

Análise forense de dispositivos móveis: desafios técnicos na extração, preservação e validação de evidências digitais

Mobile device forensics: technical challenges in the extraction, preservation, and validation of digital evidence

Vanderlei Alves Ferreira¹

Resumo

Esta pesquisa analisa os principais desafios técnicos relacionados à extração, à preservação e à validação de evidências digitais em dispositivos móveis. O estudo parte da constatação de que smartphones concentram dados relevantes para investigações criminais, mas apresentam arquiteturas de segurança, criptografia, mecanismos de bloqueio e processos de atualização que limitam o acesso e tornam o exame dependente do estado específico do aparelho. Adotou-se abordagem qualitativa, exploratória e descritiva, com pesquisa bibliográfica e documental. O corpus foi formado por 27 fontes acadêmicas, normativas, técnicas, institucionais e legais, analisadas nas categorias métodos de extração, desafios técnicos, preservação e cadeia de custódia, validação e confiabilidade. Os resultados demonstram que não existe método de extração universalmente superior: a adequação depende do objetivo pericial, do modelo, da versão do sistema, do estado de bloqueio e dos riscos de alteração. Verificou-se também que a integridade da prova não decorre apenas do cálculo de hash, mas de um conjunto documentado de decisões, controles, cópias, registros e verificações. A confiabilidade exige validação da ferramenta e do método no contexto concreto, confirmação independente dos artefatos relevantes e comunicação expressa das limitações. Conclui-se que a segurança metodológica resulta da integração entre preservação do estado, aquisição proporcional, análise contextual, rastreabilidade e revisão técnica, sendo recomendável que laboratórios mantenham protocolos adaptáveis, testes por versão e documentação suficiente para permitir o escrutínio dos resultados. Como contribuição aplicada, propõe-se um modelo integrado de segurança metodológica e instrumentos de apoio ao planejamento, à revisão e ao relato pericial.

¹ Universidad Europea del Atlántico (UNEATLANTICO) – Santander – Cantábria – Espanha

Palavras-chave: evidência digital; dispositivos móveis; análise forense; cadeia de custódia; validação.

Abstract

This research analyzes the main technical challenges related to the extraction, preservation, and validation of digital evidence from mobile devices. Smartphones contain information of high relevance to criminal investigations, yet their security architectures, encryption, locking mechanisms, and continuous updates restrict access and make examinations dependent on the specific state of each device. A qualitative, exploratory, and descriptive approach was adopted through bibliographic and documentary research. The corpus comprised 27 academic, normative, technical, institutional, and legal sources, organized into extraction methods, technical challenges, preservation and chain of custody, validation, and reliability. The results show that no extraction method is universally superior: suitability depends on the forensic objective, device model, operating-system version, lock state, and risk of alteration. Evidence integrity was also found to depend on more than hash calculation; it requires a documented set of decisions, controls, copies, records, and verification procedures. Reliable findings require validation of both tools and methods in the specific context, independent confirmation of relevant artifacts, and explicit disclosure of limitations. It is concluded that methodological assurance results from integrating state preservation, proportionate acquisition, contextual analysis, traceability, and technical review. Forensic laboratories should therefore maintain adaptable protocols, version-specific testing, and documentation sufficient to support independent scrutiny of their results. As an applied contribution, an integrated methodological assurance model and practical instruments for planning, review, and forensic reporting are proposed.

Keywords: digital evidence; mobile devices; digital forensics; chain of custody; validation.

1 Introdução

Os dispositivos móveis deixaram de ser simples instrumentos de telefonia e passaram a concentrar atividades pessoais, profissionais e financeiras. Mensagens, imagens, documentos, registros de acesso, dados de localização e informações produzidas por aplicativos compõem uma representação fragmentada da rotina de seus usuários. Quando relacionados a um fato investigado, esses registros podem contribuir para estabelecer vínculos, sequências temporais e circunstâncias relevantes. A centralidade do smartphone na

vida cotidiana explica por que sua apreensão e seu exame se tornaram frequentes em investigações criminais, mas também torna a análise tecnicamente mais complexa, pois um único aparelho reúne diferentes camadas de hardware, sistema operacional, aplicativos e serviços remotos (Fukami et al., 2021; Lyle et al., 2022).

A utilidade investigativa desses dados depende de um percurso que não se resume a localizar uma informação de interesse. É necessário identificar corretamente o dispositivo, preservar seu estado, escolher um método de aquisição compatível, registrar as intervenções efetuadas e interpretar os artefatos dentro de seu contexto técnico. A evidência digital é especialmente sensível a mudanças: uma conexão de rede, uma inicialização, a sincronização automática ou a execução de uma ferramenta pode criar, modificar ou eliminar registros. Por essa razão, a qualidade do resultado está ligada tanto ao conteúdo recuperado quanto à transparência do procedimento que permitiu recuperá-lo (International Organization for Standardization [ISO], 2012; Scientific Working Group on Digital Evidence [SWGDE], 2025).

O problema torna-se mais evidente nos smartphones atuais. Criptografia baseada em arquivo, proteção de chaves por hardware, códigos de acesso, biometria e mecanismos de inicialização verificada foram incorporados para proteger a privacidade e reduzir acessos não autorizados. Essas medidas são legítimas e necessárias, porém alteram as possibilidades forenses. Uma aquisição que funcionava em determinada versão pode deixar de funcionar depois de uma atualização; dados visíveis enquanto o aparelho está desbloqueado podem ficar inacessíveis após uma reinicialização; e técnicas invasivas podem oferecer maior alcance ao custo de maior risco, menor repetibilidade e necessidade de fundamentação específica (Apple, 2024; Fukami et al., 2021; Google, 2026a).

Além do acesso, existe o desafio de demonstrar que os resultados são tecnicamente confiáveis. Ferramentas forenses automatizam etapas importantes, mas não são neutras nem infalíveis. Elas podem interpretar de modo diferente uma mesma base, omitir artefatos não suportados ou apresentar resultados sem tornar visíveis todas as transformações internas. A validação precisa considerar a ferramenta, o método e a aplicação concreta, incluindo versão do software, modelo do aparelho, sistema operacional, condições de aquisição e verificações independentes. A confiança, portanto, não decorre apenas da reputação comercial do produto, mas de testes documentados e da possibilidade de explicar como o resultado foi obtido (Hargreaves et al., 2024; Stoykova & Franke, 2023; SWGDE, 2024).

Nesse contexto, a pesquisa é orientada pela seguinte pergunta: quais são os principais desafios técnicos identificados pela literatura científica e normativa recente na extração, preservação e validação de evidências digitais em dispositivos móveis no contexto da análise forense? O recorte concentra-se em smartphones Android e iOS e nos procedimentos associados ao tratamento de dados armazenados no aparelho ou acessíveis a partir dele. Não se pretende avaliar um produto comercial específico nem executar testes laboratoriais. O interesse está em relacionar os problemas recorrentes descritos pela bibliografia com os requisitos de integridade, rastreabilidade, adequação metodológica e reprodutibilidade que sustentam a evidência digital (Almuqren et al., 2024; ISO, 2015a, 2015b).

O objetivo geral é analisar, por meio de pesquisa bibliográfica e documental, os principais desafios técnicos relacionados à extração, preservação e validação de evidências digitais em dispositivos móveis. Para alcançá-lo, o estudo identifica os métodos de extração descritos na literatura, descreve os obstáculos decorrentes da criptografia, dos mecanismos de bloqueio, da evolução dos sistemas operacionais e das limitações das ferramentas, examina a cadeia de custódia digital, verifica critérios internacionais de validação e sistematiza boas práticas capazes de aumentar a segurança metodológica do exame (Al-Dhaqm et al., 2020; Kumar, 2021; SWGDE, 2026).

A justificativa acadêmica e profissional decorre da distância que pode existir entre a disponibilidade de ferramentas e a compreensão de seus limites. A multiplicação de modelos, versões, aplicativos e formatos dificulta a padronização absoluta, enquanto a automação pode induzir à aceitação de uma interface como se ela representasse diretamente o dado original. Uma síntese crítica ajuda a distinguir aquisição, decodificação, apresentação e interpretação, reduzindo o risco de conclusões que excedam o que os artefatos efetivamente permitem afirmar. Também favorece relatórios mais claros, nos quais limitações e hipóteses alternativas sejam apresentadas ao destinatário da prova (Hargreaves et al., 2024; Lyle et al., 2022).

O trabalho adota abordagem qualitativa, finalidade exploratória e descritiva e procedimentos exclusivamente bibliográficos e documentais. O corpus é constituído por artigos científicos, normas técnicas, orientações de organismos especializados, documentação de segurança das plataformas e legislação pertinente. Não há entrevistas, questionários, grupos focais, observação de pessoas ou acesso a casos reais. A análise organiza as fontes nas categorias extração, preservação, validação e confiabilidade, buscando convergências, divergências e relações entre os desafios técnicos e as medidas de controle recomendadas (ISO, 2012, 2015a, 2015b; Lyle et al., 2022).

Após esta introdução, o texto apresenta os fundamentos da evidência digital e as particularidades dos dispositivos móveis. Em seguida, examina os métodos de extração, os obstáculos técnicos, a cadeia de custódia e os critérios de validação, encerrando o referencial com uma síntese crítica das boas práticas. O capítulo metodológico descreve o percurso da revisão. Na sequência, os resultados são organizados pelas categorias de análise, discutidos à luz do problema e dos objetivos e consolidados nas conclusões. Essa estrutura mantém distinguíveis obtenção, preservação, validação e interpretação, sem desconsiderar a interdependência existente entre essas dimensões (Al-Dhaqm et al., 2020; SWGDE, 2025, 2026).

A análise forense móvel situa-se em um ponto de tensão entre a abundância informacional e a crescente resistência técnica ao acesso. O mesmo dispositivo que registra comunicações, deslocamentos, autenticações e interações também aplica controles destinados a impedir leitura por terceiros. Essa dupla condição exige abandonar a ideia de que o smartphone é um repositório estático. Ele deve ser compreendido como um sistema em funcionamento, conectado a serviços, sujeito a processos automáticos e dependente de estados criptográficos transitórios. A decisão inicial — isolar, manter ligado, alimentar ou desligar — pode repercutir em todo o exame e precisa ser tratada como escolha metodológica justificável, e não como rotina indiferenciada (Apple, 2024; Fukami et al., 2021; SWGDE, 2025).

A contribuição central desta versão final consiste em articular os achados da literatura em um modelo de segurança metodológica aplicável ao planejamento e à avaliação do exame. O modelo não pretende substituir protocolos laboratoriais ou validar ferramentas específicas. Sua função é organizar seis dimensões que apareceram de forma convergente no corpus: conhecimento do estado e do contexto, proporcionalidade do método, preservação, rastreabilidade, validação e comunicação dos limites. Ao relacioná-las, torna-se possível verificar não apenas se um dado foi localizado, mas se o percurso entre a fonte e a conclusão permanece explicável e auditável. Essa perspectiva também permite identificar onde uma incerteza foi introduzida e qual controle pode reduzi-la (ISO, 2015a, 2015b; Lyle et al., 2022; Stoykova & Franke, 2023).

