada.

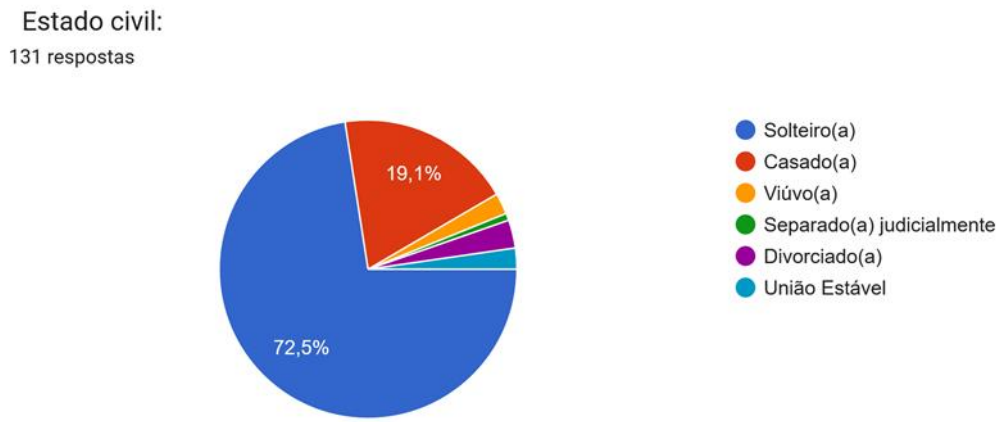
Figura 4 - Grau de escolaridade dos participantes da pesquisa.



Fonte: Elaborado pelos autores (2025).

Quanto ao estado civil dos participantes, apresentado na Figura 5, a maioria solteiros, atingindo 72,5% dos indivíduos que responderam, seguido de 19,1% de pessoas casadas, o restante, apenas 8,4% distribuídos entre as outras opções.

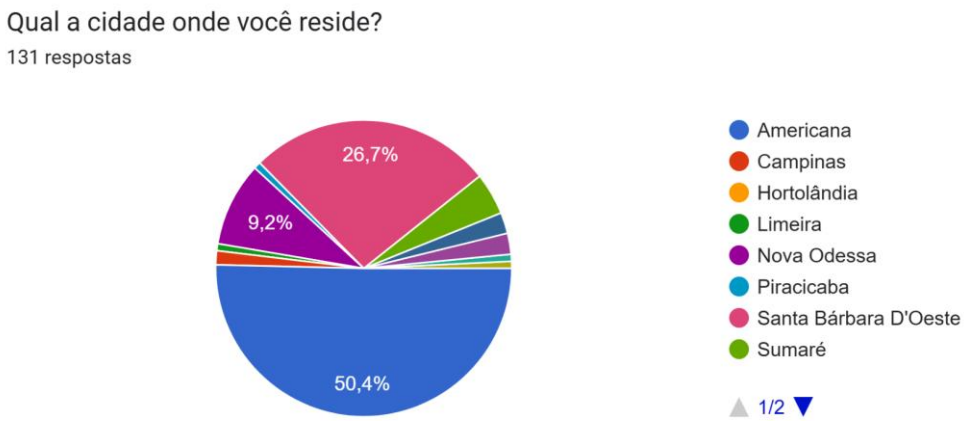
Figura 5 - Estado civil dos participantes.



Fonte: Elaborado pelos autores (2025).

Por fim, no quesito de localização geográfica há um foco regional na região metropolitana de Campinas, também por conta da área onde a pesquisa foi aplicada. Em grande maioria os respondentes são residentes da cidade de Americana, representando 50,4% dos respondentes, metade do público total. Os demais estão divididos em 26,7% de residentes de Santa Bárbara d'Oeste, e 9,2% moradores de Nova Odessa. Os demais respondentes são de cidades diversas e representam 13,7% do total. Como podemos conferir na Figura 6.

Figura 6 - Distribuição demográfica dos participantes.



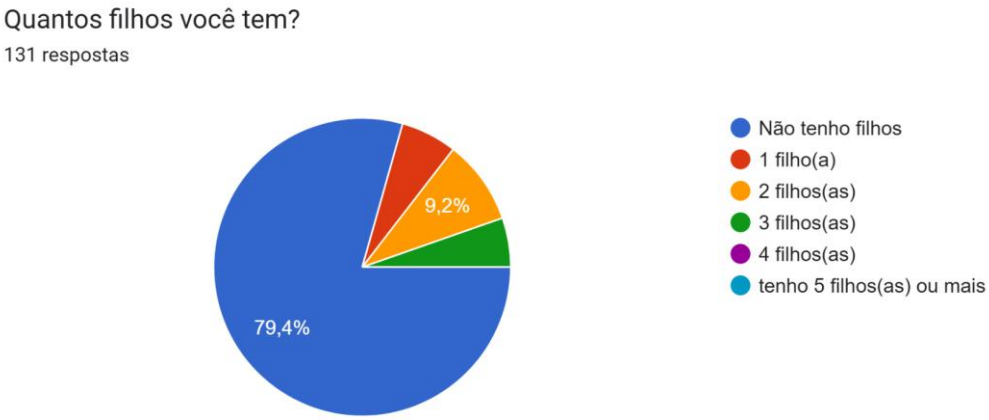
Fonte: Elaborado pelos autores (2025).

De modo geral, a análise sociodemográfica revela que o estudo reflete a percepção de um grupo majoritariamente jovem (18 a 29 anos), com alto nível de escolaridade (ensino superior em curso ou completo) e geograficamente concentrado no interior paulista. Essa caracterização é essencial para compreender as tendências observadas nas respostas, uma vez que fatores como idade, escolaridade e contexto regional influenciam diretamente as atitudes, comportamentos e percepções dos indivíduos diante dos temas abordados pela pesquisa.

2.4 A Lacuna entre Experiência Parental e Percepção de Risco

Os dados levantados na pesquisa expressam que a maioria dos respondentes não possui nenhum descendente direto, ou criança à qual seja um guardião legal, mostrado na Figura 7. Conforme o estudo feito, 104 respondentes não possuem filhos (79,4%), oito possuem um filho (6,1%), 12 possuem dois filhos (9,2%) e sete possuem três filhos (5,3%). Nenhum dos questionados possui quatro ou mais filhos.

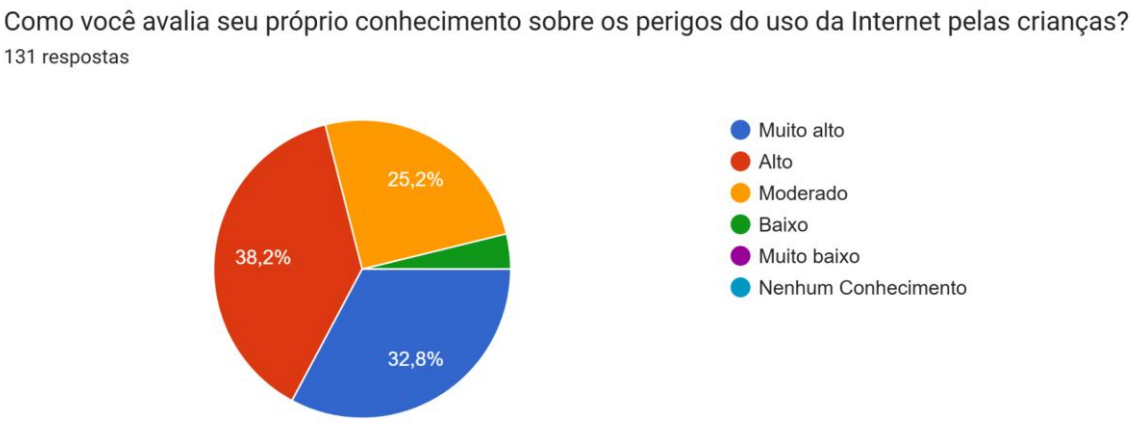
Figura 7 - Número de filhos declarados pelos participantes.



Fonte: Elaborado pelos autores (2025).

Todavia, o mesmo levantamento indica que 93 entrevistados, ou 71%, consideram o seu conhecimento sobre perigos do uso da internet por crianças como alto ou muito alto, de acordo com a Figura 8.

Figura 8 - Conhecimento sobre os perigos da Internet para as crianças



Fonte: Elaborado pelos autores (2025).

O levantamento indica uma clara adversidade do esperado, uma vez que a lógica indica que pessoas que não possuem nenhuma responsabilidade com manter um descendente em segurança no ambiente digital deveriam conhecer menos sobre os perigos nos quais eles correm on-line, entretanto, a sondagem de dados indica o exato oposto.

Prensky (2001) defende em seu artigo “Nativos Digitais, Imigrantes Digitais” a existência de dois tipos de pessoas no que se diz respeito à conectividade e habilidades com ferramentas digitais. Os “nativos digitais”, sendo aqueles que desde a infância estão cercados de computadores, aparelhos celulares, gravadores e reprodutores de áudios, câmeras digitais, dentre outros equipamentos tecnológicos, possuindo uma “habilidade nativa” com tais dispositivos. Tal assunção implica a existência de “imigrantes digitais”, sendo pessoas que não tiveram contato com tal tecnologia desde uma idade jovem, e tiveram que aprender a utilizá-las depois de adultos, possuindo uma grande dificuldade para tal, visto que estes instrumentos surgiram para substituir outros mais arcaicos no qual os imigrantes já possuíam afinidades.

