



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS PICOS
TECNÓLOGO EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PEDRO CÁSSIO LEAL DE SOUSA

**DESAFIOS TÉCNICOS E COMPUTACIONAIS NA DETECÇÃO DE
PHISHING EM DISPOSITIVOS MÓVEIS: REVISÃO BIBLIOGRÁFICA**

PEDRO CÁSSIO LEAL DE SOUSA

**DESAFIOS TÉCNICOS E COMPUTACIONAIS NA DETECÇÃO DE
PHISHING EM DISPOSITIVOS MÓVEIS: REVISÃO BIBLIOGRÁFICA**

Artigo científico apresentado ao Instituto
Federal de Educação, Ciência e
Tecnologia do Piauí – Campus Picos,
como requisito parcial para obtenção do
título de Tecnólogo em Análise e
Desenvolvimento de Sistemas.

Orientador: Prof. Me. Israel Cardoso
Araújo

PEDRO CÁSSIO LEAL DE SOUSA

DESAFIOS TÉCNICOS E COMPUTACIONAIS NA DETECÇÃO DE PHISHING EM DISPOSITIVOS MÓVEIS: REVISÃO BIBLIOGRÁFICA

Artigo científico apresentado ao Instituto
Federal de Educação, Ciência e
Tecnologia do Piauí – Campus Picos,
como requisito parcial para obtenção do
título de Tecnólogo em Análise e
Desenvolvimento de Sistemas.

Aprovado em: 06 / 08 / 2026

BANCA EXAMINADORA



Documento assinado digitalmente

ISRAEL CARDOSO ARAUJO

Data: 25/08/2026 09:44:28-0300

Verifique em <https://validar.iti.gov.br>

Prof. Me. Israel Cardoso Araújo(Orientador)

Instituto Federal do Piauí (IFPI)



Documento assinado digitalmente

DENIS COSTA PAIVA

Data: 25/08/2026 18:17:03-0300

Verifique em <https://validar.iti.gov.br>

Prof. Esp. Denis Costa Paiva

Instituto Federal do Piauí (IFPI)



Documento assinado digitalmente

LUIS GUILHERME SOUSA E SILVA

Data: 25/08/2026 20:09:17-0300

Verifique em <https://validar.iti.gov.br>

Prof. Me. Luis Guilherme Sousa e Silva

Instituto Federal do Piauí (IFPI)

A Deus, que transformou minhas incertezas em fé e me capacitou a superar cada obstáculo ao longo dessa jornada.

RESUMO

O crescimento acelerado do uso de dispositivos móveis nas últimas décadas transformou a forma como as pessoas se comunicam e realizam transações digitais, ao mesmo tempo em que criou um ambiente propício para a expansão de ataques de *phishing*. Esta pesquisa realiza uma revisão bibliográfica sobre os desafios técnicos e computacionais enfrentados na detecção de *phishing* em dispositivos móveis, com foco especial no *smishing*, modalidade que explora mensagens de texto, e nas abordagens baseadas em aprendizado de máquina e aprendizado profundo. A partir da análise de dezenove trabalhos publicados entre 2022 e 2026, identificaram-se os principais algoritmos empregados, os resultados obtidos em termos de acurácia e as limitações mais recorrentes, como a dependência de conjuntos de dados restritos, a dificuldade de generalização para idiomas diferentes do inglês e o custo computacional de modelos mais sofisticados. Os resultados indicam que algoritmos clássicos e arquiteturas de aprendizado profundo alcançam desempenho elevado em ambientes controlados, mas enfrentam obstáculos significativos quando aplicados a cenários reais em dispositivos com recursos limitados. Conclui-se que o avanço da área depende tanto do desenvolvimento de soluções mais leves e adaptáveis quanto da criação de bases de dados multilíngues e atualizadas regularmente.

Palavras-chave: *phishing*; *smishing*; dispositivos móveis; aprendizado de máquina; segurança da informação.

ABSTRACT

The rapid growth in *mobile* device usage over recent decades has reshaped communication and digital transactions while simultaneously creating a fertile ground for *phishing* attacks. This study presents a literature review on the technical and computational challenges involved in detecting *phishing* on *mobile* devices, with particular emphasis on *smishing*, the SMS-based variant, and on *machine learning* and *deep learning* approaches. Through the analysis of nineteen papers published between 2022 and 2026, the main algorithms employed were identified, along with reported *accuracy* results and recurring limitations such as dependence on restricted *datasets*, difficulty generalising across languages other than English, and the computational cost of more complex models. Findings indicate that classical algorithms and *deep learning* architectures achieve high performance in controlled settings but face significant obstacles when *deployed* in real-world scenarios on resource-constrained devices. It is concluded that progress in this field requires both the development of lighter and more adaptable solutions and the creation of multilingual, regularly updated *datasets*.

Keywords: *phishing*; *smishing*; *mobile* devices; *machine learning*; information security.

LISTA DE ABREVIATURAS E SIGLAS

SMS	Short Message Service (Serviço de Mensagens Curtas)
CNN	Convolutional Neural Network (Redes Neurais Convolucionais)
LSTM	Long Short-Term Memory (Redes com Memória de Longo e Curto Prazo)
BERT	Bidirectional Encoder Representations from Transformers
URL	Uniform Resource Locator
RAM	Random Access Memory (Memória de Acesso Aleatório)
5G	5ª Geração de Redes Móveis
AM	Aprendizado de Máquina
SVM	Support Vector Machine (Máquina de Vetores de Suporte)
KNN	K-Nearest Neighbors (K-Vizinhos Mais Próximos)
ONNX	Open Neural Network Exchange
DNS	Domain Name System (Sistema de Nomes de Domínio)
AUC	Area Under the Curve (Área sob a Curva)
BDTD	Biblioteca Digital Brasileira de Teses e Dissertações
BiLSTM	Bidirectional Long Short-Term Memory
GPU	Graphics Processing Unit (Unidade de Processamento Gráfico)
MLP	Multilayer Perceptron (Perceptron Multicamadas)
NLP	Natural Language Processing (Processamento de Linguagem Natural)
QR Code	Quick Response Code (Código de Resposta Rápida)
RISTI	Revista Ibérica de Sistemas e Tecnologias de Informação
SBSEG	Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais
TF-IDF	Term Frequency–Inverse Document Frequency (Frequência do Termo–Frequência Inversa do Documento)

LISTA DE SÍMBOLOS

% Percentual

ms Milissegundo

> Maior que

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS.....	6
LISTA DE SÍMBOLOS.....	7
1 INTRODUÇÃO.....	7
2 OBJETIVOS.....	9
2.1 Objetivo Geral.....	9
2.2 Objetivos Específicos.....	9
3 REFERENCIAL TEÓRICO.....	10
3.1 Phishing e suas modalidades em dispositivos móveis.....	10
3.2 Aprendizado de máquina aplicado à detecção de ameaças.....	12
3.3 Desafios computacionais em ambientes móveis.....	14
3.4 Aplicativos e ferramentas de proteção contra phishing.....	16
4 METODOLOGIA.....	17
5 RESULTADOS E DISCUSSÃO.....	21
6 CONSIDERAÇÕES FINAIS.....	26
REFERÊNCIAS.....	29

1 INTRODUÇÃO

Nas últimas duas décadas, os dispositivos móveis mudaram completamente a maneira como as pessoas interagem com a tecnologia e acessam informações. O que antes era restrito a chamadas de voz e mensagens de texto simples tornou-se uma plataforma multifuncional: hoje, pelo celular, as pessoas fazem compras, trabalham, consultam médicos e realizam praticamente tudo o que antes exigia um computador de mesa ou um deslocamento físico. No Brasil, esse fenômeno é ainda mais marcante, segundo levantamentos recentes, a maioria da população usa o celular como principal meio de acesso à internet, e uma parcela significativa sequer dispõe de outro dispositivo para se conectar (CETIC.BR, 2025). É um avanço real em termos de inclusão digital, mas que criou, ao mesmo tempo, um ambiente bastante favorável para que criminosos atuem.