2 Revisão da literatura

2.1 Evidência digital e dispositivos móveis

Evidência digital pode ser entendida como informação de valor potencial para uma investigação que é armazenada ou transmitida em forma digital. O conceito abrange tanto o conteúdo percebido pelo usuário, como uma mensagem ou uma fotografia, quanto estruturas menos visíveis, como metadados, bases SQLite, registros de sistema e identificadores. A condição de evidência não decorre apenas da existência do dado: depende de sua pertinência à questão investigada, da forma como foi obtido e da possibilidade de demonstrar sua origem e seu significado. Por isso, a atividade pericial transforma dados brutos em informação examinável por meio de procedimentos controlados e explicáveis (ISO, 2012; Lyle et al., 2022).

Nos dispositivos móveis, a fonte de informação não se limita à memória interna. Cartões, módulos de identidade do assinante, dispositivos pareados, cópias de segurança e contas sincronizadas podem complementar ou contradizer o conteúdo local. O aparelho funciona como um ponto de convergência entre vestígios gerados pelo usuário, pelo sistema e por serviços de terceiros. Essa amplitude exige delimitação do objeto e da autoridade de acesso: reconhecer que uma credencial ou um token pode permitir alcançar dados remotos não significa que toda utilização técnica seja automaticamente adequada ao escopo da investigação (Almuqren et al., 2024; SWGDE, 2026).

A prova digital é replicável em nível lógico, mas essa possibilidade não elimina sua volatilidade. Uma cópia pode preservar os mesmos valores binários de um conjunto adquirido, enquanto o dispositivo de origem continua sujeito a processos automáticos, comunicações e alterações de estado. A preservação deve começar antes da cópia e considerar energia, conectividade, bloqueio de tela, condição do sistema e risco de apagamento remoto. O paradoxo é que desligar o aparelho pode preservar alguns dados, mas também tornar chaves inacessíveis; mantê-lo ligado pode conservar uma condição útil, porém aumenta a exposição a mudanças (Ayers et al., 2014; SWGDE, 2025).

Outra característica é a dependência de contexto. Um horário registrado pode estar em tempo universal, no fuso configurado pelo usuário ou em uma representação própria do aplicativo. A presença de um arquivo não demonstra, isoladamente, quem o criou ou conhecia seu conteúdo. Um registro de localização pode refletir GPS, rede, estimativa de serviço ou sincronização proveniente de outro equipamento. A interpretação forense precisa relacionar a estrutura do artefato, o funcionamento da aplicação e os demais vestígios disponíveis,

evitando atribuições categóricas baseadas em um único indicador (Lyle et al., 2022; SWGDE, 2026).

O valor investigativo dos smartphones decorre da continuidade de uso e da diversidade de atividades registradas. Chamadas, mensagens, fotografias, buscas, deslocamentos e interações com serviços podem ajudar a reconstruir eventos, identificar relacionamentos e testar versões apresentadas. Mesmo quando um dado não comprova diretamente um fato, sua combinação com fontes independentes pode fornecer coerência temporal ou apontar lacunas. O potencial informativo, contudo, não autoriza interpretar o aparelho como retrato integral da conduta de uma pessoa; ele contém registros selecionados por mecanismos técnicos e sujeitos a retenção, exclusão e sincronização (Kumar, 2021; SWGDE, 2026).

A relevância também decorre do caráter relacional desses dispositivos. Identificadores como IMEI, IMSI e ICCID podem ser comparados com registros de operadoras, enquanto contas e aplicativos relacionam o aparelho a serviços externos. A análise pode revelar novas fontes, mas exige distinguir o que foi produzido localmente do que foi importado ou sincronizado. A versão mais recente das boas práticas de análise móvel ressalta que artefatos encontrados em um telefone podem ter origem em outro dispositivo associado à mesma conta, circunstância que limita inferências automáticas sobre posse, autoria ou local de criação (SWGDE, 2026).

Integridade se refere à manutenção do conteúdo de modo que alterações relevantes possam ser detectadas e explicadas. Funções de hash são úteis para comparar conjuntos estáticos e demonstrar que a cópia analisada não mudou, mas não resolvem sozinhas todos os problemas. Aquisições repetidas de um telefone ativo podem produzir hashes distintos porque o sistema continua registrando eventos. Nesses casos, a divergência não torna a técnica inútil; ela deve ser interpretada à luz do comportamento do dispositivo, preservando-se hashes da extração e de arquivos individualizados quando aplicável (SWGDE, 2026).

Autenticidade envolve sustentar que o artefato é aquilo que se afirma e que sua ligação com a fonte foi adequadamente estabelecida. Essa demonstração combina identificadores do aparelho, documentação de coleta, estrutura interna do dado, metadados e, quando possível, confirmação por fontes independentes. Já a confiabilidade abrange a aptidão do método e da interpretação para produzir conclusões consistentes. Assim, um arquivo íntegro pode ser interpretado de forma incorreta, e um método tecnicamente válido pode ser mal aplicado. As três dimensões se complementam, mas não são sinônimas (ISO, 2015a, 2015b; Stoykova & Franke, 2023).

Um smartphone reúne processador, memória volátil, armazenamento não volátil, componentes de segurança, sensores e interfaces de comunicação. Sobre essa base funcionam carregadores de inicialização, sistema operacional, serviços e aplicativos, cada qual produzindo registros em locais e formatos diferentes. A arquitetura condiciona a aquisição: uma técnica que acessa dados por uma interface autorizada observa apenas o que aquela camada expõe; outra que obtém uma imagem de armazenamento ainda precisa lidar com criptografia, sistemas de arquivos e chaves. Conhecer a estrutura evita tratar “extração completa” como expressão absoluta e dissociada do modelo examinado (Almuqren et al., 2024; Fukami et al., 2021).

Componentes de segurança modificam essa arquitetura ao proteger segredos e executar operações sensíveis em ambientes isolados. Chaves podem ser vinculadas ao hardware e liberadas apenas após autenticação ou após determinada condição de inicialização. Consequentemente, remover fisicamente um chip de memória não garante acesso ao conteúdo legível. A evolução dos aparelhos deslocou o problema da simples leitura de armazenamento para a obtenção legítima de dados em estados nos quais as chaves necessárias estão disponíveis, mudança que explica a redução da efetividade de algumas técnicas tradicionais (Apple, 2024; Fukami et al., 2021; Google, 2026b).

Android e iOS compartilham funções gerais, mas adotam arquiteturas, políticas de atualização e modelos de segurança distintos. No Android, fabricantes podem combinar versões do sistema, interfaces próprias, diferentes chips e calendários de correção. Essa fragmentação amplia o número de combinações que uma ferramenta precisa suportar. O iOS possui integração mais centralizada entre hardware e software, porém incorpora mecanismos rigorosos de proteção e atualizações que também alteram os métodos disponíveis. Em ambos os ecossistemas, a identificação precisa do modelo, da versão e do estado do aparelho é condição para selecionar a abordagem (Almuqren et al., 2024; SWGDE, 2025).

No Android, a criptografia baseada em arquivo permite que chaves distintas protejam conjuntos de dados e oferece armazenamento acessível antes ou somente depois do desbloqueio do usuário. Dispositivos lançados com versões recentes devem implementar esse modelo, e a inicialização direta permite funções limitadas antes da autenticação. Para o examinador, a distinção entre dados protegidos por credenciais e dados disponíveis após a inicialização ajuda a explicar por que o mesmo aparelho pode expor volumes diferentes conforme o estado em que é recebido (Google, 2026a).

Os dados de interesse podem ser classificados por origem e função: conteúdo criado pelo usuário, informações geradas por aplicativos, registros do sistema e elementos de comunicação. Fotografias e documentos costumam ser perceptíveis, mas bases internas mantêm atributos, relações e estados não mostrados pela interface. Caches, miniaturas e registros de transação podem conservar indícios de conteúdo já removido da visualização normal. O valor desses vestígios depende do conhecimento do formato e do ciclo de vida do aplicativo, porque a mesma estrutura pode assumir significado diferente após uma atualização (Kumar, 2021; SWGDE, 2026).

O armazenamento móvel é dinâmico. Processos de limpeza, otimização e reutilização de espaço reduzem a expectativa de recuperação de itens apagados, especialmente quando a criptografia e comandos de descarte estão presentes. Uma aquisição física pode conter regiões não alocadas, mas não se deve presumir que elas tragam dados decifráveis ou completos. A ausência de um artefato também não prova sua inexistência anterior, pois políticas de retenção, sincronização e exclusão influenciam o que permanece. A conclusão pericial deve diferenciar “não localizado” de “não ocorreu” (Fukami et al., 2021; Lyle et al., 2022).

Aplicativos armazenam informações em formatos estruturados e proprietários, como SQLite, XML, JSON, listas de propriedades e buffers de protocolo. A ferramenta pode transformar esses registros em uma linha do tempo amigável, mas a apresentação é resultado de regras de decodificação. Quando a questão é relevante, o examinador precisa conferir a fonte subjacente, os campos utilizados e a versão do esquema. Essa verificação é especialmente importante diante de valores nulos, registros órfãos ou campos cujo significado não está documentado (Hargreaves et al., 2024; SWGDE, 2026).

Metadados e logs apoiam a contextualização, mas não devem ser lidos isoladamente. Uma fotografia pode conter horário e coordenadas, enquanto registros do sistema revelam importação, edição ou sincronização. Dados de localização podem vir de sensores, redes ou serviços e apresentar diferentes graus de precisão. A correlação entre fontes permite testar consistência e detectar discrepâncias; ainda assim, deve-se preservar a incerteza quando não é possível determinar se o evento representa a posição do aparelho, da conta ou de outro equipamento conectado (Lyle et al., 2022; SWGDE, 2026).

Figura 1 – Ciclo integrado de tratamento da evidência móvel



Fonte: elaboração própria, com base na síntese da literatura e das normas analisadas.

2.2 Métodos de extração

A extração lógica utiliza interfaces oferecidas pelo sistema, protocolos de sincronização, cópias de segurança ou APIs para solicitar objetos reconhecidos pelo aparelho. Em geral, apresenta menor risco físico e produz conteúdo já organizado, como contatos, mensagens e mídias. Sua principal limitação é a dependência das permissões e das funções expostas: dados apagados, áreas protegidas e estruturas internas podem não ser incluídos. Por isso, a denominação do método precisa ser acompanhada da descrição do que efetivamente foi obtido, e não de uma suposição sobre completude (Ayers et al., 2014; Kumar, 2021).

O método lógico pode ser adequado quando o objetivo está claramente delimitado e os dados necessários são acessíveis sem intervenção invasiva. Também pode servir como primeira etapa para preservar informações voláteis antes de procedimentos mais complexos. A vantagem operacional não dispensa validação. É necessário registrar o protocolo utilizado, as categorias solicitadas, mensagens de erro e eventuais restrições impostas pelo sistema. A comparação com a interface do aparelho ou com outra fonte pode confirmar se a ferramenta omitiu, duplicou ou interpretou incorretamente objetos relevantes (SWGDE, 2024, 2026).

A extração física busca reproduzir conteúdo de armazenamento em nível inferior ao sistema de arquivos, podendo incluir regiões não alocadas. Historicamente, ela foi associada a maior amplitude e possibilidade de recuperação de dados excluídos. Nos smartphones modernos, contudo, a leitura de blocos não equivale automaticamente à obtenção de informações legíveis. Criptografia vinculada ao hardware, chaves derivadas de credenciais e mecanismos de apagamento tornam inadequada a expectativa de que uma imagem bruta sempre será a melhor ou a mais completa aquisição (Fukami et al., 2021; Ayers et al., 2014).