Embora antigo, essa hipótese traçada por Prensky (2001), se mostrou extremamente verdadeira nos últimos 15 anos, principalmente com o surgimento da internet banda larga e fibra óptica além dos smartphones. Estudos futuros sobre a obra de Prensky (2001), sugerem que embora o fator geracional seja muito importante, não é determinante, visto que as pessoas têm a capacidade de se adaptar às novas realidades e ferramentas, mas fato é que as gerações Y, Z e Alfa (não contabilizada na pesquisa) possuem sim mais facilidade com as ferramentas e meios digitais.

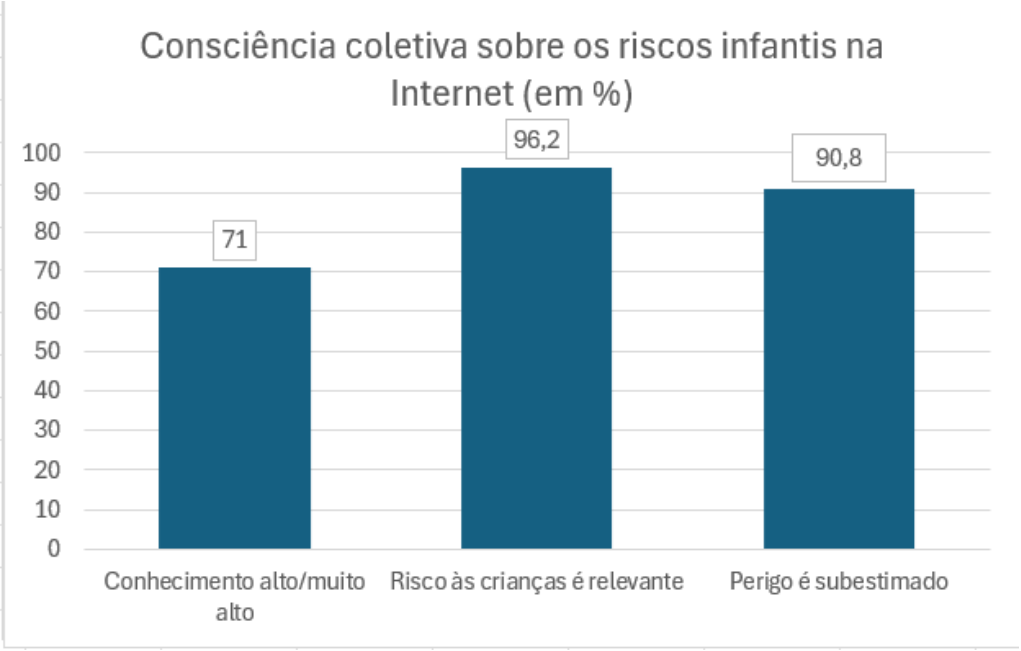
Essa hipótese se ajusta adequadamente aos dados da pesquisa de campo elaborada, visto que, as pessoas mais jovens, embora estatisticamente não possuam experiência parental, conhecem melhor os ambientes virtuais da internet, e por esse fato, tem mais repertórios sobre os possíveis perigos que crianças podem estar sendo submetidas lá.

2.5 A Consciência Coletiva: Relevância e Subestimação do Perigo.

A pesquisa aplicada revelou que a maioria dos respondentes demonstra consciência sobre os riscos que a internet representa para o público infantil. Entre os entrevistados, 71,0% afirmam possuir conhecimento alto ou muito alto sobre os perigos do uso da internet pelas crianças, enquanto 96,2% consideram o tema muito ou extremamente relevante. Em contradição, 90,8% concordaram que esses perigos para o escopo infantil são subestimados pela sociedade.

Conforme mostra a Figura 9, apesar da maioria dos usuários da internet reconhecerem que o ambiente digital apresenta riscos, observa-se uma diferença discrepante entre a percepção coletiva e as práticas de segurança realmente aplicadas.

Figura 9 - Consciência coletiva sobre os riscos digitais infantis.



Fonte: Elaborado pelos autores (2025).

Essa diferença, aqui denominada minimização social dos riscos digitais, representa um dos maiores desafios para a conscientização em Segurança da Informação.

A chamada consciência coletiva digital pode ser compreendida como o nível de entendimento social compartilhado sobre os perigos e responsabilidades associados ao ambiente virtual. Essa ideia reflete o que Castells (1999, p. 421) define como *"sociedade em rede"*, contexto em que o conhecimento circula de maneira ampla e descentralizada, mas nem sempre se converte em ações coletivas efetivas.

Nos últimos anos, o tema da segurança online recebeu maior espaço nas mídias e nos debates públicos, indicando que os usuários estão cada vez mais expostos a informações sobre golpes, vazamentos de dados e manipulação digital. Porém, esse avanço informacional não tem sido acompanhado de mudanças concretas de comportamento. Mesmo com campanhas educativas e alertas constantes, ainda é comum que usuários mantenham senhas frágeis, acessem links

suspeitos ou compartilhem dados pessoais de forma imprudente, evidenciando a distância entre a consciência do risco e as adoções efetivas de práticas seguras.

Essa contradição entre consciência e ação se torna ainda mais preocupante quando o público analisado envolve crianças e adolescentes, cuja imaturidade cognitiva e emocional as torna mais vulneráveis a comportamentos impulsivos e à falta de percepção de riscos. Segundo Bozzola et al. (2022), a exposição precoce e não supervisionada às redes sociais pode comprometer o discernimento, afetar desenvolvimento psíquico e facilitar interações potencialmente perigosas. Evidencia-se, portanto, que a ausência de uma consciência coletiva sólida sobre a segurança digital não somente colabora com comportamentos descuidados, mas também aumenta a vulnerabilidade infantil, reforçando a urgência de políticas e ações educativas que ultrapassem o campo individual e se consolidem socialmente por meio de escolas, famílias e instituições públicas.

Apesar da maioria dos participantes demonstrar compreender os riscos associados ao ambiente digital, os dados revelam um comportamento de inércia coletiva. A consciência sobre o perigo não se mostra em atitudes preventivas efetivas, evidenciando o que Bauman (2001), descreve como *modernidade líquida*, um cenário em que as responsabilidades são fragmentadas e as ações coletivas são vistas como raras. Como observa o autor, “a desintegração da rede social e a derrocada das agências de ação coletiva são tanto uma condição quanto resultado da nova técnica do poder” (BAUMAN, 2001, p. 18). Seguindo essa ideia, a análise do autor ajuda a compreender que, mesmo diante da consciência dos riscos digitais, prevalece a falta de ação conjunta: as responsabilidades se “diluem” e o engajamento comum enfraquece. Em contextos digitais, esse fenômeno é intensificado pela falsa sensação de controle pessoal transmitida pelas tecnologias, que cria uma ilusão de segurança e enfraquece o engajamento coletivo, impedindo que o saber sobre os riscos se converta em ação. Na prática, isso se manifesta em comportamentos como a ausência de diálogo entre pais e filhos sobre segurança digital ou a falta de políticas escolares que tratem o tema de forma sistemática.

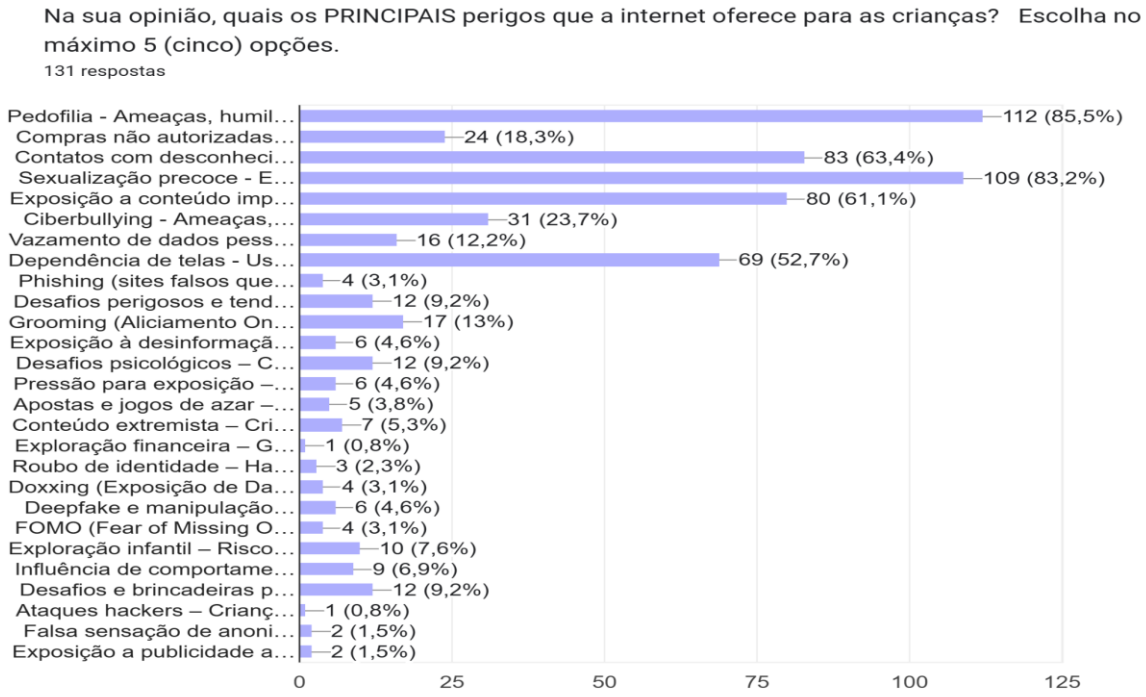
Em síntese, a consciência coletiva sobre os riscos digitais infantis se mostra existente, mas fragilizada pela ausência de ação conjunta. Na seção seguinte, busca-se compreender como essa percepção se reflete na hierarquia das ameaças mais

temidas pelos respondentes, ampliando o entendimento na amostra pesquisada sobre a forma como o público hierarquiza os perigos no ambiente digital.