O *phishing* é um dos problemas mais antigos e persistentes nesse cenário. Em essência, trata-se de uma técnica que engana o usuário para que ele tome alguma ação prejudicial, fornecer senhas, confirmar transações fraudulentas, instalar aplicativos maliciosos ou revelar dados pessoais, por meio de mensagens ou páginas que aparentam ser legítimas. O que torna o *phishing* particularmente difícil de combater é que ele não explora falhas técnicas dos sistemas, mas sim traços humanos como confiança, urgência e falta de atenção. Mesmo pessoas com experiência em tecnologia podem cair nessa armadilha quando a mensagem chega num momento de distração ou quando a imitação é convincente o suficiente (IBM, 2025).

Nos dispositivos móveis, essa ameaça assumiu formas adaptadas às características dessas plataformas. O smishing, nome que une SMS e phishing, é a modalidade central desta pesquisa e talvez a variante mais comum no contexto móvel, aproveitando o hábito dos usuários de responder mensagens de texto com mais rapidez e menos ceticismo do que fariam com um e-mail. O vishing, que usa chamadas de voz para extrair informações confidenciais, e o quishing, que emprega QR codes como ponto de entrada para páginas maliciosas, são modalidades complementares também abordadas na literatura, ainda que com menor volume de

estudos do que o smishing (WANG et al., 2025). Essa diversificação mostra que os criminosos acompanham de perto as mudanças de comportamento dos usuários e se adaptam rapidamente.

Os impactos econômicos e sociais disso são concretos. Segundo Santos (2025), as fraudes digitais cresceram mais de 17% entre 2023 e 2024 no Brasil, com perdas estimadas em R\$ 10,1 bilhões, afetando de forma desproporcional usuários de serviços bancários e plataformas de comércio eletrônico. Bezerra, Millian e Silva (2024) documentaram que 61% das páginas falsas identificadas em experimentos simulados imitavam instituições financeiras, e que 43% dos participantes clicaram em links suspeitos recebidos por SMS dado que evidencia a eficácia do smishing como vetor de ataque e reforça a centralidade dessa modalidade no escopo desta pesquisa.

A comunidade científica tem se dedicado bastante a esse problema. As abordagens baseadas em aprendizado de máquina e aprendizado profundo se destacam na literatura, com resultados expressivos em testes controlados. Algoritmos como Random Forest, redes neurais convolucionais (CNN), redes com memória de longo e curto prazo (LSTM) e modelos baseados em Transformers, como o BERT e suas variantes mais compactas, foram aplicados com sucesso à classificação de mensagens e *URLs* como legítimas ou maliciosas (PREETI; SHARMA, 2024). Os avanços são reais e mostram que o campo amadureceu bastante nos últimos anos.

O problema é que transferir essas soluções para o ambiente real dos celulares não é simples. Smartphones operam com processadores menos potentes, memória RAM limitada e dependência de bateria, o que impõe restrições sérias à execução de modelos complexos em tempo real. Muitos ataques acontecem justamente em situações de conectividade instável ou ausente, o que inviabiliza abordagens que precisam consultar serviços externos para funcionar. Há ainda a necessidade de atualizar os modelos continuamente, para que acompanhem a evolução das táticas dos atacantes, algo que é bem mais simples de fazer em servidores do que em dispositivos móveis distribuídos. E, no caso do Brasil

especificamente, existe uma lacuna linguística relevante: boa parte dos modelos disponíveis foi treinada com dados em inglês, o que compromete sua eficácia para detectar ataques em português.

É nesse cruzamento de desafios que se situa o problema investigado neste trabalho, orientado pela seguinte questão de pesquisa: quais são os principais desafios técnicos e computacionais enfrentados pelos sistemas de detecção de phishing, em especial o smishing, quando aplicados a dispositivos móveis, e como a literatura recente tem buscado superá-los?

Com esse objetivo, esta pesquisa realizou uma revisão bibliográfica sistemática de dezenove trabalhos publicados entre 2022 e 2026. O recorte temporal não foi aleatório: trata-se de um período em que o campo passou por mudanças relevantes, impulsionadas pelo avanço dos grandes modelos de linguagem e pela expansão do 5G, que ampliou o acesso à internet móvel em regiões antes pouco conectadas. A partir dessa base, buscou-se mapear as principais abordagens adotadas, comparar resultados, identificar padrões e lacunas na literatura e apontar direções para pesquisas futuras, contribuindo para uma leitura mais completa e crítica de um problema que afeta diretamente milhões de brasileiros.

2 OBJETIVOS

2.1 Objetivo Geral

Analisar, por meio de revisão bibliográfica sistemática, os principais desafios técnicos e computacionais na detecção de phishing e smishing em dispositivos móveis, identificando as abordagens baseadas em aprendizado de máquina e aprendizado profundo mais empregadas na literatura recente e avaliando em que medida essas soluções consideram as restrições reais dos dispositivos móveis, como capacidade de processamento, consumo de memória e funcionamento offline.

2.2 Objetivos Específicos

a) Identificar as técnicas e algoritmos mais empregados na literatura recente para detecção de *phishing* e *smishing* em dispositivos móveis;

b) Comparar os resultados reportados nos estudos selecionados, considerando métricas de acurácia e, quando disponíveis, informações sobre custo computacional, tamanho do modelo, consumo de memória e tempo de inferência em dispositivos móveis;"

c) Mapear as principais limitações apontadas pelos autores, como dependência de datasets restritos, dificuldades de generalização para outros idiomas e contextos, custo computacional elevado e ausência de validação em condições reais de uso em dispositivos móveis;

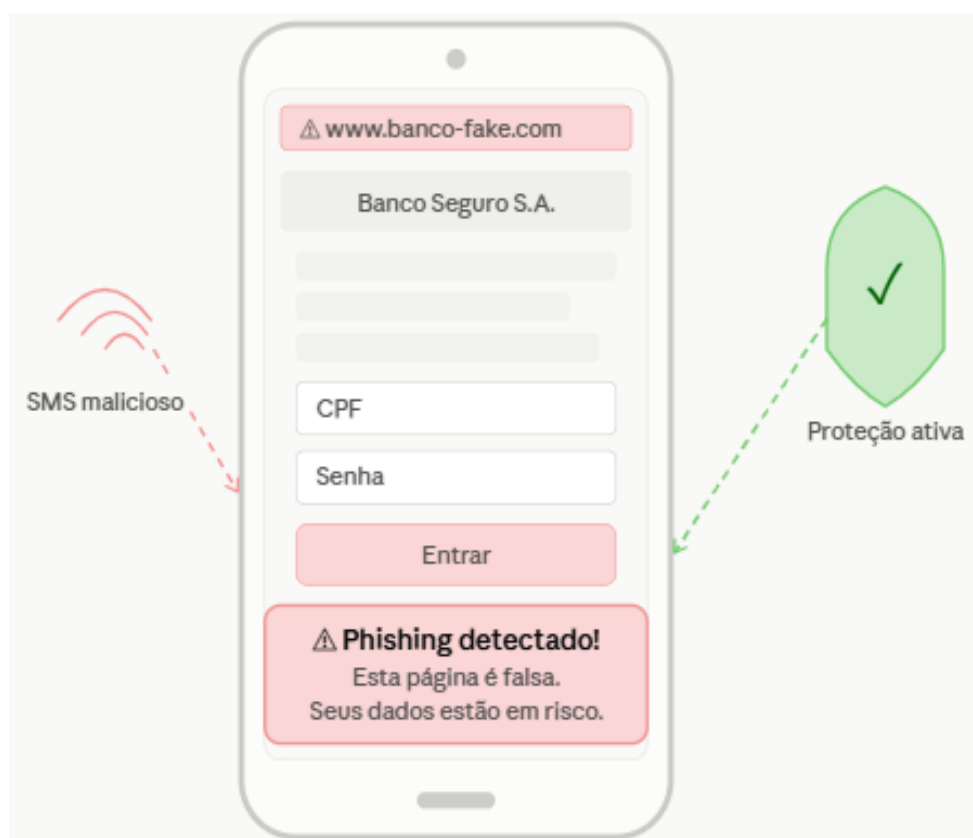
d) Discutir as tendências e lacunas identificadas, apontando caminhos para pesquisas futuras na área de segurança móvel.