Técnicas físicas variam quanto à invasividade. Interfaces de depuração e modos de inicialização podem permitir leitura controlada; JTAG e chip-off exigem conhecimento especializado e podem danificar o dispositivo. A decisão deve equilibrar necessidade, proporcionalidade, risco e possibilidade de repetição. Antes de uma técnica destrutiva ou de último recurso, convém documentar alternativas tentadas, testar o procedimento em exemplar compatível quando possível e preservar imagens detalhadas do estado físico. O resultado deve registrar tanto o conteúdo alcançado quanto as limitações decorrentes da intervenção (Ayers et al., 2014; SWGDE, 2025).

A extração por sistema de arquivos ocupa uma posição intermediária: procura recuperar a hierarquia de diretórios, arquivos e atributos com maior profundidade do que a aquisição lógica tradicional, sem necessariamente obter todos os blocos físicos. Seu valor está na preservação de estruturas internas utilizadas por aplicativos e pelo sistema, o que permite análise manual e verificação da decodificação automática. Dependendo do acesso disponível, a aquisição pode abranger apenas determinadas partições ou contêineres, razão pela qual o relatório deve indicar o alcance real do conjunto (SWGDE, 2026).

Esse tipo de extração favorece a rastreabilidade porque mantém caminhos, tamanhos, datas e relações entre arquivos. Entretanto, timestamps podem ser alterados durante exportação, e permissões ou links podem não ser representados integralmente no formato produzido. A validação deve verificar se o contêiner preserva os atributos necessários à pergunta pericial e se os arquivos extraídos correspondem ao conjunto original. Quando houver dúvida, a análise direta da base ou do arquivo fonte reduz a dependência da camada de apresentação da ferramenta (Hargreaves et al., 2024; ISO, 2015b).

A extração seletiva limita a aquisição a categorias, períodos, aplicativos ou objetos definidos. Pode ser necessária por restrições jurídicas, volume de dados, urgência ou finalidade do exame. Seu benefício é reduzir exposição desnecessária e acelerar a análise, mas o recorte precisa ser transparente. Filtros dependem de indexação e interpretação; se o mecanismo não reconhecer um formato ou usar um campo temporal inadequado, informações pertinentes podem ser excluídas sem que o usuário perceba (Hargreaves et al., 2024; SWGDE, 2026).

Para que a seleção seja defensável, devem ser preservados os critérios utilizados, a versão da ferramenta e o universo sobre o qual o filtro operou. Sempre que viável, mantém-se uma aquisição mais ampla sob custódia, enquanto se disponibiliza ao exame apenas o subconjunto autorizado. Quando isso não for possível, a limitação passa a integrar o resultado e precisa ser comunicada. A extração seletiva não deve ser confundida com uma busca perfeita: ela é uma decisão metodológica condicionada pelo modo como o dado foi indexado e pelo objetivo investigativo (ISO, 2015a; Lyle et al., 2022).

Técnicas avançadas incluem exploração de vulnerabilidades, uso de modos especiais de inicialização, obtenção de privilégios elevados e procedimentos sobre componentes. Elas surgem quando mecanismos de segurança impedem as interfaces usuais. Fukami et al. (2021) demonstram que a criptografia deslocou parte da aquisição moderna para métodos que contornam proteções ou exploram falhas. Essa realidade amplia o alcance, mas introduz dependência de combinações específicas de hardware e software, possibilidade de alteração e dificuldade de revelar detalhes protegidos por fabricantes ou fornecedores (Fukami et al., 2021; SWGDE, 2025).

O uso de uma vulnerabilidade não torna o resultado, por si só, inválido. A questão central é demonstrar o que a técnica fez, quais dados produziu e quais riscos foram controlados. Quando o método não pode ser integralmente divulgado, cresce a importância de testes com dispositivos de referência, verificação cruzada de artefatos e documentação das condições. Também é necessário distinguir o mecanismo de acesso da interpretação posterior: uma falha pode permitir copiar arquivos, mas não garante que a ferramenta os decodifique corretamente (Stoykova & Franke, 2023; SWGDE, 2024).

2.3 Desafios técnicos do exame forense móvel

A criptografia protege dados em repouso e tornou insuficiente a simples leitura do armazenamento. Em modelos atuais, chaves podem depender de segredos mantidos em hardware e da credencial do usuário. A proteção também pode variar conforme o estado do aparelho: antes do primeiro desbloqueio após a inicialização, apenas um conjunto limitado fica disponível; depois da autenticação, outras chaves podem permanecer acessíveis enquanto o sistema está ligado. O examinador precisa reconhecer esse estado e evitar ações automáticas, pois reiniciar o dispositivo pode eliminar uma oportunidade de aquisição que não será recuperada sem a credencial (Apple, 2024; Fukami et al., 2021; Google, 2026a).

Os bloqueios de acesso atuam em conjunto com atrasos, limites de tentativas e eventuais mecanismos de apagamento. Uma abordagem de força bruta pode ser impraticável ou produzir risco desproporcional. Mesmo quando uma ferramenta informa suporte ao modelo, o resultado depende da versão, do nível de correção e das condições específicas. A compatibilidade deve ser confirmada, não presumida. Antes de interagir, é necessário registrar a tela, o horário, o nível de bateria, a conectividade e outras características, além de planejar alimentação e isolamento de rede sem modificar desnecessariamente o estado (Ayers et al., 2014; SWGDE, 2025).

Biometria e senha não são equivalentes do ponto de vista técnico. Em geral, a biometria autoriza o uso de uma chave mantida pelo sistema, enquanto o código participa da proteção e volta a ser exigido em situações definidas, como reinicialização ou período de inatividade. O aparelho encontrado desbloqueado pode retornar rapidamente a uma condição mais restritiva. A atuação no local precisa observar autorização jurídica, protocolos institucionais e risco de perda de acesso, sem improvisar tentativas que ativem bloqueios adicionais (Apple, 2024; SWGDE, 2025).

A autenticação multifator amplia a dependência de elementos externos. Um aplicativo pode exigir senha, token, confirmação em outro dispositivo ou validação por servidor. Mesmo com acesso ao telefone, o conteúdo remoto pode permanecer protegido; inversamente, tokens presentes no aparelho podem abrir serviços que não integram automaticamente o escopo autorizado. A perícia deve separar capacidade técnica de permissão, registrar a origem dos dados e evitar que uma sessão ativa seja tratada como autorização irrestrita para navegar em contas remotas (ISO, 2012; SWGDE, 2026).

Atualizações corrigem vulnerabilidades, alteram formatos e reforçam controles. Uma ferramenta pode reconhecer o modelo, mas interpretar inadequadamente um banco modificado em versão recente. A rapidez do ciclo de software dificulta que documentação, treinamento e testes acompanhem todas as combinações. Por isso, o número de versão e o nível de correção são dados periciais, não detalhes administrativos. Eles devem aparecer nas notas do caso e orientar a escolha da ferramenta e do conjunto de testes aplicável (Almuqren et al., 2024; SWGDE, 2024).

O risco não se limita à aquisição. Mudanças no esquema de um aplicativo podem deslocar campos, modificar épocas temporais ou substituir formatos. Uma interface pode continuar exibindo resultados plausíveis embora a regra de análise esteja desatualizada. Nesses casos, plausibilidade não equivale a correção. Conferência manual, documentação do desenvolvedor, conjuntos de teste conhecidos e comparação entre ferramentas ajudam a detectar erros silenciosos. Se não houver base suficiente para interpretar um campo, a incerteza deve ser preservada no relatório (Hargreaves et al., 2024; Lyle et al., 2022).

Ferramentas forenses combinam aquisição, processamento, indexação e apresentação. Um erro inicial pode propagar-se pelas etapas e chegar ao relatório com aparência de precisão. Hargreaves et al. (2024) observam que a arquitetura monolítica dificulta localizar a origem do erro quando resultados intermediários não são expostos. Isso reforça a necessidade de acessar artefatos subjacentes, preservar logs e distinguir aquilo que foi copiado daquilo que foi inferido pelo software (Hargreaves et al., 2024; Lyle et al., 2022).

O suporte declarado por um fornecedor deve ser compreendido de modo específico. Pode significar apenas aquisição de determinadas categorias, não decodificação integral de todos os aplicativos. Recursos podem variar entre licenças e versões, e atualizações podem corrigir um problema enquanto introduzem outro. A organização precisa validar ferramentas antes do uso e reavaliá-las após mudanças relevantes. Ferramentas críticas, capazes de interagir com a fonte original ou contaminar dados, exigem atenção especial e procedimentos de teste proporcionais ao risco (SWGDE, 2024).

Perda e alteração podem ocorrer antes, durante ou depois da aquisição. Bateria esgotada, conexão de rede, comando remoto, atualização automática e manuseio não registrado são exemplos de riscos. O isolamento não possui solução universal: modo avião depende de interação; recipientes de bloqueio podem falhar em determinadas frequências; desligar muda o estado de chaves. A decisão precisa considerar o caso concreto e ser registrada com horário, justificativa e efeito observado (Ayers et al., 2014; SWGDE, 2025).

Contaminação digital pode ser compreendida como transferência inadvertida de características para um objeto relevante em qualquer etapa do processo forense. O conceito inclui, por exemplo, criação de arquivos, alteração de metadados, inclusão de uma conta ou instalação de componente não necessário. Nem toda mudança é evitável, sobretudo em aquisição ao vivo, mas ela deve ser minimizada e diferenciada do conteúdo anterior. A documentação permite avaliar se a intervenção afetou justamente o artefato utilizado na conclusão (Gruber et al., 2023).

O dispositivo móvel funciona como ponto de acesso a um ecossistema distribuído. Parte do conteúdo apresentado na tela pode estar armazenada localmente; outra parte pode ser recuperada sob demanda de serviço remoto; e uma terceira pode existir em cache com temporalidade distinta. Essa mistura afeta a definição da fonte. Antes de atribuir um item ao aparelho, o examinador precisa identificar se ele foi encontrado na aquisição local, sincronizado durante o procedimento ou obtido por requisição à conta. A documentação deve separar esses caminhos e preservar horários, mecanismo e autoridade, pois cada um possui cadeia de custódia própria (SWGDE, 2025, 2026; ISO, 2012).

Tokens e credenciais encontrados no aparelho podem permitir continuidade técnica, mas sua utilização exige planejamento específico. A existência de acesso não resolve a autorização nem garante que a coleta remota reproduza o estado existente no momento da apreensão. Serviços podem atualizar registros, aplicar filtros e apresentar dados transformados. Quando o acesso for autorizado, deve-se registrar endpoint, conta, intervalo, método de autenticação, respostas e eventuais paginações, além de verificar integridade do conjunto produzido. O conteúdo remoto deve permanecer distinguível dos dados preservados na memória do dispositivo (ISO, 2012, 2015b; SWGDE, 2026).

2.4 Cadeia de custódia, preservação e validação

A cadeia de custódia registra a história do vestígio desde o reconhecimento até sua destinação, identificando responsáveis, transferências, condições e intervenções. No ambiente digital, ela sustenta a ligação entre o aparelho apreendido, a aquisição realizada e o material analisado. Seu valor não é meramente burocrático: permite reconstruir o percurso, avaliar riscos e contestar ou confirmar a identidade do objeto. Uma lacuna documental não prova alteração, mas reduz a capacidade de demonstrar que o conjunto apresentado corresponde ao que foi coletado (ISO, 2012; SWGDE, 2025).