2.6 Mapeamento dos Riscos: A Hierarquia das Ameaças Percebidas

A partir das respostas obtidas por meio do questionário, foi possível identificar uma clara hierarquia de preocupações entre os participantes da pesquisa. O gráfico apresentado na Figura 10, representa os principais perigos que os respondentes associam ao uso da internet por crianças, revelando a predominância de temores voltados às ameaças de natureza sexual e interativa, que ocupam as primeiras posições do ranking de preocupações mais recorrentes, as opções apresentadas no questionário podem ser conferidas no Apêndice A, ou, na Seção 2.2.1.

Figura 10 - Percepção sobre os principais perigos da Internet.



Fonte: Elaborado pelos autores (2025).

Entre os 131 participantes, 85,5% apontaram a pedofilia como o maior perigo, seguida pela sexualização precoce (83,2%) e pelo contato com desconhecidos (63,4%). Em segundo plano, aparecem os perigos relacionados ao desenvolvimento psicológico e social, como a exposição a conteúdo impróprio (61,1%), a dependência de telas e uso excessivo (52,7%) e o cyberbullying (23,7%). Por outro lado, os riscos

técnicos e financeiros, como vazamentos de dados pessoais (12,5%), *phishing* (3,1%), roubo de identidade (2,3%) e ataques hackers (0,8%) aparecem entre as menores preocupações registradas.

Essa distribuição das respostas mostra que os participantes tendem a classificar como mais graves os perigos mais visíveis e emocionalmente marcantes, especialmente os ligados à exposição sexual e às interações online com desconhecidos, que remetem ao medo do assédio e da exploração infantil, os perigos de caráter técnico ou financeiro são menos perceptíveis no cotidiano, recebendo menor atenção. Esse padrão sugere que, mesmo que a consciência sobre os perigos digitais seja alta, parte do público ainda associa o risco principalmente a ameaças externas e imediatas, enquanto demonstra menor atenção a vulnerabilidades cotidianas e comportamentos que também podem comprometer a segurança digital.

Essa hierarquia de percepções demonstra que o medo digital é construído mais pela visibilidade e pela carga emocional dos temas do que por um conhecimento técnico sobre segurança. Segundo Castells (1999, p. 421), “vivemos em um ambiente de mídia, e a maior parte de nossos estímulos simbólicos vem dos meios de comunicação”, e que “o poder real da televisão é armar o palco para todos os processos que se pretendem comunicar à sociedade em geral”. Assim, os perigos amplificados pelas narrações midiáticas ganham maior destaque social, enquanto riscos menos “noticiáveis”, como os de natureza técnica, permanecem em segundo plano.

É nesse cenário que se insere a análise a seguir, que aborda as Ameaças de Natureza Sexual e Interativa, classificada pelos participantes como os riscos mais graves no ambiente digital infantil.

2.6.1 Ameaças de Natureza Sexual e Interativa (O Alerta Máximo)

As ameaças de natureza sexual e interativa foram as mais selecionadas entre os participantes, apresentando os maiores índices de preocupação na pesquisa. Entre elas, destacam-se a pedofilia (85,5%), a sexualização precoce (83,2%) e o contato com desconhecidos (63,4%), configurando esse grupo de ameaças como sendo as mais alarmantes entre os respondentes. Esses resultados mostram que o pensamento coletivo sobre os perigos digitais está mais associado à exposição infantil e à interação com agentes externos com potencial predatório.

Conforme mostrado anteriormente, a visibilidade desses temas é aumentada por conta da comunicação social em conjunto com a mídia, que reforçam representações desses perigos a partir de casos extremos com narrativas de grande apelo emocional.

Essa predominância também se mostra nas narrativas públicas e nos casos de maior repercussão social. Um exemplo recente é o processo movido por uma mãe contra as plataformas Discord e Roblox, após seu filho de 15 anos sofrer abuso online e tirar a própria vida, conforme noticiado pela Globo (2025). A ampla abertura midiática desse caso reforça como esses episódios despertam indignação pública e promovem debates sociais, se estruturando como uma representação máxima do perigo digital.

Em contraste, outras formas de vulnerabilidade digital permanecem praticamente invisíveis. Dados divulgados pela Unicesumar (2024), apontam que o Brasil perde mais de R$ 25,5 bilhões por ano em golpes financeiros e, apesar do prejuízo individual, grande parte das vítimas não chega nem mesmo a registrar denúncia ou buscar reparação. Essa falta de reação revela uma cultura de banalização das perdas virtuais e de baixa percepção de risco diante de ameaças técnicas ou financeiras. Se muitos adultos negligenciam sua própria segurança digital e normalizam prejuízos financeiros online, é ainda menos provável que compreendam e valorizem a importância de proteger seus filhos de riscos menos tangíveis como os vazamentos de dados e coleta indevida de informações pessoais em plataformas infantis.

Essa diferença entre o que é amplamente noticiado e o que é silenciosamente vivido reforça o padrão identificado na pesquisa: a sociedade tende a superestimar os perigos com maior apelo emocional e visibilidade, enquanto subestima vulnerabilidades estruturais e persistentes do ambiente digital.

2.6.2 Riscos ao Desenvolvimento Psicológico e Social.

Entre os perigos apontados pelos participantes da pesquisa, os riscos de natureza psicológica e social aparecem numa posição intermediária na hierarquia de preocupações. A exposição a conteúdo impróprio (61,1%), a dependência de telas e uso excessivo (52,7%) e o *cyberbullying* (23,7%) foram os perigos mais citados dentro dessa categoria. Mesmo que sejam menos associadas a danos imediatos, essas ameaças produzem impactos considerados cumulativos, afetando o desenvolvimento

emocional, cognitivo e social das crianças, desde a construção da identidade até a capacidade de convivência e empatia no ambiente digital. Esses riscos se manifestam de maneira contínua e silenciosa, muitas vezes passando despercebidos pelos responsáveis, tornando sua identificação e mitigação mais complexa ainda.

A exposição a conteúdos impróprios vem se tornando um dos elementos mais recorrentes no ambiente digital infantil, representando uma ameaça ao desenvolvimento psíquico. Plataformas como Youtube, TikTok, Instagram e jogos online repetidamente misturam constantemente conteúdos informativos e materiais potencialmente inadequados, sendo comum que crianças encontrem, mesmo que acidentalmente, conteúdos violentos, sexualizados ou com discursos de ódio. Esse tipo de exposição pode causar dessensibilização emocional, ansiedade, medo e distorções na percepção de normas sociais, especialmente quando se repetem ao longo do tempo. Segundo Bozzola et al. (2022), esse tipo de conteúdo inadequado pode interferir na formação da identidade e impactar negativamente a compreensão infantil sobre sexualidade, relacionamentos e limites sociais.

Além dessa exposição, outro aspecto relevante dentro dessa categoria é a crescente dependência de telas, que já se consolidou como um comportamento comum entre crianças e adolescentes na última década. A pesquisa TIC Kids Online Brasil, NICBR (2023), traz diversos pontos relevantes sobre esse campo, apontando também que o uso da internet já faz parte da rotina da maioria dos jovens brasileiros, principalmente por dispositivos móveis. Esse uso contínuo e prolongado contribui para a criação de hábitos compulsivos e padrões comportamentais que afetam diretamente o desenvolvimento saudável, sendo um fenômeno observado pela literatura científica. Em um estudo, Twenge e Campbell (2018), identificaram que níveis altos de tempo de tela estão associados a maior distração, irritabilidade, dificuldades de concentração, piora da qualidade do sono e redução do bem-estar emocional geral, principalmente entre crianças em idade escolar.

Por sua vez, o *cyberbullying*, mesmo tendo sido mencionado por uma parcela menor de participantes (23,7%), representa um dos maiores riscos psicológicos do ambiente digital. Diferente de agressões físicas ou pessoais, o ataque virtual se caracteriza principalmente pela sua permanência, pelo alcance ampliado e essencialmente pela capacidade de ocorrer em anonimato, intensificando o impacto emocional para as vítimas. São várias possíveis vertentes que podem ser seguidas nesse campo, desde insultos, humilhações públicas, divulgação de boatos, edição de

imagens ou exposição de informações pessoais, que acabam acarretando em sentimento de insegurança, medo, vergonha e isolamento social. Crianças e adolescentes submetidos a essa violência costumam relatar maior vulnerabilidade emocional, dificuldades de convivência e queda no rendimento escolar, além de mais tendência a sintomas depressivos e ansiosos.