3 REFERENCIAL TEÓRICO

3.1 Phishing e suas modalidades em dispositivos móveis

O *phishing* é uma das formas mais antigas e persistentes de ataque cibernético, cuja essência consiste em induzir o usuário a tomar uma ação prejudicial, como fornecer credenciais, realizar pagamentos ou instalar aplicativos maliciosos, por meio de comunicações que aparentam ser legítimas. A engenharia social é o elemento central dessa técnica: o atacante explora a confiança, a urgência e o despreparo da vítima para alcançar seus objetivos (IBM, 2025).

Figura 1 - Representação conceitual da detecção de phishing em dispositivos móveis



Elaborado pelo autor (2026).

A Figura 1 apresenta uma representação conceitual do processo de detecção de uma página maliciosa acessada por dispositivo móvel.

Com a migração massiva dos usuários para dispositivos móveis, surgiram variantes adaptadas a esse ambiente. O *smishing*, contração de SMS e *phishing*, é talvez a mais prevalente delas, explorando a característica dos usuários de ler e responder mensagens de texto com maior rapidez e menor ceticismo do que *e-mails*. Estudos indicam que mais de 40% dos usuários clicam em *links* suspeitos recebidos por SMS quando simulados em ambientes de teste controlado

(BEZERRA; MILLIAN; SILVA, 2024), o que evidencia a eficácia da abordagem sob o ponto de vista do atacante.

Outras modalidades relevantes no contexto móvel incluem o *vishing*, que utiliza chamadas de voz automatizadas ou humanas para obter informações confidenciais, e o *quishing*, modalidade mais recente que emprega *QR codes* para redirecionar vítimas a páginas maliciosas. Essa última tem crescido de forma expressiva, em parte porque os usuários tendem a confiar mais em *QR codes* do que em *links* de texto e porque a *URL* de destino não é exibida antes da leitura (WANG et al., 2025).

Nesse contexto, as características de cada modalidade influenciam diretamente a estratégia de detecção. Em mensagens SMS, a análise pode considerar principalmente o conteúdo textual, remetente e presença de links suspeitos, enquanto a análise direta de URLs permite explorar características estruturais do endereço, como domínio, comprimento e uso de caracteres incomuns. No caso dos *QR codes*, existe uma etapa adicional de processamento, pois o código precisa ser interpretado para que a URL de destino seja obtida e posteriormente analisada. Dessa forma, abordagens baseadas somente em URLs tendem a apresentar menor custo computacional, enquanto a análise de mensagens e *QR codes* pode exigir etapas adicionais de processamento.

Do ponto de vista do impacto econômico, os números são expressivos. Levantamentos recentes apontam um crescimento superior a 17% nas fraudes digitais entre 2023 e 2024 no Brasil, com perdas estimadas em bilhões de reais, afetando especialmente usuários de serviços bancários e plataformas de e-commerce. Páginas falsas que imitam instituições financeiras representam parcela significativa das ocorrências registradas (BEZERRA; MILLIAN; SILVA, 2024).

3.2 Aprendizado de máquina aplicado à detecção de ameaças

O aprendizado de máquina (AM) consolidou-se nas últimas décadas como uma das abordagens mais promissoras para a detecção automatizada de ameaças

cibernéticas. Diferentemente das soluções baseadas em regras fixas ou assinaturas, os modelos de AM são capazes de aprender padrões a partir de dados históricos e generalizar esse conhecimento para identificar instâncias maliciosas não vistas anteriormente. Essa capacidade de generalização é especialmente valiosa em um domínio como o *phishing*, no qual as táticas dos atacantes evoluem continuamente (PREETI; SHARMA, 2024).

Entre os algoritmos clássicos mais utilizados na literatura de detecção de *smishing* e *phishing*, destacam-se o Random Forest, o Naïve Bayes, o K-Nearest Neighbors (KNN) e o Support Vector Machine (SVM). O Random Forest, em particular, tem mostrado desempenho consistentemente elevado em múltiplos estudos, com taxas de acurácia frequentemente superiores a 94%, combinando robustez a ruídos e interpretabilidade relativa (FRANCO, 2024; ZARDO; EMER, 2024). Algoritmos de *gradient boosting*, como XGBoost e LightGBM, também têm ganhado destaque, especialmente em tarefas que envolvem análise de *URLs*, onde a extração de características estruturais é determinante para o desempenho (SANTOS; VASCONCELLOS, 2024).

Apesar dos resultados apresentados, a escolha do algoritmo deve considerar as características dos dados e as limitações do ambiente móvel. Para mensagens de SMS, algoritmos capazes de trabalhar com características textuais podem ser mais apropriados, enquanto modelos baseados em características estruturais podem apresentar maior adequação à classificação de *URLs*. Além disso, em dispositivos móveis, algoritmos com menor custo computacional podem ser preferíveis quando a diferença de desempenho em relação a modelos mais complexos não for significativa. Portanto, a escolha do modelo não deve considerar somente a acurácia, mas também o tempo de processamento, o consumo de memória e a possibilidade de execução local.

No campo do aprendizado profundo, as redes neurais convolucionais (CNN) e as redes recorrentes com memória de longo e curto prazo (LSTM) têm sido amplamente exploradas para a análise de texto, aproveitando sua capacidade de capturar dependências sequenciais e padrões locais nas mensagens. Arquiteturas

híbridas que combinam CNN e LSTM mostraram resultados expressivos, atingindo acurácias superiores a 99% em alguns conjuntos de dados (MEHMOOD et al., 2024). Mais recentemente, modelos baseados em Transformers, como o DistilBERT, têm sido adaptados para essa tarefa, oferecendo representações semânticas mais ricas do texto, embora com custo computacional mais elevado (LOPES; GONÇALVES; BENFICA, 2026).

A qualidade e a representatividade dos conjuntos de dados utilizados para treinamento são fatores determinantes para o desempenho dos modelos. Grande parte dos estudos utiliza *datasets* públicos compostos majoritariamente por mensagens em inglês, o que limita a aplicabilidade das soluções em contextos multilíngues. A ausência de dados rotulados em português, por exemplo, é apontada como um dos principais entraves para o desenvolvimento de sistemas eficazes para o mercado brasileiro.