No Brasil, o Código de Processo Penal disciplina a cadeia de custódia nos artigos 158-A a 158-F e descreve etapas como reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte. Embora formulada para vestígios em sentido amplo, essa sequência oferece referência para evidências digitais. Sua aplicação deve respeitar particularidades técnicas, como necessidade de energia, preservação do estado lógico, uso de identificadores e produção de cópias de trabalho (Brasil, 1941; ISO, 2012).

A identificação começa pela observação do ambiente e do estado do aparelho. Fotografias, posição, cabos, tela, notificações visíveis e equipamentos associados podem influenciar a estratégia. O registro deve evitar exploração indevida do conteúdo e concentrar-se nas condições necessárias à preservação. Modelo, número de série, IMEI e demais identificadores são coletados por meios que não provoquem mudanças desnecessárias. Se o dispositivo estiver ligado, a decisão sobre conectividade e energia deve ser tomada por pessoa capacitada (Ayers et al., 2014; SWGDE, 2025).

Na coleta, acondicionamento e transporte, o objetivo é proteger o aparelho de dano físico e comunicação não autorizada, mantendo a rastreabilidade. Embalagens, lacres e etiquetas precisam ser individualizados, enquanto acessórios potencialmente úteis devem ser preservados sem mistura. Para um aparelho ligado, pode ser necessário manter alimentação; para um danificado, a movimentação pode agravar a condição. Não existe uma receita única, mas qualquer desvio do procedimento habitual precisa ser justificado pelas circunstâncias observadas (ISO, 2012; SWGDE, 2025).

Uma documentação útil permite que outro profissional compreenda o que ocorreu sem depender da memória do examinador. Deve incluir datas e horários, responsáveis, identificação de equipamentos, versões de hardware e software, comandos ou opções relevantes, resultados, erros e decisões. Capturas de tela podem complementar, mas não substituem notas estruturadas. Quanto mais automatizado o processo, maior a necessidade de preservar logs, pois a interface final tende a ocultar etapas internas e mensagens que explicam uma limitação (Hargreaves et al., 2024; ISO, 2015a).

Também devem ser registrados os fatos negativos: tentativa sem sucesso, categoria não suportada, arquivo corrompido, senha não disponível ou diferença entre ferramentas. Omitir esses elementos cria impressão artificial de linearidade. Relatar limitações não enfraquece automaticamente o exame; ao contrário, delimita o alcance da conclusão e permite avaliação técnica. A transparência torna possível diferenciar um dado inexistente de um dado que o método não conseguiu recuperar ou interpretar (Lyle et al., 2022; Stoykova & Franke, 2023).

Rastreabilidade significa poder relacionar cada resultado à fonte e às transformações que sofreu. Uma mensagem apresentada em relatório deve ser vinculada ao registro ou banco de dados do qual foi decodificada, à extração que o contém e ao aparelho correspondente. Essa trilha reduz ambiguidades e permite revisão seletiva. Quando o software não oferece ligação suficiente, o examinador deve complementar o relatório com caminhos,

identificadores, consultas ou capturas que possibilitem localizar o artefato (ISO, 2015b; SWGDE, 2026).

A integridade é fortalecida por controles combinados: hashes, proteção de cópias mestres, registros de acesso, cópias de trabalho e documentação de conversões. Em aparelhos ativos, a mutabilidade pode impedir igualdade entre aquisições realizadas em momentos distintos. O controle passa então a demonstrar o que foi preservado em cada momento e por que as diferenças eram esperadas. A cadeia de custódia não promete imobilidade absoluta do sistema; oferece evidências para avaliar mudanças e sua relevância para o conteúdo examinado (Ayers et al., 2014; SWGDE, 2026).

Validar significa demonstrar, por evidências objetivas, que um método atende aos requisitos de seu uso pretendido. O teste deve formular uma pergunta específica: por exemplo, se a ferramenta recupera determinado tipo de mensagem de uma versão definida e preserva os campos necessários. Declarações genéricas de que um produto é “validado” têm pouco valor, porque o desempenho varia com versão, configuração e artefato. A validação precisa ser proporcional à importância do resultado e atualizada quando mudanças possam afetá-lo (ISO, 2015a; SWGDE, 2024).

Conjuntos de teste conhecidos permitem comparar entradas e saídas, calcular omissões e identificar transformações. Devem abranger situações normais e limites, como campos vazios, caracteres especiais, exclusões e diferentes fusos. O teste do fornecedor pode contribuir, mas não substitui a responsabilidade do laboratório de compreender o uso local. Resultados publicados pelo programa CFTT do NIST oferecem referência independente para classes de ferramentas, devendo ser conferida a correspondência entre a configuração testada e aquela utilizada no caso (National Institute of Standards and Technology, n.d.; SWGDE, 2024).

A ISO/IEC 27037:2012 orienta identificação, coleta, aquisição e preservação de evidência digital e inclui expressamente telefones móveis. Seu foco é o tratamento inicial e a manutenção da aptidão probatória. A ISO/IEC 27041:2015 aborda a adequação dos métodos de investigação e o uso da validação para demonstrar que requisitos foram atendidos. Lidas em conjunto, as normas conectam preservação da fonte à justificativa do método, evitando que cadeia de custódia e validação sejam tratadas como controles separados (ISO, 2012, 2015a).

A ISO/IEC 27042:2015 dirige-se à análise e interpretação, com ênfase em continuidade, validade, reprodutibilidade e repetibilidade. A ISO/IEC 27043:2015 organiza princípios e processos de investigação de incidentes, enquanto a ISO/IEC 17025:2017 fornece requisitos gerais para competência e operação consistente de laboratórios de ensaio. Esses documentos não substituem procedimentos locais nem prescrevem uma ferramenta; oferecem critérios para estruturar competência, registros, verificação e comunicação de resultados (ISO, 2015b, 2015c, 2017).

Repetibilidade refere-se à obtenção de resultados consistentes sob condições semelhantes pelo mesmo ambiente; reprodutibilidade amplia a comparação para outros profissionais ou condições. Em dispositivos móveis ativos, igualdade binária pode ser impossível porque o sistema muda. O objetivo deve ser definido no nível apropriado: os mesmos artefatos relevantes, a mesma interpretação de campos ou a confirmação independente de uma relação, e não necessariamente um hash global idêntico entre aquisições sucessivas (ISO, 2015b; SWGDE, 2026).

Para favorecer reprodução, é preciso registrar versões, configurações, filtros, fuso horário, credenciais utilizadas e etapas manuais. Quando um procedimento depende de exploração proprietária, a reprodução completa pode não estar disponível; nesse caso, verificações sobre os dados extraídos ganham importância. Preservar arquivos fonte, consultas e valores originais possibilita que outra pessoa teste a interpretação mesmo sem repetir o acesso inicial. O relatório deve distinguir partes reproduzíveis, partes apenas verificáveis e partes cuja confirmação ficou limitada (Stoykova & Franke, 2023; SWGDE, 2024).

As boas práticas começam pelo planejamento: esclarecer a pergunta, a autoridade, o estado do aparelho e os riscos antes de conectar uma ferramenta. A aquisição deve seguir progressão justificada, preservar o máximo possível e produzir registros contemporâneos. O exame ocorre sobre cópia de trabalho, mantendo-se o conjunto mestre protegido. Artefatos decisivos recebem confirmação manual ou independente, e qualquer diferença é investigada em vez de ocultada (ISO, 2012; SWGDE, 2025, 2026).

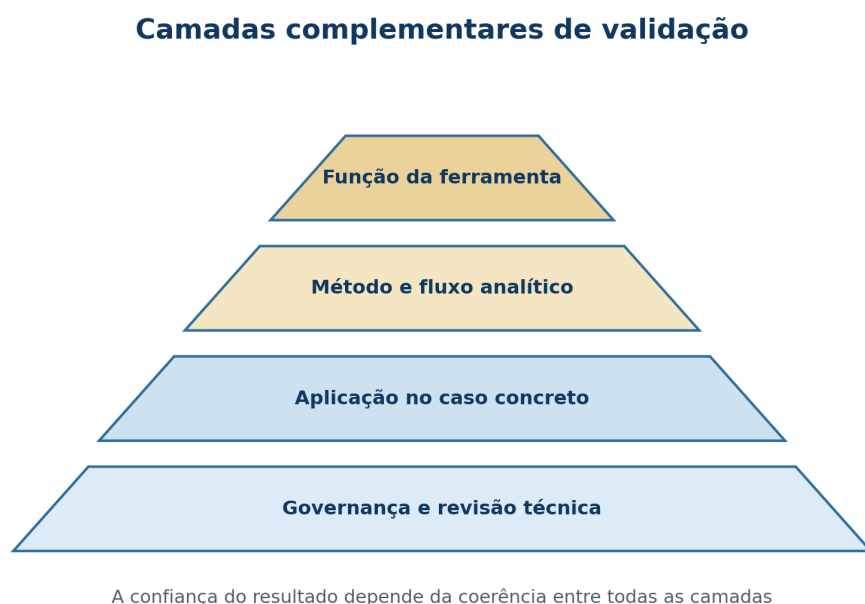
Outra prática é manter competência e ambiente controlado. Treinamento precisa incluir funcionamento dos sistemas, não apenas operação de interfaces. Versões de ferramentas, módulos, dependências e relógios devem ser administrados; mudanças relevantes exigem verificação. Procedimentos operacionais devem admitir exceções justificadas, porque a diversidade móvel impede roteiros totalmente rígidos. Revisão por pares é especialmente

útil quando o método é novo, o artefato é central ou a conclusão depende de interpretação complexa (ISO, 2017; Lyle et al., 2022; SWGDE, 2024).

A gestão da qualidade transforma boas práticas individuais em capacidade institucional. Procedimentos controlados, registros, equipamentos identificados, tratamento de desvios e revisão permitem que exames diferentes mantenham requisitos comparáveis. Em um campo mutável, o sistema não deve congelar técnicas, mas definir como uma mudança é avaliada e autorizada. Versões novas precisam passar por análise de impacto; funções críticas, por testes; e resultados inesperados, por registro de não conformidade. Esse ciclo reduz a dependência de conhecimento informal e conserva evidência das decisões de qualidade (ISO, 2017; INTERPOL, 2019).

Competência deve ser demonstrada para a atividade concreta. Conhecimento geral de informática não comprova capacidade para interpretar bancos móveis, estados criptográficos ou logs específicos. Um programa pode combinar formação, exercícios com dados conhecidos, observação supervisionada, avaliação e experiência documentada. O escopo autorizado de cada examinador deve acompanhar a complexidade da tarefa e ser revisto quando tecnologias mudarem. Essa abordagem protege tanto o resultado quanto o profissional, porque permite encaminhar situações fora de sua competência sem transformar a limitação em falha individual (ISO, 2017; SWGDE, 2024).

Figura 2 – Camadas complementares de validação do exame móvel



Fonte: elaboração própria, com base em ISO/IEC 27041, ISO/IEC 27042, NISTIR 8354 e SWGDE.