De modo geral, os riscos psicológicos e sociais analisados neste subcapítulo têm uma característica em comum: são silenciosos, progressivos e muitas vezes naturalizados dentro do ambiente digital. Como não acarretam em marcas físicas e muitas vezes são confundidos com comportamentos típicos da fase de desenvolvimento, podem ser negligenciados pelos responsáveis, dificultando sua identificação precoce. Esses fatores afetam a formação emocional e cognitiva, a construção da identidade de crianças e adolescentes, bem como as relações interpessoais e a maneira como elas percebem a si mesmas dentro do ambiente digital. Assim, compreender e reconhecer que são riscos fundamentais é essencial para efetuar mediações mais ativas e conscientes dos responsáveis, estabelecer limites, acompanhar conteúdos consumidos e incentivar práticas digitais mais saudáveis.

Após compreender os riscos emocionais e sociais, torna-se essencial abordar outro conjunto de ameaças igualmente relevantes: os riscos técnicos e financeiros associados ao ambiente digital, que compõem o terceiro eixo de preocupações identificado na pesquisa.

2.6.3 Riscos Técnicos e Financeiros: A Percepção Secundária

A pesquisa também evidencia um conjunto de ameaças de natureza técnica e financeira que, apesar de menos citadas pelos respondentes, trazem relevância significativa no cenário digital contemporâneo. Esses riscos podem ser desde vulnerabilidades de segurança até práticas fraudulentas que exploram a inexperiência e inocência infantil, comprometendo tanto a privacidade quanto o patrimônio das famílias.

O ambiente digital exige que crianças e adolescentes mantenham contato diário com dispositivos conectados, plataformas de entretenimento e sistemas que coletam dados pessoais, muitas vezes sem ter essa compreensão plena dos

mecanismos e seus respectivos funcionamentos e permissões concedidas. Ao criar contas em jogos online, redes sociais ou aplicativos, é comum que forneçam informações sensíveis, como nome, e-mail, telefone e até mesmo dados de responsáveis associados a pagamentos. Sem uma supervisão adequada, esse comportamento auxilia na ampliação da superfície de exposição, facilitando a atuação de agentes mal-intencionados e ampliando o risco de acesso indevido a dados.

Nesse cenário, golpes digitais como o *phishing*, páginas falsas, clonagem de perfis, solicitações fraudulentas e engenharia social vem se tornando cada vez mais frequentes. Crianças especialmente são alvos fáceis, pois não possuem repertório suficiente para identificar mensagens suspeitas, links perigosos ou solicitações enganosas. Muitos desses golpes simulam plataformas de jogos, recarga de moedas virtuais, ofertas de itens exclusivos ou promessas de vantagens dentro de aplicativos populares, explorando o interesse e a impulsividade infantil. Além disso, práticas como downloads de arquivos inseguros, instalação de aplicativos não verificados e interação com desconhecidos podem introduzir *malwares*, vírus ou programas espiões nos dispositivos da família.

Os riscos financeiros também recebem seu devido destaque nesse eixo, jogos digitais e plataformas de entretenimento incorporam sistemas de compras internas, recompensas e micro transações que, quando interpretados de maneira errada, podem gerar gastos inesperados. Em ambientes onde esse design persuasivo é utilizado, como *loot boxes* e itens cosméticos em jogos, crianças são incentivadas a consumir sem ter a consciência plena do valor real envolvido. Em casos mais graves também ocorrem fraudes que simulam pagamentos ou serviços legítimos, resultando em prejuízos.

Do ponto de vista técnico, a falta de boas práticas de segurança traz ainda mais gravidade ao problema. Senhas fracas, reutilização de credenciais, ausência de autenticação em duas etapas, utilizar informações sensíveis em nomes de usuário ou senha e também liberação de permissões excessivas para aplicativos aumentam exponencialmente a vulnerabilidade. Incidentes como invasões de contas, sequestro de perfis, perda de acessos, vazamento de informações e uso indevido de dados são consequências comuns quando medidas sérias de segurança não são utilizadas.

Apesar de serem menos mencionados na percepção dos respondentes, os riscos técnicos e financeiros possuem impactos imediatos e potencialmente graves. Subestimar esses perigos, junto ao desconhecimento de como golpes digitais operam,

cria um ambiente que direciona as crianças e os adolescentes a serem vítimas de fraudes, violações de privacidade e danos patrimoniais.

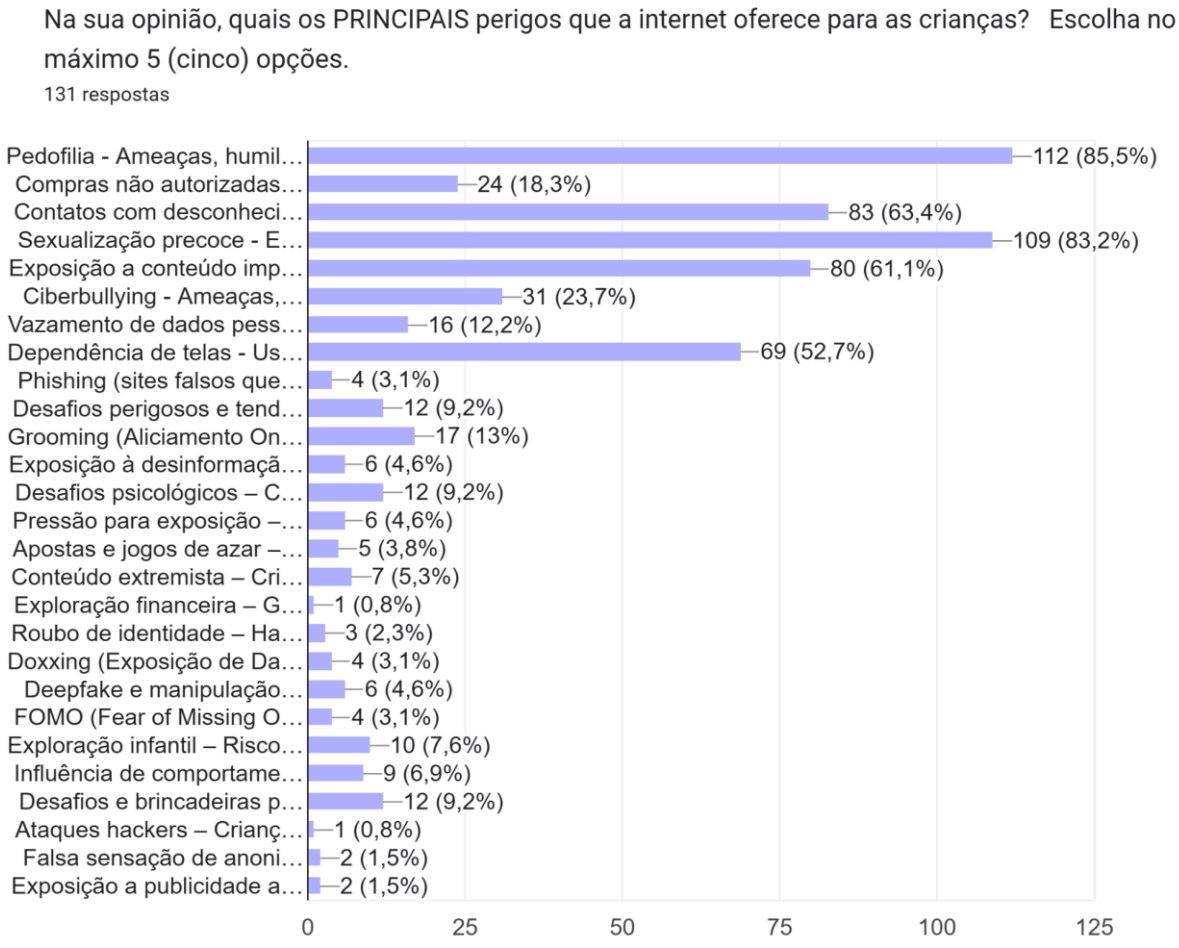
Assim, compreender esses riscos é fundamental para consolidar um ecossistema digital mais seguro. Adotar medidas preventivas como educação digital, incentivo ao pensamento crítico, monitoramento ativo e criação de hábitos seguros de navegação contribuem para reduzir vulnerabilidades e aumentar a segurança das interações online.

2.7 O Descompasso entre o Risco (Pedofilia) e o Processo (*Grooming*).

O estudo realizado indica uma grande percepção de risco da população em relação ao risco “Pedofilia - Ameaças, humilhações e agressões de cunho sexual contra crianças”, com 112 votos, ou 85,5% dos respondentes considerando como um dos principais perigos, como mostra a Figura 11. Todavia, o risco “*Grooming* (Aliciamento *Online*) - Quando adultos mal-intencionados se passam por crianças para ganhar a confiança delas e manipulá-las.” apresenta pouco reconhecimento como uma ameaça para as crianças no Brasil, com apenas 13 votos, 13% dos entrevistados.