Além da escolha do algoritmo, o processo de detecção depende das características utilizadas como entrada e do pré-processamento aplicado aos dados. Em mensagens de texto, por exemplo, podem ser necessárias etapas como normalização, remoção de elementos irrelevantes e transformação do conteúdo textual em características que possam ser utilizadas pelo modelo. No caso das URLs, podem ser extraídos atributos relacionados ao domínio, comprimento, quantidade de caracteres especiais e estrutura do endereço. Essas características são então utilizadas pelo algoritmo para realizar a classificação. Em um dispositivo móvel, esse processo deve ainda considerar o custo computacional das etapas de pré-processamento e inferência, buscando um equilíbrio entre capacidade de detecção e utilização dos recursos disponíveis.

3.3 Desafios computacionais em ambientes móveis

A aplicação de modelos de aprendizado de máquina em dispositivos móveis impõe restrições que não estão presentes em ambientes de servidor. Smartphones e tablets operam com processadores de menor capacidade, memória RAM limitada e bateria como recurso finito. Executar modelos computacionalmente intensivos

nesses dispositivos pode resultar em latência perceptível, consumo excessivo de energia e, em casos extremos, travamentos do sistema (OLIVEIRA, 2024).

Uma estratégia amplamente adotada para contornar essas limitações é a compressão e otimização de modelos para inferência em dispositivos de borda. O formato ONNX (Open Neural Network Exchange), por exemplo, permite exportar modelos treinados em Python para um formato interoperável que pode ser carregado por *runtimes* otimizados para dispositivos móveis, reduzindo significativamente o tempo de inferência sem perdas substanciais de acurácia (ZARDO; EMER, 2024). Técnicas como quantização, que reduz a precisão numérica dos pesos do modelo, e *pruning*, que elimina parâmetros de menor importância, também têm sido exploradas para viabilizar o uso de arquiteturas mais complexas em dispositivos com recursos limitados. Nesse sentido, existe uma relação direta entre a complexidade do modelo e os recursos necessários para sua execução. Modelos mais simples tendem a apresentar menor tempo de inferência e consumo de memória, enquanto arquiteturas mais complexas podem oferecer maior capacidade de representação, mas exigir mais processamento. Assim, em aplicações móveis de detecção de *phishing*, a escolha da abordagem deve considerar não apenas o desempenho obtido nos testes, mas também a viabilidade de execução no dispositivo utilizado.

Outro desafio relevante é a necessidade de funcionamento *offline*. Soluções que dependem de consultas a serviços externos, como listas negras de *URLs* ou APIs de reputação, ficam inoperantes quando o dispositivo não possui conectividade. Isso é especialmente problemático em contextos de ataques que exploram justamente momentos de menor atenção do usuário, que muitas vezes ocorrem em ambientes sem acesso estável à internet. O desenvolvimento de modelos embarcados, capazes de operar inteiramente no dispositivo, é apontado como uma necessidade crescente pela literatura (OLIVEIRA, 2024; MISHRA; SONI, 2023).

A atualização contínua dos modelos é outra questão crítica. Técnicas de *phishing* evoluem rapidamente, e um modelo treinado com dados de alguns meses

atrás pode apresentar queda significativa de desempenho frente a novas campanhas de ataque. Em servidores, essa atualização pode ser feita de forma centralizada e transparente. Em dispositivos móveis, porém, ela exige mecanismos de atualização incremental ou aprendizado federado, abordagem em que modelos são refinados localmente em cada dispositivo sem que os dados brutos sejam transmitidos para um servidor central, preservando a privacidade do usuário.

3.4 Aplicativos e ferramentas de proteção contra phishing

Além das abordagens algorítmicas, a literatura recente registra iniciativas voltadas ao desenvolvimento de aplicativos móveis que integram diferentes mecanismos de proteção. Essas soluções geralmente combinam verificação em tempo real de *URLs*, consulta a listas negras, análise de conteúdo textual e, em alguns casos, gamificação para educar os usuários sobre os riscos do *phishing* (CARDOSO, 2024; ERHARD, 2025).

O uso de APIs externas de reputação, como o Google Safe Browsing, é uma estratégia recorrente por oferecer ampla cobertura com baixo esforço de implementação. Contudo, essa abordagem apresenta limitações importantes: a eficácia depende da atualização da base de dados do provedor, o que pode deixar janelas de vulnerabilidade para *sites* maliciosos recém-criados, e o funcionamento é comprometido sem conectividade à internet (FERREIRA; FREITAS, 2024).

Soluções baseadas em análise de DNS, como o sistema desenvolvido por Montagner (2023), oferecem uma camada de proteção mais transparente para o usuário, atuando no nível da resolução de nomes de domínio. Esse tipo de abordagem é particularmente eficaz para bloquear domínios maliciosos conhecidos, mas apresenta dificuldades frente a técnicas que utilizam domínios legítimos como vetores, como o uso indevido de serviços de encurtamento de *URL*.

A análise forense de mensagens e *e-mails* suspeitos, exemplificada pelo trabalho de Camargo (2023) com a ferramenta PhishTool, é relevante especialmente para profissionais de segurança que precisam investigar incidentes. Embora não seja uma solução para o usuário final, esse tipo de ferramenta contribui para o

entendimento das táticas utilizadas pelos atacantes e para a alimentação de bases de dados que subsidiam o treinamento de modelos automatizados.

4 METODOLOGIA

Esta pesquisa é uma revisão bibliográfica de carácter qualitativo e quantitativo, com abordagem exploratória e descritiva. Do ponto de vista dos procedimentos técnicos, segue o modelo de revisão sistemática da literatura, que se distingue das revisões narrativas tradicionais por adotar um protocolo explícito e replicável de busca, seleção e análise das fontes, reduzindo o risco de vieses na escolha dos trabalhos incluídos (PREETI; SHARMA, 2024). Para garantir a replicabilidade, o protocolo adotado nesta pesquisa seguiu as seguintes etapas em ordem: (1) definição dos critérios de inclusão e exclusão antes do início das buscas; (2) execução das buscas nas bases IEEE Xplore, ACM Digital Library, Scopus, Google Scholar e BDTD, utilizando os termos "phishing detection", "smishing", "mobile security", "machine learning mobile", "detecção de phishing" e "segurança móvel", isolados e em combinação; (3) triagem por título e resumo; (4) leitura integral dos textos selecionados; e (5) extração dos dados segundo protocolo padronizado. O foco central foi mapear e sintetizar o estado da arte na detecção de phishing em dispositivos móveis, com atenção especial aos aspectos técnicos e computacionais das soluções propostas na literatura recente.

Antes de iniciar as buscas, foram definidos os critérios que um trabalho precisaria atender para ser incluído na revisão. O primeiro critério era temático: o estudo deveria tratar diretamente da detecção automatizada de *phishing*, *smishing*, *vishing* ou *quishing*. O segundo era contextual: o trabalho deveria envolver dispositivos móveis como plataforma alvo ou demonstrar aplicabilidade clara nesse ambiente. O terceiro era técnico: era necessário que houvesse alguma contribuição computacional concreta, seja no desenvolvimento ou avaliação de algoritmos, na implementação de aplicativos de proteção ou na análise de vulnerabilidades específicas do ambiente móvel. Trabalhos voltados exclusivamente ao comportamento do usuário, sem qualquer componente técnico de detecção, foram considerados fora do escopo principal, embora estudos sobre conscientização e

educação tenham sido aceitos quando complementam a análise técnica de forma relevante.