3 Metodologia

3.1 Abordagem e delineamento da pesquisa

A pesquisa possui abordagem qualitativa, caráter exploratório e descritivo e delineamento bibliográfico e documental. A abordagem qualitativa é adequada porque o objetivo não é medir frequência ou testar associação estatística, mas compreender como a literatura científica e as normas caracterizam problemas técnicos e medidas de controle. O caráter exploratório permite organizar um campo sujeito a mudança rápida; o descritivo orienta a exposição dos métodos, limites e critérios encontrados. A pesquisa bibliográfica oferece discussão acadêmica, enquanto a documental acrescenta normas, guias técnicos e documentação oficial das plataformas (Gil, 2022).

O estudo não adota etnografia, fenomenologia, pesquisa-ação ou estudo de caso, pois não investiga experiências de participantes nem uma unidade empírica delimitada. Trata-se de revisão qualitativa orientada por problema, estruturada segundo os objetivos aprovados no D1. A unidade de análise é o conteúdo técnico e normativo referente a extração, preservação, validação e confiabilidade em smartphones. Essa definição evita apresentar a revisão como teste de desempenho ou avaliação laboratorial, resultados que exigiriam dados e procedimentos diferentes (Gil, 2022; Lyle et al., 2022).

O delineamento qualitativo foi adequado porque o problema exige compreender relações entre técnicas, riscos e critérios de confiabilidade, e não estimar frequência populacional. A dimensão exploratória permitiu organizar um campo sujeito a rápida transformação, enquanto a dimensão descritiva orientou a apresentação das características de métodos e controles. A revisão não foi tratada como enumeração de textos: adotou-se leitura comparativa, com registro de convergências, divergências, pressupostos e limites de aplicação. Esse procedimento favoreceu a construção de categorias analíticas vinculadas aos objetivos específicos (Gil, 2022; Al-Dhaqm et al., 2020).

A opção documental também preservou coerência ética com o projeto aprovado, pois não envolveu pessoas, dados pessoais de casos, entrevistas, questionários ou experimentos em aparelhos. Foram examinados apenas materiais publicamente disponíveis e referências normativas. Consequentemente, os resultados descrevem o estado do conhecimento e propõem um modelo conceitual; não medem desempenho de produto nem afirmam eficácia operacional em todas as combinações. Essa delimitação é essencial para interpretar corretamente o alcance das conclusões (Gil, 2022; Lyle et al., 2022).

3.2 Constituição do corpus e estratégia de busca

O corpus reúne artigos científicos revisados por pares, normas internacionais, publicações de organismos técnicos, documentação oficial de Android e iOS e legislação brasileira sobre cadeia de custódia. Foram priorizados materiais publicados entre 2021 e julho de 2026 para representar o estado recente do campo. Obras anteriores foram mantidas quando constituem referência normativa vigente ou fundamento técnico ainda utilizado, como a ISO/IEC 27037:2012 e o NIST SP 800-101 Rev. 1. O ano antigo, nesses casos, não significa abandono: a pertinência foi avaliada pela vigência e pela função conceitual da fonte (ISO, 2012; Ayers et al., 2014).

Foram incluídos documentos que tratassem diretamente de pelo menos uma das seguintes dimensões: arquitetura de segurança móvel; métodos de aquisição; preservação e cadeia de custódia; teste de ferramentas; interpretação de artefatos; repetibilidade, reprodutibilidade ou confiabilidade. Excluíram-se textos sem autoria ou procedência identificável, páginas promocionais, publicações centradas em dispositivos que não fossem móveis sem contribuição transferível ao problema e materiais que apenas enumerassem ferramentas sem discutir método ou limitação. A seleção por pertinência é compatível com uma revisão bibliográfica qualitativa de finalidade exploratória (Gil, 2022).

O corpus final reúne 27 fontes mobilizadas diretamente na análise. Foram incluídos estudos acadêmicos sobre processos, criptografia, contaminação, confiabilidade, ferramentas e aplicações; normas ISO; orientações do NIST, INTERPOL e SWGDE; documentação oficial de Android e Apple; e legislação brasileira. A inclusão das fontes institucionais não ocorreu como simples argumento de autoridade, mas para obter definições de processo, requisitos de teste e descrições técnicas que os artigos nem sempre reproduzem integralmente (ISO, 2012; INTERPOL, 2019; Lyle et al., 2022).

Documentos anteriores a 2021 foram mantidos quando possuíam função normativa ou fundacional ainda pertinente. Para temas sujeitos a mudança rápida, como mecanismos de plataforma e práticas móveis, priorizaram-se versões atuais disponíveis até setembro de 2026. Essa combinação evitou dois extremos: excluir fundamentos vigentes apenas pela idade e tratar textos antigos como descrição suficiente de tecnologias atuais. A data foi avaliada junto com vigência, finalidade, autoridade e correspondência com o problema (Ayers et al., 2014; Google, 2026a; SWGDE, 2026).

As buscas foram orientadas por combinações em português e inglês, incluindo “mobile device forensics”, “smartphone forensic acquisition”, “encrypted mobile devices”, “digital evidence preservation”, “forensic tool validation”, “digital chain of custody”, “Android file-based encryption” e “iOS Data Protection”. Foram consultados portais de periódicos, mecanismos de busca acadêmica e sítios oficiais do NIST, ISO, SWGDE, Apple, Android Open Source Project e Presidência da República. As referências dos estudos centrais também foram examinadas para localizar documentos normativos e trabalhos relacionados (Gil, 2022; Lyle et al., 2022).

A seleção ocorreu em três movimentos. Primeiro, títulos e resumos foram verificados quanto à relação com a pergunta de pesquisa. Em seguida, o texto integral ou a descrição oficial foi lido para confirmar autoria, ano, escopo e contribuição. Por fim, os materiais foram confrontados entre si, privilegiando fonte primária para características técnicas e fonte oficial para normas e legislação. Duplicatas e referências cuja existência ou dados bibliográficos não puderam ser confirmados foram retiradas, inclusive referências preliminares que constavam na versão D1 (Gil, 2022).

O recorte temporal não foi aplicado mecanicamente. Normas vigentes e documentos fundacionais permaneceram no corpus, enquanto publicações recentes foram escolhidas para criptografia, ferramentas e plataformas. Essa combinação reduz dois riscos: usar material antigo para descrever tecnologia modificada ou descartar uma norma apenas por sua data de edição. A data de confirmação de uma norma não foi tratada como nova edição; as referências registram o ano efetivo de publicação, preservando precisão bibliográfica (ISO, 2012, 2015a, 2015b, 2015c, 2017).

As buscas combinaram termos em português e inglês relacionados a mobile forensics, digital evidence, extraction, encryption, chain of custody, validation, reliability e tool testing. A seleção exigiu relação direta com ao menos uma categoria, autoria identificável, publicação acessível e contribuição técnica ou metodológica. Foram excluídos materiais promocionais sem explicação, conteúdos duplicados, referências cuja existência ou dados editoriais não puderam ser confirmados e trabalhos que dependiam de coleta com participantes. A conferência de DOI, página institucional ou catálogo normativo reduziu o risco de referências imprecisas (Gil, 2022; Lyle et al., 2022).

Após a triagem, cada fonte foi lida segundo sua finalidade. Estudos foram examinados quanto a problema, método e limites; normas, quanto a requisitos; documentos de plataforma, quanto a mecanismos; e guias, quanto a práticas. Essa leitura funcional impediu que recomendações institucionais fossem apresentadas como evidência experimental ou que uma descrição do fabricante fosse tomada como validação independente. O cruzamento entre tipos documentais serviu como forma de triangulação conceitual (ISO, 2015a, 2015b; Stoykova & Franke, 2023).

3.3 Categorias de análise, aspectos éticos e limitações

Após a seleção, as fontes foram submetidas a leitura exploratória e analítica. Informações relevantes foram registradas em fichas contendo identificação, tipo de documento, objeto, método, achados, limitações e contribuição para os objetivos. O conteúdo foi agrupado em quatro categorias principais: métodos de extração; desafios técnicos; preservação e cadeia de custódia; validação e confiabilidade. Subcategorias emergiram do índice aprovado, como criptografia, estado do aparelho, atualizações, contaminação, documentação, teste de ferramentas e reprodutibilidade (Gil, 2022).

A interpretação buscou convergências e diferenças entre estudos, normas e orientações técnicas. Recomendações repetidas por fontes independentes receberam maior peso analítico, enquanto afirmações dependentes de uma plataforma foram mantidas em seu contexto. Não foi realizada contagem bibliométrica nem cálculo de efeito. O resultado é uma síntese argumentativa: cada conclusão deve ser rastreável às fontes citadas, e as incertezas são apresentadas quando os documentos não permitem generalização. Esse procedimento é coerente com a finalidade de compreender e sistematizar, e não de produzir estimativas populacionais (Gil, 2022; Lyle et al., 2022).

Para reduzir erro de interpretação, as informações técnicas sobre mecanismos das plataformas foram conferidas em documentação oficial, e os critérios de qualidade foram confrontados com ISO, NIST e SWGDE. Trabalhos científicos foram utilizados para problematizar limitações, contaminação, automação, confiabilidade e prática profissional. Essa triangulação documental não torna as fontes equivalentes: cada uma foi utilizada segundo sua função, distinguindo descrição de produto, orientação normativa, evidência empírica e proposta teórica (Gruber et al., 2023; Hargreaves et al., 2024; Stoykova & Franke, 2023).

A codificação foi orientada por quatro categorias principais: métodos de extração; desafios técnicos; preservação e cadeia de custódia; validação e confiabilidade. Para cada trecho pertinente, registraram-se o problema descrito, a consequência para o exame, o controle proposto e a condição de aplicação. Em seguida, os registros foram agrupados por convergência e contrastados com fontes de natureza diferente. Essa matriz permitiu passar da descrição isolada à relação entre risco e resposta metodológica (Al-Dhaqm et al., 2020; ISO, 2015c).

Na etapa interpretativa, adotou-se uma cadeia de raciocínio explícita: fonte, achado documental, síntese comparativa e implicação. Recomendações finais somente foram formuladas quando havia convergência ou compatibilidade entre a literatura científica e referências técnicas. Divergências foram mantidas quando dependiam do contexto, como a decisão de desligar ou manter ligado. O resultado é um modelo condicionado, e não uma sequência automática, coerente com a variabilidade dos dispositivos móveis (Fukami et al., 2021; SWGDE, 2025, 2026).

Figura 5. Percurso de constituição e análise do corpus documental.

Fonte: elaboração própria (2026).

O estudo não envolve seres humanos, dados pessoais de casos reais, entrevistas, questionários, grupos focais ou intervenção em dispositivos. Todo o material analisado é bibliográfico ou documental de acesso acadêmico e institucional. Por essa razão, não se prevê submissão à Plataforma Brasil, sem prejuízo da observância de integridade acadêmica, atribuição de autoria e uso responsável das fontes. As citações e referências seguem APA, e não são reproduzidos conteúdos sigilosos, técnicas operacionais restritas ou dados individualizados (Gil, 2022).

As limitações decorrem do próprio recorte. Não foram testadas ferramentas, aparelhos ou versões, de modo que as recomendações não equivalem a validação operacional. Parte das tecnologias de aquisição é proprietária e possui documentação pública limitada. Além disso, atualizações podem alterar rapidamente a aplicabilidade de uma técnica. O trabalho procura controlar essas limitações indicando datas e versões das fontes, evitando avaliar produtos específicos e formulando recomendações em nível de processo, que ainda precisam ser adaptadas e testadas em ambiente laboratorial (Lyle et al., 2022; SWGDE, 2024).