O “*Grooming*”, é uma palavra de língua inglesa que se refere ao aliciamento de menores de idade especificamente em um ambiente virtual, o ato de manipular crianças on-line de diversas formas para conseguir uma conexão emocional com a mesma levando o menor a ceder a realizar a atos de cunho sexual, como fornecer fotos e vídeos íntimos, ou até mesmo ter e manter relações sexuais com os “*Groomers*”, como são chamados os que cometem tal delito (Esteves, 2020). O “*Grooming*” se difere do ato de “abuso sexual infantil”, visto que, segundo Lowenkron, (2010, p. 18), “a categoria é definida como interações sexuais com crianças.”, enquanto o *grooming* é uma ferramenta ou *modus operandi* que permite, ou ao menos, facilita, o abuso sexual infantil.

Figura 11 - Principais perigos da Internet para crianças.



Fonte: Elaborado pelos autores (2025).

Essa diferença entre a quantidade de votos não é meramente semântica, é o indício da falta de alfabetização digital dos entrevistados. O público demonstra uma grande consciência, ou ao menos preocupação, com o resultado temido (o abuso sexual infantil em si) cometido pelo agente criminoso (o abusador), mas em grande escala, desconhece o processo metodológico de possibilita o crime de ocorrer. O resultado da pesquisa implica que uma grande atenção e foco ao produto final de um abuso digital, mas não ao processo que permite e capacita adultos a realizarem tal abuso.

Esta, por sua vez, não é a primeira vez que a pesquisa indica um pânico moral à ideia de um abuso sexual infantil por meio das redes. Como fortemente abordado no capítulo anterior, a ideia de uma criança sendo ferida ou sexualmente explorada gera uma reação de repulsa tão hedionda no público que muitas vezes cega a

população a outros problemas, ou muitas vezes, como neste caso, a própria causa do problema em si.

2.8 Os Riscos "Invisíveis": Porque ameaças técnicas são sub-priorizadas.

Os dados levantados na pesquisa de campo indicam que ameaças de cunho social são consideradas pela população como muito mais importantes do que ameaças técnicas. Perigos como “Pedofilia - Ameaças, humilhações e ofensas feitas online por outras crianças ou adolescentes”, “Contatos com desconhecidos - Risco de interação com predadores virtuais, golpistas ou pessoas mal-intencionadas”, “Sexualização precoce - Exposição de crianças a conteúdos, estímulos ou comportamentos sexuais antes da idade adequada.”, e “*Ciberbullying* - Ameaças, humilhações e ofensas feitas online por outras crianças ou adolescentes” receberam respectivamente 112, 83, 109 e 80 votos. Enquanto ameaças como “*Phishing* (sites falsos que imitam um site real) e golpes online - Crianças podem ser enganadas a fornecer dados ou clicar em links maliciosos.”, “Roubo de identidade – Hackers podem roubar informações e usá-las para fraudes.”, “*Doxxing* (Exposição de Dados) - Vazamento de informações pessoais que podem levar a perseguições ou ameaças.” e “Ataques hackers – Crianças podem baixar vírus ou malwares sem perceber, colocando dispositivos e redes em risco.”, recebem apenas quatro, três, três, quatro e um voto, respectivamente.

Kahneman (2011), defende em seu livro “Pensar rápido, pensar despacio” a existência de uma distinção entre dois sistemas de pensamento, o “Sistema 1” e o “Sistema 2”. O “Sistema 1” se refere ao pensamento rápido, julgamentos imediatos, automáticos, intuitivo e principalmente, emocional, um pensamento que não exige grande esforço consciente e se é o que gera pensamentos imediatos, como equações matemáticas simples como 2 + 2, além de resposta de luta e fuga, como correr de um perseguidor ou prestar socorro imediato a uma pessoa ao testemunhá-la sofrer um acidente. O principal fator que ativa o nosso Sistema 1 são as experiências passadas, seguindo o exemplo anterior, uma pessoa que já testemunhou outra sofrendo um acidente sabe que aprende que é necessário um socorro imediato, logo ao ver o mesmo ocorrido novamente, não perde tempo e acode o acidentado imediatamente.

O Sistema 2, por outro lado, é o pensamento lento, deliberativo, lógico e exigente em termos de energia cognitiva. Ela é utilizada, segundo Kahneman (2011),

para raciocínios complexos, análise crítica e esforço consciente, como resolver equações matemáticas complexas, resolver problemas que não possuem soluções óbvias ou ações de alta precisão, como estacionar um carro em um espaço apertado. Kahneman (2011) também defende que o Sistema 2 é mantido em “repouso” até ser utilizado para economizar energia cognitiva, o que muitas vezes, pode gerar falhas de pensamentos críticos e ações realizadas por “impulso”.

A ideia de sistemas binários de pensamento defendido por Kahneman (2011), é crucial no entendimento da resposta dos participantes da pesquisa de campo, pois ameaças como “predadores” sexuais ou “*cyberbullying*” ativam o Sistema 1 imediatamente, pois a imagem de uma criança em correndo o risco de sofrer um abuso sexual ou psicológico gera uma imediata resposta visceral de repúdio. Enquanto a ideia de ataques de *hacking* ou engenharia social requerem um esforço cognitivo alto e muitas vezes, conhecimento teórico para ser compreendido em sua totalidade, e por isso, é menos reconhecido pela população.

Como mencionado anteriormente, Kahneman (2011) defende que o Sistema 1 de pensamento depende bastante de experiências passadas para se moldar, o que também expressa sentido considerando o quão comuns são abusos sexuais em crianças no Brasil. Segundo a Fundação Abrinq, em 2023, houveram 78.537 notificações de abusos sexuais recebidas, onde 57,6 mil são referente a vítimas de menos de 19 anos, isso indica que, 73,5% das vítimas de abuso sexual são crianças ou adolescentes, o que corresponde a quase três a cada quatro casos. Além disso, segundo Brasil (2024), na reportagem da TV Senado, apenas 10% dos casos de violência sexual são reportados às autoridades, esse dado gera o entendimento que, existem muitos mais casos de violência sexual no Brasil são ainda mais frequentes do que os dados fornecidos pela Fundação Abrinq apontam. Essa familiaridade com o problema no Brasil gera, segundo teoria de Kahneman (2011), uma resposta empática mais imediata e visceral do que os riscos relacionados a crimes sexuais do que crimes técnicos, o que justifica o resultado das pesquisas.

2.9 Perigos Cotidianos vs. Ameaças Extremas: A Hierarquia do Medo.

Ao analisar os dados da pesquisa de campo é possível observar que os perigos percebidos se organizam em uma espécie de hierarquia: alguns riscos são vistos como ameaças extremas de alto impacto e visibilidade - como pedofilia, exposição a

contato com estranhos e exploração sexual -, enquanto outros se camuflam como perigos cotidianos, mais sutis, porém ainda nocivos, como a dependência de telas e o cyberbullying. Essa distinção reflete diretamente na forma como a sociedade compreende e reage aos riscos do ambiente digital.

A pesquisa de campo a pedofilia aparece como o principal perigo na opinião dos participantes, sendo citada por 85,5% dos respondentes. Já problemas recorrentes e cotidianos como a dependência de telas (52,7%) e o *cyberbullying* (23,7%) também se destacam, revelando preocupações que, embora menos “extremas”, estão diretamente presentes na rotina digital das crianças. Essa diferença de percepção oferece um campo para compreender como o medo é estruturado socialmente e como ele orienta as práticas de proteção e educação digital.

A pedofilia sendo indicada como o maior risco pelos participantes demonstra que o maior medo das pessoas referente ao uso da internet pelas crianças vem das ameaças externas, a figura de um “predador” - um indivíduo mal-intencionado que se infiltra nesse meio para se aproveitar e explorar crianças. A diferença discrepante entre essa problemática e as outras apresentadas no formulário se dá por conta do impacto direto e quase instantâneo que essa situação pode causar, tanto a vítima quanto a sua família e amigos.

Esse receio não vem sem fundamento, pois, de acordo com a pesquisa TIC Kids Online Brasil de 2023, cerca de nove milhões de crianças e adolescentes relataram ter vivenciado alguma situação envolvendo conteúdo sexual ao utilizar a internet (CETIC.br, 2023). Ainda sobre essa problemática, a preocupação é amplamente reforçada ao levar em consideração a quantidade de casos denunciados referente a esse tipo de situação, segundo dados do Governo Federal divulgados em 2020 a exposição de crianças e adolescentes ocupou o quinto lugar no ranking de denúncias feitas ao Disque 100 (Disque Direitos Humanos, serviço gratuito Ministério dos Direitos Humanos e da Cidadania que recebe denúncias de violações de direitos humanos) (Brasil, 2020).

É importante destacar que esse número representa apenas os casos reportados - o que significa que a quantidade de ocorrências não denunciadas pode ser significativamente maior, reforçando o caráter silencioso e recorrente do problema.

Também há estudos brasileiros que justificam a preocupação. Paulino (2021), enfatiza que o uso da internet aumenta a vulnerabilidade infantil, já que as redes sociais e aplicativos facilitam o acesso dos agressores às vítimas. De forma

semelhante, Amara et al. (2023) afirmam que a exposição de imagens e informações das crianças e adolescentes na internet - muitas vezes feita de forma inocente e descuidada, até mesmo pelos próprios responsáveis - cria um ambiente que favorece pedofilia virtual e o uso indevido de conteúdo infantil.