As buscas foram conduzidas entre os meses de abril e julho de 2026 nas seguintes bases de dados: IEEE Xplore, ACM Digital Library, Scopus e Google Scholar, além da Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) e repositórios institucionais de USP, UFRJ, UNESP, UFSC, PUC Minas, PUCRS, Mackenzie e FATEC. Foram consultados também os anais do SBSEG e publicações da RISTI. Cada base foi pesquisada de forma independente, utilizando os seguintes termos isolados e em combinação: "phishing detection", "smishing detection", "mobile security", "machine learning mobile phishing", "deep learning smishing", "Android security", "URL analysis phishing" e "SMS fraud detection", e seus equivalentes em português. O número de resultados retornados por base não foi registrado individualmente, mas o total de registros encontrados antes da triagem foi de 85. Quanto à inclusão excepcional do artigo disponível no arXiv, o critério adotado foi a relevância técnica da contribuição combinada à evidência de submissão para publicação em periódico com revisão por pares, verificada no momento da coleta. A qualidade dos estudos foi avaliada com base na clareza metodológica, na descrição dos experimentos e na identificação das limitações pelos próprios autores.

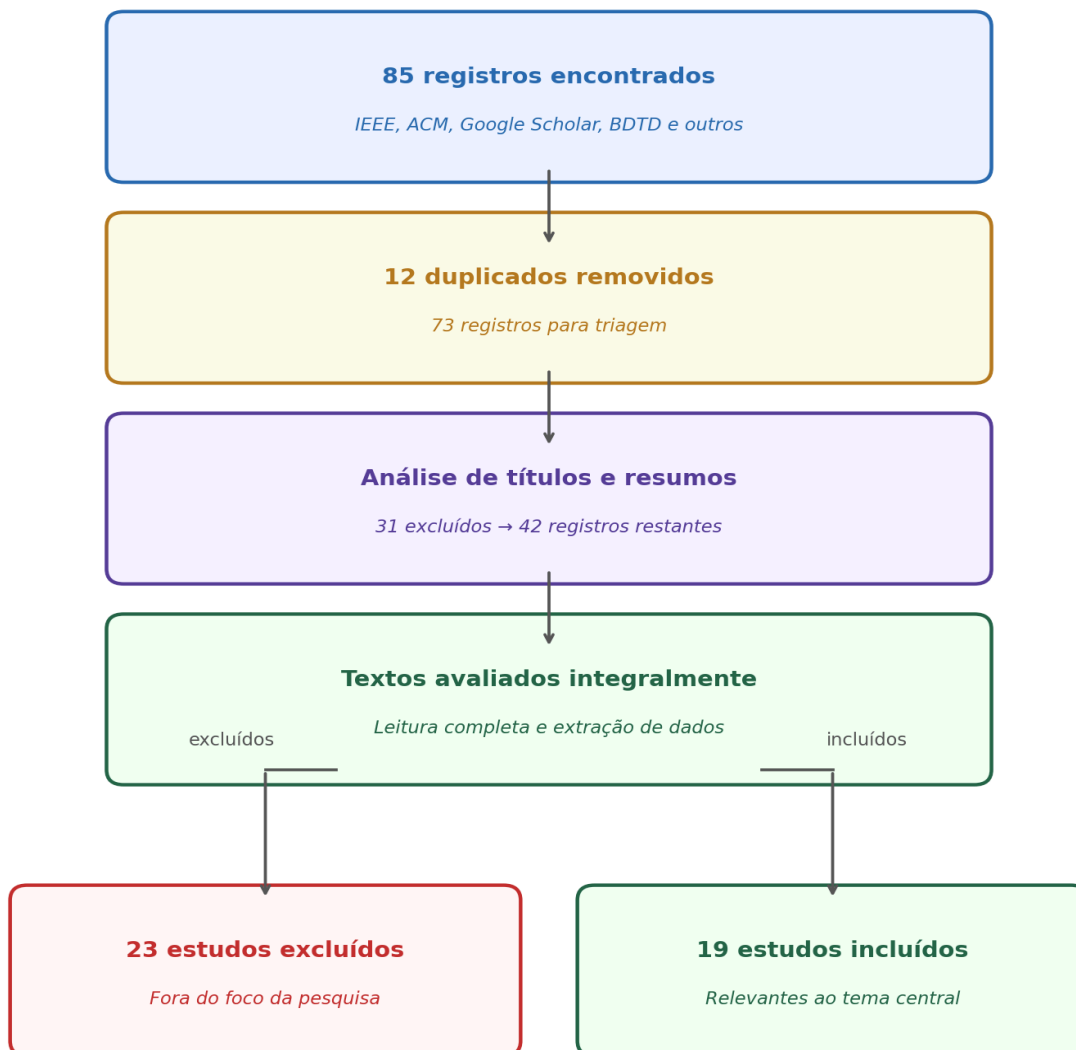
O recorte temporal definido foi de 2022 a 2026. A escolha não foi arbitrária. O campo evolui em ritmo acelerado, e trabalhos com mais de quatro ou cinco anos tendem a descrever cenários técnicos já bastante superados, tanto em termos do *hardware* disponível nos dispositivos quanto das capacidades dos algoritmos. O período escolhido captura, em particular, a consolidação das arquiteturas baseadas em Transformers para processamento de texto, como o BERT e suas variantes mais compactas, que representam uma mudança qualitativa significativa em relação às abordagens anteriores. Quando necessário, foram aceitas referências anteriores a 2022 desde que se tratasse de trabalhos seminais ou de revisões com relevância consolidada para o tema.

A triagem dos trabalhos encontrados ocorreu em três etapas sucessivas. Na primeira, os resultados das buscas foram filtrados por título e palavras-chave,

eliminando rapidamente os trabalhos claramente fora do escopo. Na segunda etapa, os resumos dos candidatos remanescentes foram lidos na íntegra, permitindo uma avaliação mais precisa da pertinência de cada estudo. Na terceira etapa, os textos completos foram lidos e analisados com base no protocolo de extração definido previamente. Foram excluídos: trabalhos que abordavam *phishing* exclusivamente em ambientes desktop, sem qualquer menção ao contexto móvel; estudos sem metodologia clara de avaliação experimental, que não permitiam comparação objetiva dos resultados; versões duplicadas de um mesmo estudo, nesses casos, manteve-se a versão mais completa; e textos em estágio de *preprint* sem revisão por pares, com uma única exceção: um artigo disponível no arXiv foi incluído por apresentar contribuição técnica considerada relevante e por ter sido posteriormente aceito para publicação em periódico.

O processo de seleção dos estudos está representado na Figura 2. A busca inicial resultou em 85 registros encontrados nas bases de dados consultadas. Em seguida, foram removidos os trabalhos duplicados ou com temáticas sobrepostas. Os registros restantes passaram por uma análise de títulos e resumos, etapa em que foram eliminados os trabalhos claramente fora do escopo da pesquisa. Os candidatos remanescentes tiveram seus textos avaliados integralmente, o que permitiu identificar os estudos que fugiam do foco central da investigação. Ao final desse processo, chegou-se a dezenove trabalhos considerados relevantes ao tema e incluídos na revisão.

Figura 2 - Fluxograma de seleção dos estudos



Fonte: Elaborado pelo autor (2026.)

Ao final da triagem, chegou-se a dezenove trabalhos, que compõem o *corpus* principal desta revisão. Para organizar a análise, eles foram agrupados em três blocos temáticos. O Bloco A, o mais numeroso, reúne dez estudos dedicados ao desenvolvimento e à avaliação de algoritmos de aprendizado de máquina e aprendizado profundo para detecção de *smishing* e *phishing*. O Bloco B agrupa seis trabalhos voltados à implementação de aplicativos e ferramentas de proteção para usuários finais em dispositivos móveis. O Bloco C reúne três estudos de natureza complementar, que abordam vulnerabilidades gerais de segurança móvel, comportamento do usuário diante de tentativas de *phishing* e aspectos legais das fraudes digitais.