Outra limitação é a heterogeneidade terminológica. Expressões como extração física, sistema de arquivos e aquisição avançada podem receber significados diferentes entre fornecedores e autores. A pesquisa adota definições funcionais e alerta para a necessidade de descrever o conteúdo obtido, em vez de depender apenas do rótulo comercial. Essa cautela reduz generalizações, mas aumenta a precisão do estudo e mantém a resposta à pergunta vinculada às evidências disponíveis (Fukami et al., 2021; SWGDE, 2026).

Embora não haja participantes, a pesquisa observa responsabilidade na comunicação. Não foram reproduzidos dados pessoais de casos, instruções operacionais destinadas a contornar segurança nem alegações sobre ferramentas sem base verificável. Marcas e plataformas são citadas apenas quando necessárias à descrição técnica. A discussão privilegia requisitos de processo e não classifica produtos comerciais. Essa postura reduz riscos de uso indevido e preserva a finalidade acadêmica da análise (Gil, 2022; Sunde, 2022).

As limitações incluem dependência de documentação pública, rápida mudança tecnológica e heterogeneidade terminológica. O corpus não é uma revisão sistemática exaustiva de todas as ferramentas, e algumas técnicas proprietárias não podem ser avaliadas internamente. Não houve mensuração de taxa de erro nem comparação laboratorial. Para controlar esses limites, as conclusões foram redigidas em nível de princípios e decisões, com indicação de que toda aplicação concreta requer teste local, competência e autorização adequada (Lyle et al., 2022; SWGDE, 2024).

4 Resultados e discussão

4.1 Caracterização do corpus documental

A análise foi realizada sobre 27 fontes efetivamente mobilizadas no trabalho. O conjunto é composto por dez publicações acadêmicas, treze documentos normativos ou técnico-institucionais, três documentos oficiais das plataformas Android e iOS e um diploma legal brasileiro. Essa composição corresponde ao delineamento definido na metodologia: os estudos científicos sustentam a problematização e a avaliação crítica; as normas e guias fornecem critérios de processo e qualidade; a documentação das plataformas esclarece mecanismos de segurança; e a legislação situa a cadeia de custódia no contexto jurídico nacional (Gil, 2022; ISO, 2012; Lyle et al., 2022).

O recorte temporal conferiu maior presença a fontes publicadas entre 2021 e julho de 2026, sem excluir documentos anteriores que permanecem vigentes ou conservam função estruturante. A ISO/IEC 27037:2012 e o NIST SP 800-101 Rev. 1, por exemplo, foram mantidos por tratarem de princípios e procedimentos ainda empregados, enquanto publicações recentes foram priorizadas para criptografia, contaminação, confiabilidade e práticas de análise. Esse tratamento evitou confundir atualidade tecnológica com simples data de publicação e permitiu combinar fundamentos estáveis com problemas emergentes (Ayers et al., 2014; Gruber et al., 2023; Almuqren et al., 2024).

A leitura comparativa revelou elevada convergência em torno de cinco exigências: conhecimento do estado do dispositivo, preservação das condições encontradas, escolha justificada do método, documentação de todas as intervenções e verificação do resultado por controles independentes. As divergências aparecem sobretudo na terminologia usada para classificar aquisições e no alcance prometido por cada técnica. Por esse motivo, os resultados foram organizados segundo a função desempenhada pelo procedimento e o conteúdo efetivamente obtido, e não apenas pelo nome comercial ou pela categoria atribuída por uma ferramenta (Fukami et al., 2021; Hargreaves et al., 2024; SWGDE, 2026).

Nota. Classificação elaborada a partir do corpus descrito na metodologia (Gil, 2022; Lyle et al., 2022).

A ampliação para 27 fontes fortaleceu três pontos que exigiam melhor sustentação na versão anterior: organização laboratorial, teste federado e análise de aplicativos criptografados. As diretrizes do INTERPOL complementaram as normas de qualidade com recomendações de laboratório; a página atual do NIST documentou a continuidade dos ensaios federados; e o estudo de Prabowo et al. ofereceu exemplo recente de como versão, chave e ferramenta afetam a análise de banco de mensagens. Essas inclusões não alteraram as categorias, mas aumentaram a densidade da triangulação (INTERPOL, 2019; National Institute of Standards and Technology, 2026; Prabowo et al., 2025).

Tabela 1 – Composição do corpus documental por natureza da fonte

Natureza da fonte	Quantidade	Função predominante na análise
Publicações acadêmicas	10	Artigos científicos e obra metodológica utilizados na análise crítica.
Normas e documentos técnico-institucionais	13	Normas ISO, publicações NIST, INTERPOL e orientações SWGDE.
Documentação oficial de plataformas	3	Descrição de criptografia, proteção de chaves e estados de acesso.
Legislação brasileira	1	Enquadramento jurídico da cadeia de custódia.
Total	27	Base documental integrada da pesquisa.

Fonte: elaboração própria a partir do corpus da pesquisa.

4.2 Métodos de extração e adequação ao caso concreto

A primeira constatação é que os métodos de extração formam um conjunto complementar, e não uma escala automática em que a técnica mais profunda seja sempre a melhor. Aquisições lógicas ou seletivas tendem a produzir conjuntos mais delimitados e menor intervenção, mas podem depender das interfaces disponibilizadas pelo sistema e omitir dados protegidos ou eliminados. Aquisições de sistema de arquivos ampliam a estrutura acessível e favorecem a análise de bancos, preferências e registros internos, embora permaneçam condicionadas às permissões e às chaves disponíveis (Ayers et al., 2014; Kumar, 2021; SWGDE, 2026).

A extração física, compreendida como obtenção de uma representação de áreas de armazenamento, pode oferecer maior abrangência em determinados aparelhos, porém não significa acesso imediato a conteúdo inteligível. Blocos adquiridos podem permanecer cifrados, fragmentados ou vinculados a chaves protegidas por hardware. O achado corrige uma associação comum entre profundidade e completude: quanto mais baixo o nível de aquisição, maior pode ser a quantidade de dados brutos, mas o valor forense continua dependente da possibilidade de decodificar, contextualizar e verificar esses dados (Fukami et al., 2021; Google, 2026b; Lyle et al., 2022).

As técnicas avançadas foram identificadas como recursos condicionais, adequados quando abordagens convencionais não respondem ao objetivo e quando o benefício esperado justifica riscos técnicos superiores. Sua aplicação pode exigir exploração de vulnerabilidades, interfaces de diagnóstico ou intervenção sobre componentes, criando possibilidade de alteração, dano ou menor repetibilidade. A literatura não sustenta seu uso rotineiro por mera

expectativa de obter mais informação; sustenta uma decisão proporcional, precedida de registro do estado e acompanhada de justificativa técnica (ISO, 2012, 2015a; SWGDE, 2025).

A estratégia mais consistente encontrada é incremental. O examinador delimita a pergunta, registra o estado, preserva oportunidades de acesso e inicia pelo método menos intrusivo capaz de responder ao objetivo. Se o resultado for insuficiente, avança de forma controlada, mantendo os conjuntos anteriores e registrando o que cada nova etapa modifica. Essa abordagem conserva alternativas, reduz intervenções desnecessárias e permite demonstrar por que a escalada foi tecnicamente razoável (ISO, 2015a; Stoykova & Franke, 2023; SWGDE, 2026).

A comparação mostrou que abrangência, intervenção e interpretabilidade formam dimensões distintas. Uma aquisição mais profunda pode ampliar o universo potencial, mas elevar risco e produzir conteúdo cifrado. Uma extração lógica pode ser menos abrangente e ainda responder de forma mais direta à pergunta, com metadados suficientes. Consequentemente, a hierarquia fixa entre métodos foi rejeitada. A seleção deve ser multidimensional, considerando finalidade, estado, suporte, reversibilidade, validabilidade e possibilidade de preservar etapas anteriores (Fukami et al., 2021; SWGDE, 2026).

Também se observou que o nome do método varia entre autores e fornecedores. “Física”, “avançada” e “sistema de arquivos” podem designar contêineres e alcances diferentes. O critério comparável é o resultado documentado: estruturas obtidas, estado criptográfico, conteúdo legível, metadados, erros e exclusões. Essa descrição funcional melhora o contraditório e impede que o rótulo seja utilizado como atalho para completude. O Quadro comparativo do trabalho foi construído com esse princípio (Hargreaves et al., 2024; Lyle et al., 2022).

A sequência de métodos emergiu como variável de qualidade. Adquirir primeiro categorias acessíveis pode preservar informações antes de técnica mais arriscada; contudo, operações iniciais podem alterar a fonte ou consumir tempo crítico. O planejamento deve identificar ações irreversíveis, ponto de parada e conjunto mínimo. Nenhuma sequência é universal, mas a decisão precisa ser registrada antes da execução sempre que o cenário permitir. Essa prática favorece avaliação retrospectiva e reduz justificativas construídas apenas após o resultado (ISO, 2015a; SWGDE, 2025).

Os resultados confirmam que a escolha metodológica precisa começar pela pergunta pericial. Se o objetivo é verificar a presença de uma conversa específica, uma aquisição delimitada e validada pode ser suficiente; se é reconstruir atividade de aplicativo ou recuperar registros excluídos, será necessário avaliar técnicas de maior alcance. A decisão deve refletir suficiência, risco e proporcionalidade, e não uma preferência abstrata por profundidade (ISO, 2015a; Kumar, 2021; SWGDE, 2026).

O estado do aparelho funciona como variável metodológica. Em dispositivos protegidos por criptografia associada à autenticação, manter uma sessão útil pode ser mais importante do que obter imediatamente uma cópia bruta. Contudo, essa opção prolonga a atividade e exige controle de energia e rede. A tensão não é resolvida por regra fixa, mas por avaliação documentada das perdas e ganhos de cada ação, com prioridade à preservação das oportunidades que não possam ser recriadas (Apple, 2024; Google, 2026a, 2026b; SWGDE, 2025).

Essa orientação exige planejamento anterior à coleta. Equipes que só definem recursos depois da apreensão podem perder condições transitórias ou agir sem compreender consequências. Protocolos devem prever triagem inicial, materiais de isolamento, alimentação segura, escalonamento técnico e registro de decisão. Ao mesmo tempo, precisam permitir exceções justificadas, pois rigidez excessiva é incompatível com a diversidade de aparelhos e estados encontrados (ISO, 2012, 2015c; SWGDE, 2025).

No entanto, a incrementalidade não deve ser aplicada mecanicamente quando a primeira intervenção puder destruir uma oportunidade única. Em certas configurações, aguardar ou executar procedimento inadequado pode provocar bloqueio, reinicialização ou perda de chaves. O princípio correto é preservar opções e escolher a sequência com base no conhecimento técnico disponível. A prudência pericial é ativa: exige diagnóstico, antecipação e registro, não simples repetição de uma ordem padronizada (Fukami et al., 2021; SWGDE, 2025, 2026).