Por outro lado, as ameaças que não têm um impacto tão repentino, como por exemplo a dependência de telas, apesar de conhecidas, podem acabar não recebendo a devida atenção ou até mesmo passar despercebidas - principalmente pelos responsáveis.

De acordo com a mesma pesquisa mencionada anteriormente, a TIC Kids Online Brasil de 2023, 93% da população brasileira de 9 a 17 anos é usuária da internet, sendo que desses, vinte milhões de crianças e adolescentes relatam usar a internet mais de uma vez por dia, totalizando 82.7% do público total da pesquisa. Outro tópico é a percepção dos jovens referente ao uso excessivo da internet, onde 24% responderam que tentou passar menos tempo na internet e não conseguiu, 16% afirmaram se sentir mal em algum momento por não poder acessar e 15% afirmaram dormir ou se alimentar mal em consequência ao uso da internet.

Quando o uso de aparelhos eletrônicos - em particular os aparelhos celulares que são o meio mais usado para acessar a internet entre os jovens (CETIC.br, 2024) - ocorre em excesso ele se aproxima do padrão da “dependência”, além do tempo gasto, esse constante uso passa a interferir em outros aspectos e atividades essenciais no desenvolvimento infantil. O artigo Impactos da dependência de telas infantil de Brito et al., (2024) aponta que a utilização em excesso pode causar diversos problemas como: Dificuldade no desenvolvimento - capacidade cognitiva e de concentração comprometidas, rendimento escolar prejudicado, atraso na aquisição de linguagem ou habilidades comunicativas. Problemas psicológicos como depressão, ansiedade, estresse e esgotamento/cansaço extremo. Além disso, também pode levar a problemas físicos - hábitos alimentares pouco saudáveis, obesidade, distúrbio de sono, problemas na visão. O tempo excessivo de tela pode reduzir também a participação em atividades que promovem interação social, brincar livre, e vínculo familiar, aspectos cruciais para o desenvolvimento social e interativo das crianças e adolescentes.

Além da ameaça externa representada pela pedofilia e da ameaça mais silenciosa ligada ao tempo de uso e dependência das telas, a pesquisa também revelou uma certa preocupação dos participantes referente ao *cyberbullying*, que de

certa forma pode ser considerado uma “soma” das ameaças: a ameaça externa vinda do agressor, que nesse caso costuma ser outra criança ou adolescente, e a soturna dificuldade de identificar esse tipo de problema. Embora tenha sido citado por um número menor de participantes, correspondentes à 23,7% do total, o cyberbullying representa uma das formas mais diretas de violência no ambiente digital, impactando profundamente o bem-estar psicológico das vítimas.

De acordo com o Art. 2º da Lei nº 13.185/2015 o bullying é definido pela prática de violência, física ou psicológica, de modo intencional e repetitivo, sem nenhuma motivação evidente, já o cyberbullying se enquadra na mesma situação, porém no ambiente virtual.

Embora o *bullying* seja um tema que já foi bastante discutido, continua sendo um dos maiores e mais recorrentes problemas em escolas no Brasil e no mundo. O avanço da tecnologia agravou a situação, fazendo com que essa violência migrasse ao meio virtual, onde o cyberbullying se estabeleceu como uma extensão do problema. Apesar disso a pesquisa da CETIC.br indica que aproximadamente quinhentas mil crianças e adolescentes relatam sofrer de situações ofensivas na internet todos os dias, porém em contrapartida, cerca de cinco milhões relatam que não comentam com país e/ou responsáveis sobre situações ofensivas ocorridas na internet e seis milhões responderam que não contaram a ninguém. O fato das vítimas se manterem em silêncio, as vezes por medo, falta de informação ou até mesmo ameaças, somado ao anonimato que os agressores usam ao seu favor nesse tipo de situação torna difícil a identificação e a tomada de atitude a respeito.

A priorização das ameaças externas pode ofuscar os perigos cotidianos por estes não apresentarem o mesmo caráter de urgência e visibilidade imediata que as ameaças externas, indicando que os conhecimentos e estratégias de proteção digital ainda são guiadas mais pelo pavor de eventos extremos e imediatos do que pela atenção às vulnerabilidades silenciosas e contínuas da rotina online das crianças e adolescentes.

2.10 O Top 5 das Ameaças: O Ciclo de Riscos Sexuais

A análise dos dados dessa pesquisa demonstra que os riscos mais temidos pelos participantes têm um aspecto em comum: todos estão relacionados a ameaças de natureza sexual. Esse núcleo composto por Exposição a Conteúdo Impróprio,

Sexualização Precoce, Contatos com Desconhecidos e Pedofilia, pode estar ligado a um ciclo, no qual um problema pode desencadear o seguinte, culminando na ameaça considerada a mais grave pelos respondentes: a pedofilia.

O ciclo tem início na exposição a conteúdo impróprio, cada vez mais frequente em ambientes digitais amplos e com pouca filtragem. O acesso descontrolado e não supervisionado à internet expõe crianças e adolescentes, muitas vezes sem que tenham buscado esse material, a conteúdos adultos ou sexuais explícitos, atuando como um fator de dessensibilização e normalização. A ausência de filtros adequados permite que esse tipo de conteúdo distorça a percepção sobre a sexualidade e seus limites.

Essa exposição constante e, de certa forma, normalizada, leva diretamente a sexualização precoce, fenômeno conhecido atualmente como “adultização”. Ele ocorre quando crianças começam a reproduzir comportamentos, posturas, expressões, interesses ou linguagens com conotação sexual não coerentes com seu estágio de desenvolvimento. Essa antecipação cria brechas emocionais e comportamentais que podem chamar a atenção de pessoas mal-intencionadas, aumentando substancialmente a vulnerabilidade infantil.

A fragilidade gerada pela sexualização precoce cria um ambiente favorável que é ativamente explorado na fase seguinte do ciclo, o contato com desconhecidos. A comunicação digital, especialmente em redes sociais, chats de jogos e aplicativos de mensagens, facilita abordagens sutis e persistentes por parte de predadores. O anonimato do ambiente digital, a falta de supervisão e o silêncio da vítima transformam esse espaço em um ambiente ainda mais propício, pois o agressor se aproveita da falta de discernimento e das carências emocionais ou sociais da criança ou adolescente.

A soma desses fatores pode culminar no final do ciclo, levando à ameaça considerada mais grave pela maior parte dos respondentes da pesquisa, a pedofilia, que representa o risco terminal e a consequência mais grave dessa cadeia.

Apesar de não ser uma regra, a pedofilia pode ser o resultado da progressão de uma cadeia de vulnerabilidades digitais e sociais. A exposição e a sexualização mencionadas anteriormente criam a vulnerabilidade, e o *grooming* por meio dos contatos com desconhecidos eventualmente culmina na exploração da vítima.

As ferramentas digitais amplificam a capacidade dos agressores de acessar, persuadir e explorar as vítimas, portanto, a proteção eficaz exige a interrupção da

progressão desse ciclo desde seus estágios iniciais, principalmente no controle de conteúdo acessado e na mediação das primeiras interações online. Somente com orientação ativa, supervisão consistente e educação digital adequada é possível reduzir a probabilidade de que crianças avancem pelas etapas que compõem essa cadeia de risco.

CONSIDERAÇÕES FINAIS

O presente trabalho se propôs a analisar os riscos cibernéticos que crianças possuem ao acessar a Internet de maneira não supervisionada, além de compreender a percepção dos adultos das possíveis ameaças. Através de uma pesquisa de campo realizada com 131 pessoas e revisão bibliográfica dos dados levantados, é nítido que existe uma consciência coletiva dos adultos em relação à periculosidade da rede, mas esse conhecimento não é uniforme entre todas os possíveis riscos.

A análise dos dados levantados confirma a hipótese de que a sociedade prioriza as ameaças de acordo com a “Hierarquia do Medo”, ou seja, existe uma ordem de preocupação decrescente dos riscos corridos por crianças. Em maior prioridade se encontram ameaças de cunho sexual e interativas, como a pedofilia (85,5%) e a sexualização precoce, conforme bem ilustra a Figura 9. Logo após, vem naturezas de cunho social, como *Cyberbullying* e dependência de telas, e por último, ameaças técnicas, como *phishing* e *doxxing*. De acordo com Kahneman (2011), isso ocorre devido a atuação do “Sistema 1” de pensamento, que gera uma resposta emocional imediata a ideia de uma criança em contato com um predador, porém, negligencia riscos técnicos, financeiros e sociais, que requerem a atuação do “Sistema 2”, que necessita de alguma forma de conhecimento prévio e raciocínio lógico mais intenso para gerar uma resposta.

Uma conclusão alarmante deste estudo é a grande falta de percepção de ameaças técnicas em crianças. Riscos como *phishing*, vazamento de dados, *malware* e engenharia social foram pouquíssimos citados como preocupações, ocupando as últimas posições na lista de preocupações. Isso demonstra um grande paradoxo na percepção dos adultos aos perigos digitais para crianças: Existe uma grande preocupação com a segurança das crianças nas redes de computadores, porém existe um analfabetismo digital crítico que impossibilita os adultos de reconhecerem os meios pelos quais as crianças correm perigo. A baixa percepção dos adultos em processo como *grooming* (13%) simboliza essa constatação categoricamente. As pessoas têm medo de que ocorra abusos, mas, estatisticamente, não sabem como ele ocorre.