Cada trabalho foi analisado com base em um protocolo de extração estruturado, criado especificamente para esta revisão. Os campos registrados incluíam: identificação completa do estudo (autores, título, veículo de publicação e ano); tipo de contribuição (experimental, comparativo, proposta de sistema ou revisão); técnica ou algoritmo principal empregado; métricas de desempenho reportadas, com ênfase na acurácia, mas também registrando precisão, *recall*, F1-score e AUC quando disponíveis; plataforma alvo (Android, iOS, multiplataforma ou independente); tipo de dado processado (mensagens *SMS*, *URLs*, *e-mails*, *QR codes*); idioma do *corpus* utilizado no treinamento e nos testes; e principais limitações identificadas, tanto as reconhecidas pelos próprios autores quanto as inferidas a partir de uma leitura crítica dos resultados. Esses dados foram consolidados em planilha de controle e depois sintetizados no Quadro 1, apresentado na seção seguinte.

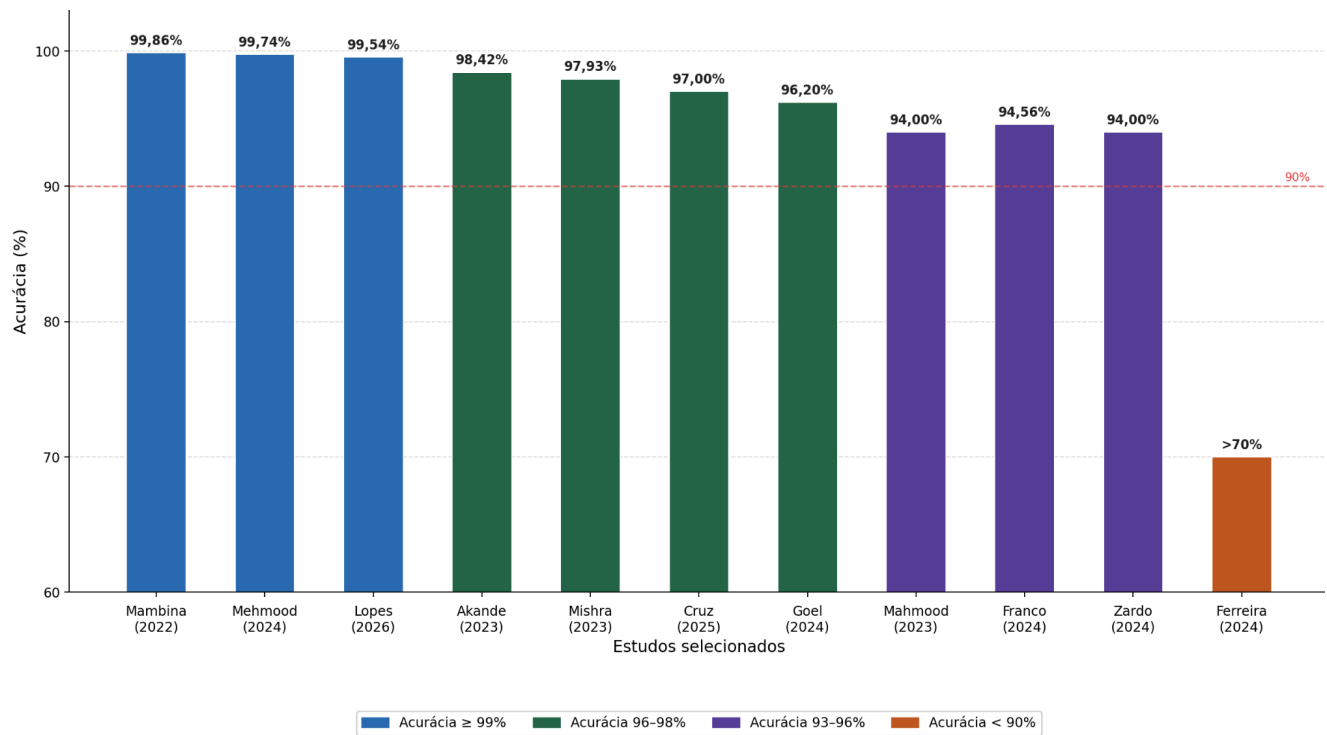
Por fim, vale registrar uma ressalva importante para a interpretação dos resultados. Como esta é uma revisão bibliográfica, e não um estudo experimental primário, os dados de desempenho apresentados refletem as condições específicas de cada pesquisa original: conjuntos de dados diferentes, configurações de *hardware* distintas e metodologias de validação variadas. Isso significa que comparações diretas entre estudos são aproximadas, não absolutas. Ter isso em mente é fundamental para não tirar conclusões apressadas a partir dos números apresentados no Quadro 1.

5 RESULTADOS E DISCUSSÃO

A análise dos dezenove trabalhos selecionados revela um campo em crescimento acelerado, com soluções cada vez mais sofisticadas em termos de acurácia, mas que ainda enfrentam desafios consideráveis quando o critério de avaliação vai além do desempenho em *datasets* controlados. Os resultados são apresentados a seguir, organizados pelos blocos temáticos definidos na metodologia.

A Figura 3 apresenta as taxas de acurácia reportadas pelos onze estudos do corpus que realizaram avaliação experimental quantitativa. Os demais oito trabalhos não reportaram esse dado por se tratar de revisões de literatura, análises forenses, aplicativos educativos ou estudos de natureza jurídica. É importante ressaltar que os valores apresentados não são diretamente comparáveis entre si: cada estudo foi conduzido com datasets distintos, em idiomas diferentes, com métodos de validação variados e em ambientes de hardware específicos. Portanto, a figura deve ser lida como um panorama geral do desempenho relatado na literatura, e não como um ranking absoluto de eficácia dos algoritmos. Com essa ressalva, os resultados indicam desempenho elevado na maioria dos casos, com destaque para Mambina et al. (2022), Mehmood et al. (2024) e Lopes et al. (2026), que superaram 99% de acurácia em seus respectivos contextos de teste. O estudo de Ferreira e Freitas (2024) apresentou o menor desempenho, com acurácia superior a 70%, reflexo da abordagem adotada, baseada em API externa em vez de modelo próprio treinado.

Figura 3 — Acurácia dos estudos selecionados (2021–2026)



Fonte: Elaborado pelo autor (2026).

O Quadro 1 apresenta uma síntese comparativa dos principais estudos do Bloco A, que reúne as abordagens baseadas em aprendizado de máquina e aprendizado profundo.