O princípio de preservação de opções sugere executar, quando compatível, procedimentos menos invasivos antes de ações irreversíveis. Isso não é uma regra de ordem absoluta: em estado crítico, a prioridade pode ser conservar sessão ou dado volátil. O plano deve indicar alternativas, risco de cada uma e critério de parada. Esse registro melhora a aprendizagem institucional, pois permite comparar decisão prevista e resultado, identificando onde protocolos precisam ser atualizados (SWGDE, 2025; Lyle et al., 2022).

Tabela 2 – Síntese comparativa dos métodos de extração

Método	Contribuição principal	Limitação dominante	Critério de escolha
Lógica ou seletiva	Rapidez e menor intervenção para dados disponibilizados pela interface.	Alcance parcial e dependência de permissões ou APIs.	Suficiência para a pergunta e preservação do estado.
Sistema de arquivos	Acesso à estrutura, bancos e metadados internos suportados.	Dependência de chaves, permissões e suporte à versão.	Necessidade de contexto estrutural além da exportação lógica.
Física	Representação mais ampla do armazenamento em cenários compatíveis.	Dados cifrados podem permanecer inacessíveis ou sem contexto.	Compatibilidade técnica e ganho verificável de alcance.
Avançada	Possibilidade de acesso quando métodos convencionais falham.	Maior risco, intervenção e dificuldade de repetição.	Proporcionalidade, competência, justificativa e controle.

Fonte: elaboração própria a partir dos resultados da pesquisa.

4.3 Desafios técnicos e controles metodológicos

A criptografia aparece como o desafio de maior efeito transversal. Ela não impede somente a leitura de arquivos: interfere na escolha da técnica, no valor do estado desbloqueado, na utilidade de uma imagem física e na possibilidade de repetir a aquisição. Nos sistemas atuais, a proteção pode combinar chaves vinculadas ao hardware, credenciais do usuário e estados distintos antes e depois da primeira autenticação. O acesso passa a depender de uma configuração concreta e temporal, e não apenas da posse física do equipamento (Apple, 2024; Fukami et al., 2021; Google, 2026b).

Os mecanismos de bloqueio e autenticação acrescentam um problema de oportunidade. Códigos, biometria, limites de tentativas e autenticação multifator protegem o usuário, mas também fazem com que certas condições de acesso sejam transitórias. A bibliografia examinada recomenda preservar o estado útil já encontrado e evitar ações intuitivas, como reiniciar ou manipular repetidamente o aparelho, antes de avaliar as consequências. O valor pericial da decisão depende de ter sido tomada por profissional competente e de estar ligada a um plano previamente documentado (Fukami et al., 2021; ISO, 2015a; SWGDE, 2025).

A fragmentação de modelos e versões constitui o segundo eixo recorrente. Android e iOS recebem atualizações frequentes, enquanto fabricantes modificam hardware, camadas de sistema e políticas de segurança. Uma ferramenta pode adquirir determinado conjunto em uma combinação e produzir resultado menor ou diferente em outra, ainda que os aparelhos sejam visualmente semelhantes. A compatibilidade declarada não substitui teste: é preciso

registrar modelo, versão, estado, ferramenta, módulo e configuração para que o alcance possa ser avaliado posteriormente (Almuqren et al., 2024; Google, 2026a; Lyle et al., 2022).

A dependência de ferramentas proprietárias cria assimetria adicional. Interfaces automatizadas ampliam produtividade, mas nem sempre revelam todas as transformações realizadas entre aquisição, decodificação e apresentação. Relatórios visualmente organizados podem ocultar falhas de interpretação, artefatos não suportados ou conversões de horário. O resultado tecnicamente mais seguro é aquele em que o examinador consegue retornar ao dado fonte, explicar a regra aplicada e confirmar os elementos decisivos sem depender exclusivamente da tela do produto (Hargreaves et al., 2024; Stoykova & Franke, 2023; Sunde, 2022).

Os dados distribuídos entre aparelho, conta e nuvem dificultam a delimitação da fonte. Um artefato exibido no smartphone pode ser cópia local, miniatura, referência, conteúdo sincronizado ou informação produzida em outro equipamento associado. A análise precisa separar o que foi adquirido do dispositivo daquilo que foi obtido por credencial ou serviço remoto, inclusive porque permissões, temporalidade e cadeia de custódia podem ser distintas. A correlação amplia a compreensão, mas não autoriza atribuir automaticamente ao aparelho toda atividade vinculada à conta (Ayers et al., 2014; Lyle et al., 2022; SWGDE, 2026).

Tabela 3

Desafios técnicos, efeitos periciais e controles correspondentes

Criptografia e estado do aparelho apresentaram a associação mais forte. A literatura convergiu em que acesso depende da disponibilidade de chaves e de condições que podem mudar com bloqueio, reinicialização ou tempo. Esse achado desloca a preservação para o início do raciocínio: conservar estado útil pode ser mais determinante do que selecionar imediatamente a ferramenta. O risco correlato é manter atividade e conectividade. A decisão deve equilibrar perdas e benefícios, com justificativa e registros temporais (Apple, 2024; Fukami et al., 2021; SWGDE, 2025).

Fragmentação e atualização apareceram como fatores que reduzem generalização. O desempenho observado em uma combinação não pode ser transferido automaticamente a modelo ou versão semelhante. Isso exige granularidade no inventário e na validação. O suporte declarado precisa ser conferido quanto à função e ao artefato, não apenas ao aparelho. Quando a combinação não foi testada, o achado deve receber confirmação adicional ou linguagem mais cautelosa (Almuqren et al., 2024; SWGDE, 2024).

A opacidade das ferramentas foi associada a erros silenciosos. Interfaces podem ocultar transformações, normalizar valores e consolidar duplicidades. O controle mais frequente foi o retorno ao dado fonte, acompanhado por comparação independente. Nos aplicativos de mensagens, a estrutura criptografada e as mudanças de esquema tornam esse controle especialmente importante. Resultados visuais precisam ser sustentados por arquivo, campo e regra de interpretação identificáveis (Hargreaves et al., 2024; Prabowo et al., 2025).

A pergunta de pesquisa buscou identificar os principais desafios técnicos presentes na extração, preservação e validação de evidências digitais em dispositivos móveis. A análise permite responder que esses desafios decorrem da interação entre proteção criptográfica, estado transitório do aparelho, diversidade de modelos e versões, opacidade de ferramentas, mutabilidade do ambiente e necessidade de demonstrar integridade e significado. Nenhum desses fatores atua de forma inteiramente isolada; uma limitação de acesso repercute no alcance, na repetição possível, na interpretação e na maneira de comunicar o resultado (Fukami et al., 2021; Gruber et al., 2023; Hargreaves et al., 2024).

Essa resposta afasta duas simplificações. A primeira é imaginar que a perícia se resolve pela obtenção da maior quantidade possível de dados. Volume não equivale a relevância, completude ou confiabilidade. A segunda é presumir que a ferramenta comercial transfere sua credibilidade ao achado. O resultado só se sustenta quando o método é adequado à pergunta, o alcance foi demonstrado e os artefatos centrais foram confirmados dentro de seu contexto (Lyle et al., 2022; Stoykova & Franke, 2023; SWGDE, 2024).

A extração deve, portanto, ser compreendida como produção controlada de uma representação, e não como reprodução perfeita e neutra do aparelho. Interfaces, permissões, chaves e transformações determinam o que entra no conjunto. Essa compreensão é especialmente importante para smartphones, nos quais o sistema pode permanecer ativo e distribuir dados entre armazenamento local e serviços sincronizados. O laudo ganha precisão quando descreve o que foi obtido e como, em vez de usar rótulos genéricos de completude (Ayers et al., 2014; Fukami et al., 2021; SWGDE, 2026).

Em consequência, a confiabilidade da prova digital móvel não é qualidade presumida de um arquivo. Ela é uma conclusão sustentada por cadeia de decisões verificáveis: identificação, preservação, aquisição, controle, interpretação e relato. Esse caráter processual aproxima as normas de evidência digital dos requisitos gerais de competência laboratorial e reforça a importância de procedimentos atualizados, revisão técnica e registros que permitam avaliar o trabalho depois de concluído (ISO, 2012, 2017; Stoykova & Franke, 2023).

A análise também mostra que confiabilidade é graduada e sustentada por evidências. Um achado confirmado em fonte, coerente com registros independentes e produzido por função testada possui suporte maior do que item exibido por uma única interface. Essa gradação deve aparecer na linguagem do laudo. Não se trata de substituir conclusão por dúvida generalizada, mas de calibrar afirmação conforme o percurso demonstrado. A transparência permite valorar adequadamente o resultado e fortalece, em vez de enfraquecer, a atuação pericial (Stoykova & Franke, 2023; Sunde, 2022).

Tabela 3 – Desafios técnicos, efeitos periciais e controles correspondentes

Desafio	Efeito sobre o exame	Controle metodológico
Criptografia e bloqueio	Restrição do acesso e dependência do estado de autenticação.	Preservar o estado, avaliar a oportunidade e justificar intervenções.
Fragmentação e atualização	Variação de suporte e de alcance entre modelos e versões.	Registrar versões, testar combinações e evitar generalizações.
Automação proprietária	Omissão de transformações ou artefatos não suportados.	Retornar à fonte e confirmar achados relevantes.
Contaminação	Criação, alteração ou perda de registros durante o exame.	Antecipar, minimizar, registrar e avaliar o impacto.
Dados distribuídos	Confusão entre aparelho, conta, nuvem e equipamento vinculado.	Identificar origem, forma de obtenção e limites de atribuição.

Fonte: elaboração própria a partir dos resultados da pesquisa.

4.4 Preservação, cadeia de custódia e validação

A preservação foi identificada como atividade iniciada no primeiro contato e mantida até o arquivamento. Não se limita à guarda física nem começa depois da aquisição. Registro fotográfico, identificação, horário, condições de energia, tela, conexões, cartões, cabos e ambiente formam a base para interpretar as ações posteriores. O procedimento preserva não somente o dispositivo, mas o contexto necessário para explicar por que determinada técnica foi escolhida e quais mudanças eram previsíveis (ISO, 2012; SWGDE, 2025).

O isolamento de rede surgiu como medida importante, porém não absoluta. Impedir comunicações pode reduzir sincronização, comandos remotos e tráfego, mas determinados modos de isolamento alteram o comportamento do aparelho, exigem interação ou podem ser incompletos. O resultado mais consistente é uma avaliação contextual: identificar interfaces ativas, selecionar o recurso compatível, verificar sua eficácia e monitorar o estado. A documentação do isolamento é tão relevante quanto a própria decisão de isolá-lo (Ayers et al., 2014; Gruber et al., 2023; SWGDE, 2025).

A continuidade de energia também exige decisão orientada por risco. Manter o aparelho ligado pode preservar chaves, sessões e dados acessíveis; ao mesmo tempo, aumenta o período de atividade e a possibilidade de alteração. O material analisado não sustenta uma regra automática. Sustenta que a equipe deve considerar autonomia, possibilidade de recarga segura, estado de desbloqueio, risco de reinicialização e disponibilidade de recurso de aquisição, registrando eventos e horários relevantes (Apple, 2024; Fukami et al., 2021; SWGDE, 2025).

Durante e depois da aquisição, a cadeia de custódia deve registrar pessoas, datas, locais, finalidade, transferência, armazenamento, acesso e condição do item. No meio digital, acrescentam-se identificadores de arquivos, hashes, logs, versões, caminhos, cópias mestres e derivados. Esses elementos cumprem funções complementares: o hash verifica igualdade de uma representação em momentos distintos, enquanto a trilha documental explica origem, posse, processamento e vínculo entre o conjunto adquirido e o resultado apresentado (Brasil, 1941; ISO, 2012; SWGDE, 2026).