Para além disso, constata-se que os riscos ao desenvolvimento psicológico, tais quais dependência de telas, *Fear of Missing Out*, e exposição a conteúdos

impróprios para a idade, são reconhecidos pelos entrevistados como nocivos, mas muitas vezes, não são levados a sério, ou até mesmo naturalizados na rotina familiar, vistos como consequências inevitáveis do mundo conectado descrito por Bauman (2001).

Conclui-se, por fim, que a segurança do ambiente digital voltada para o público infantil no Brasil é um desafio mais cultural do que tecnológico. A proteção da frágil figura das crianças não deve vir apenas de um medo ou repulsa de crimes hediondos, mas sim de uma mudança que mude o foco de um “pânico moral” para “prevenção técnica e educativa”. É necessário que pais, responsáveis e profissionais da área da educação conscientizem os menores sobre os perigos da internet, além de que os profissionais da área da computação mantenham os estudos sobre as possíveis consequências do mundo conectado, que deixou de ser um futuro iminente para se tornar uma realidade incontestável, para que, por fim, exista uma boa consciência e percepção dos adultos para que melhor sejam instruídas as crianças brasileiras.

REFERÊNCIAS

AMARA, H. C. R. do; SOUZA, L. da S. de; ALVES, M. E. A. de S. dos S. Da superexposição à vítima: como a exposição infantil na internet alimenta a pedofilia virtual. **Revista JRG de Estudos Acadêmicos**, Brasil, São Paulo, v. 8, n. 18, p. e082137, 2025. DOI: 10.55892/jrg.v8i18.2137. Disponível em: https://revistajrg.com/index.php/jrg/article/view/2137. Acesso em: 18 nov. 2025.

BAUMAN, Zygmunt. **Modernidade líquida.** Rio de Janeiro: Zahar, 2001. Disponível em: <https://www.ispsn.org/sites/default/files/documentos-virtuais/pdf/modernidade_liquida.pdf>. Acesso em: 27 out. 2025.

BOZZOLA, Elena; SPINA, Giulia; AGOSTINIANI, Rino; BARNI, Sarah; RUSSO, Rocco; SCARPATO, Elena; DI MAURO, Antonio; DI STEFANO, Antonella Vita; CARUSO, Cinthia; CORSELLO, Giovanni; STAIANO, Annamaria. **The Use of Social Media in Children and Adolescents:** Scoping Review on the Potential Risks. International Journal of Environmental Research and Public Health, v. 19, n. 16, p. 9960, 12 ago. 2022. Disponível em: https://doi.org/10.3390/ijerph19169960. Acesso em: 21 nov. 2024.

BRASIL. **Crianças, adolescentes e telas: Guia sobre usos de dispositivos digitais.** Brasilia, DF: SECOM, 2025. Disponível em: <https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia/guia-de-telas_sobre-usos-de-dispositivos-digitais_versaoweb.pdf>. Acesso em: 21 out. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. **Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências.** Diário Oficial da União: Seção 1, Brasília, DF, n. 135, p. 1-13, 16 jul. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 18 nov. 2025.

BRASIL. Ministério dos Direitos Humanos e da Cidadania. **Exposição de crianças e adolescentes na internet ocupa quinta posição no ranking de denúncias do Disque 100.** Brasília, DF, nov. 2020. Disponível em: <https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet-ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100>. Acesso em: 21 out. 2025.

BRASIL. Senado Federal. **Apenas 10% dos casos de abuso e exploração sexual de crianças e adolescentes são denunciados.** TV Senado, Brasília, DF, 18 maio 2024. Programa Cidadania. Disponível em: <https://www12.senado.leg.br/tv/programas/cidadania-1/2024/05/apenas-10-dos-casos-de-abuso-e-exploracao-sexual-de-criancas-e-adolescentes-sao-denunciados>. Acesso em: 12 nov. 2025.

BRITO, Crislane Nunes da Silva Ramos de; MENDONÇA, Francisco Cardoso; LOPES JÚNIOR, Hélio Marco Pereira; NUNES, Jenina Ferreira. Impactos da dependência de telas infantil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 10, n. 12, p. 1942–1955, 2024. DOI:

https://doi.org/10.51891/rease.v10i12.17466. Disponível em: <https://periodicorease.pro.br/rease/article/view/17466/9848>. Acesso em: 11 nov. 2025.

CASTELLS, Manuel. **A sociedade em rede.** 8. ed. São Paulo: Paz e Terra, 1999. Disponível em: <https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf>. Acesso em: 27 out. 2025.

CERT.br, **Páginas Falsas utilizadas em tentativas de Phishing**, Mensal. https://stats.cert.br/phishing/. Acesso em: 19 nov. 2024.

CETIC. Núcleo de informação e coordenação do ponto BR. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros:** TIC Domicílios 2024 [Tabelas]. 2024. Disponível em: https://cetic.br/pt/tics/domicilios/2024/individuos/C3/ Acesso em: 21 nov. 2024.

COUTO, Joana Catarina Pimenta. **Auditoria de cibersegurança:** um caso de estudo. 2018. Dissertação (Mestrado em Auditoria) - Instituto Superior de Contabilidade e Administração do Porto, Porto, 2018. Disponível em: https://recipp.ipp.pt/bitstream/10400.22/13242/1/joana_couto_MA_2018.pdf. Acesso em: 21 nov. 2024.

ESTEVES, Ana Rita Alves Ernesto. **Do Natural ao Artificial: Projetar para uma Rede de Design Regenerativo.** Universidade de Lisboa. 2022. Disponível em: <https://repositorio.ulisboa.pt/handle/10451/57782>. Acesso em: 16 out. 2025.

GLOBO. **Mãe processa Roblox e Discord após filho de 15 anos sofrer abuso online e tirar a própria vida**. G1 - Tecnologia, 16 set. 2025. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/09/16/mae-processa-roblox-e-discord-apos-filho-de-15-anos-sofrer-abuso-online-e-tirar-a-propria-vida.ghtml. Acesso em: 5 nov. 2025.

GOMES, Carolina Fernanda; REIS, Helena Macedo. **Marketing digital:** sites x redes sociais no Brasil. In: Revista Interface Tecnológica da FATEC Taquaritinga. p. 53-62,jun. de 2016.ISSN online2447-0864. Disponível em: www.fatectq.edu.br/Interfacetecnologica. Acesso em: 22 set. 2024.

KAHNEMAN, Daniel. **Rápido e devagar: duas formas de pensar.** Tradução de Cássio de Arantes Leite. Rio de Janeiro: Objetiva, 2012.

KASPERSKY. **Brasil e a cibersegurança:** ainda somos o maior alvo de ataques na América Latina. 2022 https://www.kaspersky.com.br/blog/panorama-ameacas-latam-2022/20311/ Acesso em: 21 nov. 2024.

LOWENKRON, Laura. **Abuso sexual infantil, exploração sexual de crianças, pedofilia: diferentes nomes, diferentes problemas?** Revista Latinoamericana. 2010. Disponível em: <https://www.e-publicacoes.uerj.br/SexualidadSaludySociedad/article/view/394/726>. Acesso em: 17 out. 2055.

MALAR, João Pedro. **Banco Central anuncia vazamento de dados ligados a mais de 130 mil chaves Pix**. CNN Brasil, São Paulo, 16 set. 2022. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/banco-central-anuncia-vazamento-de-dados-ligados-a-mais-de-130-mil-chaves-pix/. Acesso em: 21 nov. 2024.

NAÇÕES UNIDAS. Convenção sobre os Direitos da Criança: adotada pela Assembleia Geral das Nações Unidas em 20 de novembro de 1989. Versão disponível em: UNICEF Brasil. 1989. Disponível em: <https://www.unicef.org/brazil/convencao-sobre-os-direitos-da-crianca>. Acesso em: 18 NOV. 2025.

NICBR. Núcleo de Informação e Coordenação do Ponto BR. **TIC Kids Online Brasil 2023**: Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil, 2024. Disponível em: <https://cetic.br/media/docs/publicacoes/2/20240913124019/tic_kids_online_2023_livro_eletronico.pdf>. Acesso em: 16 nov. 2025.

PAULINO, Letícia. **A pedofilia na era digital à luz do Estatuto da criança e do adolescente.** 30f. 2022. Unicesumar - Universidade Cesumar de Maringá, 2022. Disponível em: <https://rdu.unicesumar.edu.br/handle/123456789/9311>. Acesso em: 22 out. 2025.

PRENSKY, Marc. **Nativos Digitais, Imigrantes Digitais** - Parte 1. Artigo publicado originalmente em: On The Horizon, v. 9, n. 5, out. 2001. Disponível em: <https://mundonativodigital.wordpress.com/wp-content/uploads/2015/06/texto1nativosdigitaisimigrantesdigitais1-110926184838-phpapp01.pdf>. Acesso em: 14 nov. 2025

SANTOS, Eduardo Esteves dos; SOARES, Tamires Mariana Mayumi Kurosaki. **Riscos, ameaças e vulnerabilidades:** o impacto da segurança da informação nas organizações. Revista Tecnológica da Fatec Americana, v. 7, n. 2, p. 43-51, dez. 2019. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/4383. Acesso em: 21 nov. 2024.