Quadro 1 – Comparativo das principais abordagens de detecção de smishing/phishing (2022–2026)

Autor(es)/Ano	Técnica Principal	Acurácia	Plataforma	Limitação Identificada
Akande et al. (2023)	RIPPER / C4.5 – App Android	98,42%	Android	Dataset limitado a SMS em inglês
Mishra e Soni (2023)	Backpropagation + verificação de domínio	97,93%	Android	Dependência de conectividade
Zardo e Emer (2024)	Random Forest exportado via ONNX	94,00%	Android	Vocabulário fixo, sem atualização online
Goel et al. (2024)	Naïve Bayes + normalização textual	96,20%	Independente	Baixa robustez a variações linguísticas
Mambina et al. (2022)	ExtraTrees + TF-IDF (Suaíli)	99,86%	Independente	Corpus monolíngue, Swahili
Mehmood et al. (2024)	CNN-LSTM híbrido	99,74%	Independente	Custo computacional elevado
Franco (2024)	Random Forest + LSTM (AUC 0,99)	94,56%	Independente	LSTM exige GPU para treinamento
Lopes et al. (2026)	DistilBERT + CNN + BiLSTM + MLP	99,54%	Multicanal	Modelo grande; inferência 6,91ms/amostra
Cruz (2025)	XGBoost / LightGBM para URLs	96–98%	Independente	Foco em URL; ignora conteúdo da página
Ferreira e Freitas (2024)	Flutter + Google Safe Browsing	>70%	iOS/Android	Acurácia básica; depende de API externa
Erhard (2025)	NLP + listas negras + VirusTotal	N/A	Android	Dependência de serviços de terceiros

Fonte: Elaborado pelo autor (2026).

Os dados compilados no Quadro 1 sugerem uma tendência na literatura: algoritmos baseados em aprendizado de máquina clássico, especialmente o Random Forest, tendem a apresentar boa acurácia com menor complexidade de implementação. Contudo, é importante destacar que a maioria dos estudos não reportou métricas comparáveis de custo computacional, como latência, consumo de memória, energia ou tamanho do modelo, o que impede afirmar de forma uniforme que essas abordagens são mais eficientes para dispositivos móveis. As exceções são Akande et al. (2023), que integraram algoritmos RIPPER e C4.5 diretamente em um aplicativo Android atingindo 98,42% de acurácia, e Zardo e Emer (2024), que reportaram explicitamente a latência adequada para uso em tempo real ao exportar um modelo Random Forest no formato ONNX, alcançando 94% de acurácia. Esses dois casos são os que oferecem evidências mais concretas sobre viabilidade em ambientes móveis com recursos limitados.

As arquiteturas de aprendizado profundo, por sua vez, tendem a alcançar acurácias ainda mais elevadas, com destaque para o modelo CNN-LSTM de Mehmood et al. (2024), que atingiu 99,74%, e a abordagem multimodal de Lopes, Gonçalves e Benfica (2026), com 99,54%, mas impõem custos computacionais que dificultam sua execução direta em dispositivos de menor capacidade. A proposta de Lopes et al. (2026), por exemplo, reporta um tempo de inferência de 6,91ms por amostra, o que é aceitável em termos absolutos, mas exige *hardware* compatível que não está presente em todos os smartphones do mercado brasileiro.

Um achado relevante diz respeito à diversidade linguística das soluções. A grande maioria dos trabalhos foi desenvolvida e validada com *datasets* em inglês, o que limita sua aplicabilidade direta ao contexto brasileiro. A exceção mais notável é o estudo de Mambina, Ndia Wile e Michael (2022), que desenvolveu e avaliou um classificador para mensagens em suaíli, atingindo acurácia de 99,86% com ExtraTrees e TF-IDF. Embora o idioma seja diferente, esse trabalho demonstra que é tecnicamente viável alcançar alto desempenho em línguas distintas do inglês, desde que haja um *corpus* adequado disponível. A ausência de *datasets* públicos em

português para *smishing* é, portanto, uma das lacunas mais críticas identificadas nesta revisão.

No Bloco B, os estudos voltados ao desenvolvimento de aplicativos revelam uma tendência de integração entre múltiplas camadas de proteção. O aplicativo desenvolvido por Erhard (2025) combina processamento de linguagem natural, consulta a listas negras, integração com a API do VirusTotal e geolocalização para fornecer uma análise multidimensional das ameaças. Essa abordagem é promissora, mas a dependência de serviços externos representa um ponto de vulnerabilidade em situações de conectividade reduzida.

O trabalho de Ferreira e Freitas (2024) apresenta uma solução desenvolvida em Flutter, *framework* que permite criar aplicativos para Android e iOS a partir de uma única base de código,, integrando o Google Safe Browsing para verificação de *URLs* e o LanguageTool para análise gramatical de mensagens suspeitas. Embora a acurácia reportada seja inferior à dos modelos de aprendizado de máquina, superior a 70%, a solução tem o mérito de ser portátil entre plataformas e de não exigir treinamento de modelos customizados, o que facilita sua manutenção e atualização.

O aplicativo SaPhish, desenvolvido por Cardoso (2024) com foco em gamificação e educação do usuário, apresenta uma perspectiva complementar às abordagens de detecção automatizada. Os dados de avaliação indicam que 92,6% dos participantes consideraram o conteúdo de fácil compreensão e 81,5% afirmaram que utilizariam o aplicativo no cotidiano. Esses resultados reforçam a importância da dimensão educacional no combate ao *phishing*: a tecnologia, por mais sofisticada que seja, não elimina por si só o risco enquanto o usuário permanecer vulnerável à manipulação psicológica.

Os trabalhos do Bloco C trazem perspectivas complementares que enriquecem a análise. O estudo de Oliveira (2024), voltado para a revisão de vulnerabilidades em dispositivos móveis, contextualiza os ataques de *phishing* dentro de um ecossistema mais amplo de ameaças, que inclui *malware*, ataques via *Bluetooth* e exploração de permissões excessivas de aplicativos. Bezerra, Millian e

Silva (2024) contribuem com dados empíricos sobre o comportamento do usuário frente a tentativas de *phishing* simuladas, documentando que 61% das páginas falsas identificadas nos experimentos imitavam instituições bancárias, reforçando a necessidade de soluções específicas para esse segmento.

De forma geral, a análise dos trabalhos aponta para três tensões que aparecem repetidamente na literatura. A primeira diz respeito ao equilíbrio entre desempenho e eficiência computacional: modelos mais precisos tendem a ser mais pesados, mas poucos estudos fornecem métricas suficientes como latência, consumo de memória ou tamanho do modelo, para sustentar comparações objetivas de viabilidade em dispositivos móveis. A segunda envolve a dificuldade de generalização: algoritmos treinados em datasets restritos e majoritariamente em inglês costumam falhar quando expostos a ataques com características distintas das amostras de treinamento, o que é especialmente crítico para o contexto brasileiro. A terceira, talvez a mais difícil de resolver tecnicamente, é o debate entre automação e educação do usuário, se vale mais investir em sistemas que protejam de forma transparente ou em soluções que desenvolvam a capacidade crítica do usuário para identificar ameaças. Vale ressaltar que essas tensões são identificadas com base nos dados disponíveis nos estudos analisados, sendo que nem todos forneceram informações suficientes para sustentar conclusões definitivas sobre eficiência computacional.

6 CONSIDERAÇÕES FINAIS

Esta revisão bibliográfica buscou mapear e analisar os principais desafios técnicos e computacionais na detecção de phishing em dispositivos móveis, com base em dezenove trabalhos publicados entre 2022 e 2026. Os resultados extraídos diretamente do corpus indicam que a área avançou de forma expressiva nos últimos anos: dos onze estudos que reportaram métricas quantitativas, dez alcançaram acurácia superior a 94% em seus respectivos ambientes de teste controlados, sendo que três superaram 99%. Esses números, porém, devem ser interpretados com cautela, pois foram obtidos em condições específicas de cada pesquisa, com datasets, idiomas e métodos de validação distintos, o que impede generalizações diretas.