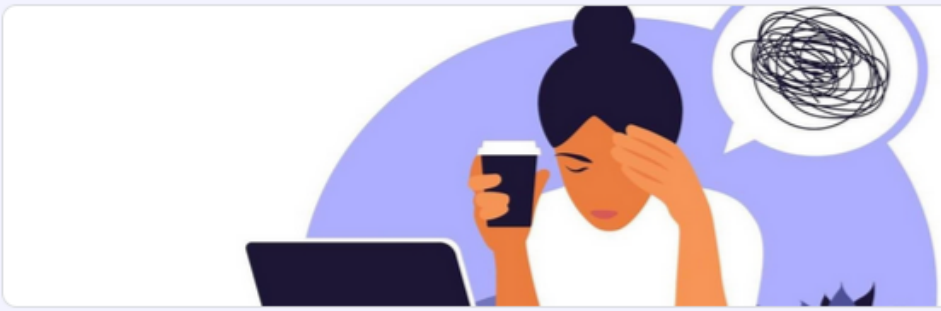
SICA, Nathalia. **Brasil é o país com mais ataques de *phishing* por WhatsApp em 2022**. Blog da Kaspersky, 17 abr. 2023. Disponível em: https://www.kaspersky.com.br/blog/phishing-whatsapp-antiphishing-informacoes-pessoais-dados-financeiros/21113/. Acesso em: 21 nov. 2024.

TIESO, Igor; SANTO, Felipe. **Ataques de Engenharia Social**. 2020 Disponível em: https://www.researchgate.net/publication/350438606_ATAQUES_DE_ENGENHARIA_SOCIAL. Acesso em: 19 nov. 2024.

TWENGE, Jean M.; CAMPBELL, W. Keith. Associations between screen time and lower psychological well-being among children and adolescents. **Preventive Medicine Reports**, v. 12, p. 271–283, 2018. Disponível em: <https://doi.org/10.1016/j.pmedr.2018.10.003>. Acesso em: 16 nov. 2025.

UNICESUMAR. **Brasil perde mais de R$ 25,5 bilhões ao ano com golpes digitais, aponta pesquisa.** Unicesumar Notícias, 18 mar. 2024. Disponível em: https://www.unicesumar.edu.br/brasil-perde-mais-de-r-255-bilhoes-por-ano-com-golpes-financeiros/. Acesso em: 5 nov. 2025.

APÊNDICE A – Formulário de pesquisa.



Questionário sobre a Internet para crianças

Olá, nos chamamos Daniel Dias, Matheus Lisboa e Vyctor Kawan, somos alunos do curso de Segurança da Informação da Fatec Americana.

Antecipadamente, gostaríamos muito de agradecer o seu tempo em responder a este questionário.

Suas respostas nos ajudarão na conclusão do nosso Trabalho de Graduação sobre

Crianças nas Redes Sociais: Exposição a riscos cibernéticos.

Todos os dados aqui informados ficarão em sigilo, ou seja, sua identidade será preservada na nossa investigação, serão utilizadas apenas as estatísticas resultantes dos questionários respondidos.

* Indica uma pergunta obrigatória

Qual o seu nome? *
Informe apenas seu primeiro nome, se preferir (será mantido em segredo, informação para controle)

Sua resposta

Qual o seu Gênero? *

- ◯ Feminino
- ◯ Masculino
- ◯ Transgênero
- ◯ Não-binário
- ◯ Prefiro não dizer
- ◯ Outro

Qual a sua Faixa Etária? *

- ◯ Abaixo de 14 anos
- ◯ de 14 até 17 anos
- ◯ de 18 a 29 anos
- ◯ de 30 a 39 anos
- ◯ de 40 a 49 anos
- ◯ de 50 a 59 anos
- ◯ com 60 anos ou mais

Estado civil: *

- ◯ Solteiro(a)
- ◯ Casado(a)
- ◯ Viúvo(a)
- ◯ Separado(a) judicialmente
- ◯ Divorciado(a)
- ◯ União Estável

Quantos filhos você tem? *

- ◯ Não tenho filhos
- ◯ 1 filho(a)
- ◯ 2 filhos(as)
- ◯ 3 filhos(as)
- ◯ 4 filhos(as)
- ◯ tenho 5 filhos(as) ou mais

Qual seu grau de escolaridade? *

- ◯ Ensino Fundamental Incompleto
- ◯ Ensino Fundamental Completo
- ◯ Ensino Médio Incompleto
- ◯ Ensino Médio Completo
- ◯ Ensino Superior Incompleto
- ◯ Ensino Superior Completo
- ◯ Especialização
- ◯ Mestrado
- ◯ Doutorado

Qual a cidade onde você reside? *

- ◯ Americana
- ◯ Campinas
- ◯ Hortolândia
- ◯ Limeira
- ◯ Nova Odessa
- ◯ Piracicaba
- ◯ Santa Bárbara D'Oeste
- ◯ Sumaré
- ◯ Paulínia
- ◯ Outro: _____

Como você avalia seu próprio conhecimento sobre os perigos do uso da Internet pelas crianças? *

- ◯ Muito alto
- ◯ Alto
- ◯ Moderado
- ◯ Baixo
- ◯ Muito baixo
- ◯ Nenhum Conhecimento

Você acredita que o risco para as crianças, na Internet, é um problema relevante nos dias de hoje? *

- ◯ Extremamente relevante
- ◯ Muito relevante
- ◯ Moderadamente relevante
- ◯ Pouco relevante
- ◯ Não é um problema

Você acredita que o perigo existente na internet, para as crianças, é subestimado? *

- ◯ Concordo totalmente
- ◯ Concordo
- ◯ Neutro
- ◯ Discordo
- ◯ Discordo totalmente

Na sua opinião, quais os PRINCIPAIS perigos que a internet oferece para as crianças? *

Escolha no máximo 5 (cinco) opções.

- [ ] Pedofilia - Abuso sexual que ocorre por meio da internet com fotos e vídeos ou com auxílio dela
- [ ] Compras não autorizadas - Uso de cartões cadastrados para compras em jogos ou aplicativos sem permissão dos pais.
- [ ] Contatos com desconhecidos - Risco de interação com predadores virtuais, golpistas ou pessoas mal-intencionadas.
- [ ] Sexualização precoce - Exposição de crianças a conteúdos, estímulos ou comportamentos sexuais antes da idade adequada.
- [ ] Exposição a conteúdo impróprio - Acesso a imagens, vídeos ou textos inadequados para a idade, como violência ou pornografia.
- [ ] Ciberbullying - Ameaças, humilhações e ofensas feitas online por outras crianças ou adolescentes
- [ ] Vazamento de dados pessoais - Crianças podem compartilhar informações privadas sem perceber os riscos.
- [ ] Dependência de telas - Uso excessivo da internet pode prejudicar o desenvolvimento social e emocional.
- [ ] Phishing (sites falsos que imitam um site real) e golpes online - Crianças podem ser enganadas a fornecer dados ou clicar em links maliciosos.

- [ ] Desafios perigosos e tendências virais - Participação em brincadeiras ou desafios que colocam a segurança em risco.
- [ ] Grooming (Aliciamento Online) – Quando adultos mal-intencionados se passam por crianças para ganhar a confiança delas e manipulá-las.
- [ ] Exposição à desinformação – Crianças podem acreditar em fake news, teorias da conspiração e informações falsas.
- [ ] Desafios psicológicos – Comparação excessiva com influenciadores pode causar baixa autoestima e ansiedade.
- [ ] Pressão para exposição – Influência para postar fotos e vídeos para ganhar curtidas e aceitação social.
- [ ] Apostas e jogos de azar – Publicidade ou acesso fácil a sites de apostas pode incentivar comportamentos compulsivos.
- [ ] Conteúdo extremista – Crianças podem ser expostas a discursos de ódio, ideologias radicais ou grupos extremistas.
- [ ] Exploração financeira – Golpes que fazem crianças gastarem dinheiro em jogos ou assinaturas sem entender as consequências.
- [ ] Roubo de identidade – Hackers podem roubar informações e usá-las para fraudes.
- [ ] Doxxing (Exposição de Dados) – Vazamento de informações pessoais que podem levar a perseguições ou ameaças.

- [ ] Deepfake e manipulação de imagens – Crianças podem ser vítimas de vídeos e fotos falsas que as envolvem.
- [ ] FOMO (Fear of Missing Out) – Ansiedade causada pelo medo de estar perdendo algo que os outros estão fazendo online.
- [ ] Exploração infantil – Risco de exploração sexual e tráfico infantil em plataformas online.
- [ ] Influência de comportamentos autodestrutivos – Sites e fóruns que incentivam distúrbios alimentares, automutilação e até suicídio.
- [ ] Desafios e brincadeiras perigosas – Algumas tendências virais incentivam atitudes arriscadas ou prejudiciais.
- [ ] Ataques hackers – Crianças podem baixar vírus ou malwares sem perceber, colocando dispositivos e redes em risco.
- [ ] Falsa sensação de anonimato – Pode levar a comportamentos inadequados, como cyberbullying e discurso de ódio.
- [ ] Exposição a publicidade abusiva – Anúncios enganosos ou direcionados que podem influenciar decisões de consumo indevidas.