No entanto, a transposição dessas soluções para a realidade dos dispositivos móveis ainda encontra obstáculos significativos. As restrições de processamento e memória dificultam o uso direto de modelos mais complexos. A dependência de conjuntos de dados em inglês limita a aplicabilidade no contexto brasileiro. A necessidade de conectividade para consultas a serviços externos representa um ponto de falha em situações críticas. E a rápida evolução das táticas de ataque exige mecanismos de atualização contínua que nem sempre são viáveis em ambientes móveis.

A pesquisa também evidenciou lacunas relevantes que merecem atenção em trabalhos futuros. A principal delas é a escassez de *datasets* em português especificamente voltados para *smishing*, o que representa uma barreira concreta para o desenvolvimento de soluções adaptadas à realidade do usuário brasileiro. Outra lacuna identificada é a ausência de estudos que avaliem o desempenho dos modelos em condições reais de uso, com variabilidade de *hardware*, versões de sistema operacional e perfis de usuário,, em contraste com os experimentos em *datasets* estáticos que dominam a literatura atual.

Entre os caminhos mais promissores para pesquisas futuras, destacam-se: o desenvolvimento de modelos leves e quantizados para smartphones de baixo custo, sustentado pela evidência de Zardo e Emer (2024), que demonstraram viabilidade dessa abordagem com Random Forest exportado via ONNX; a criação de *datasets* públicos em português para *smishing*, lacuna identificada em praticamente todos os estudos analisados que trabalham com língua inglesa; e o desenvolvimento de mecanismos de atualização contínua dos modelos em dispositivos móveis, necessidade apontada por Mishra e Soni (2023) e Oliveira (2024) diante da rápida evolução das táticas de ataque; A integração entre detecção automatizada e educação do usuário também se mostra promissora, considerando os resultados de Cardoso (2024), cujo aplicativo gamificado obteve alta aceitação entre os participantes. Essas direções decorrem diretamente das limitações e lacunas identificadas nos estudos revisados.

Por fim, cabe registrar que, embora esta revisão tenha sido conduzida com rigor metodológico, ela possui limitações inerentes ao próprio recorte realizado. A

seleção de dezenove trabalhos, por mais representativa que seja do estado da arte recente, não esgota a produção científica na área. Trabalhos em outros idiomas, produções em conferências de menor circulação e desenvolvimentos em andamento não publicados formalmente ficaram necessariamente fora do escopo. Espera-se, contudo, que os achados desta pesquisa possam servir de ponto de partida tanto para profissionais que atuam na área de segurança da informação quanto para pesquisadores interessados em aprofundar o conhecimento sobre a detecção de ameaças em ambientes móveis.

REFERÊNCIAS

- AKANDE, O. *et al.* SMSPROTECT: detecção de *smishing* em dispositivos Android com algoritmos RIPPER e C4.5. *ICT Express*, v. 9, p. 168-176, 2023.
- BEZERRA, C.; MILLIAN, L.; SILVA, R. *Estudo de técnicas de phishing e comportamento do usuário*. Revista Mackenzie de Tecnologia, São Paulo, 2024.
- CAMARGO, F. *Análise técnica de e-mails de phishing com PhishTool: um estudo de caso*. FATEC Americana, 2023.
- CARDOSO, M. *SaPhish: aplicativo gamificado para conscientização sobre phishing*. UFRJ, 2024.
- CETIC.BR. *Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil: TIC domicílios 2024/2025*. São Paulo: Comitê Gestor da Internet no Brasil, 2025.
- CRUZ, A. *Detecção de phishing por métodos ensemble: XGBoost e LightGBM aplicados à análise de URLs*. UNESP, 2025.
- ERHARD, P. *Phishing Tracker: aplicativo Android para detecção de phishing com NLP e geolocalização*. FATEC São Paulo, 2025.
- FERREIRA, L.; FREITAS, T. *Desenvolvimento de aplicativo para detecção de phishing em dispositivos móveis*. PUC Minas, 2024.
- FRANCO, B. *Filtros de alta precisão para SMS fraudulentas: comparação de 14 algoritmos de aprendizado de máquina*. USP, 2024.
- GOEL, S. *et al.* *Machine learning driven smishing detection framework*. arXiv:2412.09641, 2024.
- GUARIZI, R.; MASCARENHAS, J. *Otimização de algoritmos XGBoost para ambientes móveis: acurácia e desempenho*. Revista Brasileira de Segurança Digital, São Paulo, v. 12, n. 2, p. 45-60, 2025.
- IBM. *O que é engenharia social?* [S. l.]: IBM Education, 2025. Disponível em: <https://www.ibm.com/br-pt/topics/social-engineering>. Acesso em: mar. 2026.
- KASPERSKY. *Epidemia de phishing em 2025: como o Brasil se tornou líder em ataques cibernéticos*. [S. l.]: Kaspersky Lab, 2025.
- LECUN, Y.; BENGIO, Y.; HINTON, G. *Deep learning*. *Nature*, v. 521, n. 7553, p. 436-444, 2015.
- LEE, S. *et al.* Phish-Jam: a lightweight deep learning architecture for mobile phishing detection. *Journal of Cyber Systems*, v. 8, n. 1, p. 112-128, jan. 2025.
- LOPES, J.; GONÇALVES, M.; BENFICA, R. *Detecção de phishing multicanal com arquitetura DistilBERT+CNN+BiLSTM+MLP*. RISTI, n. E78, p. 83-97, 2026.

- MAHMOOD, A.; HAMEED, D. *Review of smishing detection approaches via machine learning*. Iraqi Journal of Science, v. 64, n. 8, p. 4244-4259, 2023.
- MAMBINA, P.; NDIBWILE, J.; MICHAEL, E. *Classifying Swahili smishing attacks using machine learning*. IEEE Access, v. 10, p. 83061-83074, 2022.
- MEHMOOD, U. *et al.* Enhancing smishing detection using CNN-LSTM hybrid architecture. IEEE Access, v. 12, p. 137176-137193, 2024.
- MISHRA, P.; SONI, D. *DSmishSMS: detecção de smishing com verificação de domínio e backpropagation*. Neural Computing and Applications, v. 35, p. 4975-4992, 2023.
- MITCHELL, T. M. *Machine Learning*. McGraw-Hill, 2025.
- MONTAGNER, F. *Sistema de detecção de requisições web maliciosas baseado em análise de DNS*. UFSC, 2023.
- MORA, A. J. *et al.* Normalização linguística e detecção de smishing em mensagens curtas. In: SBSEG, 24., 2024, São José dos Campos. Anais [...]. SBC, 2024. p. 210-222.
- NUNES, E. *Engenharia social: a face humana na cibersegurança*. PUC-Rio, 2025.
- OLIVEIRA, R. *Ameaças à segurança em dispositivos móveis: uma revisão de vulnerabilidades e boas práticas*. IFPB, 2024.
- PREETI, R.; SHARMA, K. *Machine learning in cybersecurity: a systematic review (2020-2024)*. International Journal of Information Security, v. 23, n. 4, p. 567-589, 2024.
- SANTOS, A.; VASCONCELLOS, B. *Análise comparativa de algoritmos de inteligência artificial para detecção de smishing*. PUCRS, 2024.
- SANTOS, Maiza. *A fraude eletrônica como nova modalidade de estelionato no direito penal brasileiro*. UNINOVE, 2025.
- WANG, J. *et al.* The evolution of quishing: QR code phishing attacks and mitigation via quantized LLMs. *Mobile Security Review*, v. 15, n. 3, p. 89-105, 2025.
- ZARDO, E.; EMER, M. *Detecção de smishing em dispositivos Android usando aprendizado de máquina e ONNX*. IFRS, 2024.