A apresentação da prova completa esse percurso. Exportações, planilhas, capturas de tela e relatórios são representações derivadas e precisam permanecer vinculados ao artefato fonte. A preservação da cópia mestre permite nova leitura quando houver dúvida, atualização de ferramenta ou necessidade de auditoria. Identificar claramente os derivados impede que uma visualização seja confundida com o dado original e mantém aberta a possibilidade de revisão por outro profissional qualificado (ISO, 2015b; Stoykova & Franke, 2023; SWGDE, 2026).

A cadeia de custódia foi tratada como estrutura de proveniência. Transferências físicas continuam necessárias, mas a rastreabilidade digital requer documentar processos e transformações. Logs, hashes, versões, responsáveis e parâmetros permitem explicar como um item chegou ao relatório. A ausência de um desses elementos não produz efeito automático idêntico em todos os casos; seu impacto depende do ponto e da possibilidade de verificação alternativa. O protocolo deve tornar essa avaliação possível, em vez de ocultar lacunas (Brasil, 1941; INTERPOL, 2019).

A análise também identificou que hashes podem ser supervalorizados. Eles demonstram igualdade de bytes entre objetos definidos, mas não comprovam origem, completude nem significado. Seu uso adequado exige indicar o objeto calculado, algoritmo, momento e resultado. Em conjuntos complexos, manifestos por arquivo ou contêineres verificáveis podem oferecer rastreabilidade adicional. O hash integra a cadeia, mas não

substitui a documentação da aquisição e da interpretação (ISO, 2012, 2015b; Lyle et al., 2022).

A validação aparece no corpus como verificação de adequação para uma finalidade definida. Não basta demonstrar que uma ferramenta funciona em termos gerais; é necessário saber se ela identifica, adquire ou interpreta corretamente o tipo de dado envolvido no exame. Isso requer conjuntos com conteúdo conhecido, resultados esperados, critérios de aceitação e registros suficientes para repetir o teste. O nível de esforço deve acompanhar o risco: achados decisivos exigem confirmação mais robusta do que dados meramente orientativos (ISO, 2015a, 2017; SWGDE, 2024).

A confiabilidade foi associada a três níveis. No primeiro, verifica-se a aquisição: se o conjunto obtido corresponde ao alcance declarado e se erros foram registrados. No segundo, verifica-se a decodificação: se bancos, horários, identificadores e relações foram traduzidos corretamente. No terceiro, examina-se a interpretação: se o significado atribuído é compatível com a origem, o contexto e as hipóteses alternativas. Separar esses níveis evita tratar um relatório bem formatado como demonstração suficiente da correção de todo o processo (Hargreaves et al., 2024; Lyle et al., 2022; Stoykova & Franke, 2023).

A confirmação independente dos achados centrais foi uma recomendação comum. Ela pode ocorrer pela inspeção da estrutura fonte, uso de método tecnicamente diverso, comparação com dado conhecido ou correlação com registro externo legítimo. Empregar duas interfaces que utilizam a mesma biblioteca interna não garante independência. O objetivo não é multiplicar ferramentas, mas reduzir a possibilidade de um único erro de aquisição ou interpretação determinar a conclusão (Hargreaves et al., 2024; SWGDE, 2024, 2026).

Repetibilidade e reprodutibilidade foram tratadas como propriedades desejáveis, mas condicionadas pela mutabilidade dos dispositivos. Repetir uma operação no mesmo aparelho pode produzir diferenças temporais, enquanto outro laboratório pode não dispor da mesma versão, licença ou vulnerabilidade. Por isso, a avaliação deve considerar se o procedimento foi suficientemente descrito, se as diferenças esperadas foram reconhecidas e se os elementos estáveis puderam ser confirmados. A transparência sobre o que não pode ser reproduzido é parte da confiabilidade, e não admissão automática de falha (ISO, 2015b, 2017; Lyle et al., 2022).

O relatório foi identificado como último mecanismo de controle. Ele deve distinguir observação, processamento e inferência; indicar versões, alcance e limitações; e evitar afirmações absolutas quando a aquisição foi parcial. A ausência de um registro pode significar

inexistência, eliminação, criptografia, falta de suporte ou exclusão pelo método. Comunicar essas possibilidades preserva a força legítima da prova sem transformar lacunas técnicas em certezas indevidas (Lyle et al., 2022; Stoykova & Franke, 2023; Sunde, 2022).

Nota. Estrutura analítica baseada na distinção entre aquisição, processamento, interpretação e comunicação (Hargreaves et al., 2024; Stoykova & Franke, 2023; SWGDE, 2024).

Os documentos analisados convergiram quanto à reavaliação após mudanças. Atualização de ferramenta, sistema, aplicativo ou configuração pode alterar comportamento. Registros de versão e testes regressivos precisam integrar a rotina, com intensidade proporcional ao risco. Relatórios externos, como os produzidos em iniciativas do NIST, são evidência complementar; sua aplicabilidade depende da correspondência entre a configuração testada e o uso local (National Institute of Standards and Technology, 2026; SWGDE, 2024).

A confiabilidade final também depende da objetividade do examinador. Automação, expectativa investigativa e volume podem favorecer aceitação seletiva. Revisão técnica, hipóteses alternativas e separação entre dado e inferência funcionam como controles. Confirmar apenas resultados compatíveis com a narrativa esperada não constitui validação. O processo deve procurar ativamente explicações concorrentes e registrar quando não há informação suficiente para distingui-las (Sunde, 2022; Stoykova & Franke, 2023).

A cadeia de custódia exerce dupla função. No plano técnico, permite acompanhar o item, as cópias, os acessos e as transformações. No plano jurídico, fornece elementos para demonstrar identidade, continuidade e confiabilidade do vestígio apresentado. Essas funções se encontram na documentação: um formulário sem descrição das intervenções é insuficiente para avaliar o efeito técnico, enquanto um procedimento sofisticado sem registro perde capacidade de ser escrutinado (Brasil, 1941; ISO, 2012; SWGDE, 2026).

A aplicação ao ambiente móvel requer abandonar a expectativa de imobilidade absoluta. Smartphones ligados executam processos e podem registrar mudanças mesmo durante uma coleta correta. A integridade precisa ser compreendida como controle e explicação das alterações relevantes, com preservação do conteúdo adquirido e demonstração de que o procedimento não comprometeu a conclusão. Essa visão é mais rigorosa do que afirmar genericamente que nada mudou, porque enfrenta a natureza real do sistema examinado (Gruber et al., 2023; Lyle et al., 2022).

O hash permanece essencial, mas sua função precisa ser corretamente delimitada. Ele demonstra igualdade entre representações digitais submetidas ao mesmo cálculo e ajuda a controlar cópias e transferências. Não identifica sozinho quem coletou, como o dado foi gerado, quais áreas ficaram de fora ou que alterações ocorreram antes da aquisição. A força da cadeia resulta da combinação entre verificação matemática e documentação contextual (ISO, 2012; SWGDE, 2025, 2026).

No contexto brasileiro, os arts. 158-A e seguintes do Código de Processo Penal conferem relevância expressa à cadeia de custódia. Embora a legislação apresente etapas gerais, sua aplicação a evidências digitais demanda detalhamento técnico por protocolos, normas e boas práticas. O diálogo entre o texto legal e referências como ISO/IEC 27037 e SWGDE permite traduzir exigências de reconhecimento, coleta, acondicionamento e processamento para objetos que são copiáveis, mutáveis e dependentes de software (Brasil, 1941; ISO, 2012; SWGDE, 2025).

A rastreabilidade também sustenta o contraditório. Permitir que outro especialista localize a fonte e compreenda as transformações é condição para crítica informada. Isso não exige revelar material irrelevante ou sensível sem base, mas fornecer documentação suficiente sobre o item usado. A separação entre cópia mestre e recortes apresentados permite preservar o conjunto e comunicar somente o necessário, conciliando auditabilidade e minimização (ISO, 2015b; INTERPOL, 2019).

A discussão sobre ferramentas revela que validação não é atributo permanente transferido pelo fabricante. Uma solução pode ter apresentado desempenho adequado em teste anterior e produzir comportamento diferente depois de atualização, alteração de módulo ou uso em combinação não testada. Laboratórios precisam definir funções críticas, manter dados de referência e reavaliar mudanças que possam afetar aquisição ou interpretação (ISO, 2017; Lyle et al., 2022; SWGDE, 2024).

A validação também deve abranger erros plausíveis, não apenas o cenário em que o produto funciona. Testes úteis verificam omissões, valores incorretos, conversões de horário, duplicidades, falhas de importação e mensagens de erro. Essa perspectiva se alinha ao modelo de análise de erros proposto por Hargreaves et al., pois busca entender onde o processo pode falhar e quais controles detectam a falha antes que ela alcance o laudo (Hargreaves et al., 2024; SWGDE, 2024).

A reprodutibilidade precisa ser avaliada com realismo. Nem todos os estados de um aparelho podem ser reconstruídos, e determinados recursos proprietários ou vulnerabilidades podem não estar disponíveis a outro examinador. Ainda assim, é possível tornar o raciocínio auditável por meio de documentação de versões, entradas, parâmetros, etapas, saídas e verificações. O aspecto decisivo é permitir que outro profissional compreenda a base da conclusão e teste os elementos que permanecem acessíveis (ISO, 2015b; Stoykova & Franke, 2023).

A objetividade não significa ausência de julgamento. Escolher método, filtrar dados e relacionar eventos são decisões profissionais. O controle possível é explicitar critérios, separar observação de inferência e submeter conclusões a verificação. A confiabilidade cresce quando o examinador reconhece limites e reduz afirmações categóricas que não possam ser sustentadas pelos dados e pelo alcance da ferramenta (Stoykova & Franke, 2023; Sunde, 2022; SWGDE, 2026).

Reprodutibilidade parcial deve ser informada com precisão. Se não é possível repetir o estado do aparelho, ainda pode ser possível repetir a análise sobre a aquisição preservada. Se o formato é proprietário, pode ser necessário manter ambiente compatível ou exportações verificáveis. O plano de preservação deve antecipar a obsolescência, incluindo documentação de versão, formatos e dependências. A longevidade do caso pode superar a do software, tornando a conservação do contexto parte da confiabilidade (ISO, 2017; Lyle et al., 2022).

4.5 Síntese integrada e implicações para a Criminalística

A integração das categorias mostra que a qualidade da evidência móvel é cumulativa. Uma aquisição tecnicamente possível pode perder valor se o estado inicial não foi registrado; uma cópia íntegra pode ser interpretada incorretamente; e um artefato corretamente decodificado pode ser apresentado com certeza maior do que seu contexto permite. Extração, preservação, validação e comunicação funcionam como elos interdependentes, de modo que o controle tardio não compensa integralmente uma decisão inicial não documentada (ISO, 2012, 2015b; Lyle et al., 2022).

Os resultados respondem aos objetivos específicos. Foram diferenciados os principais métodos e seus limites; identificados criptografia, bloqueio, fragmentação, atualizações, automação, contaminação e distribuição dos dados como desafios centrais; examinados os elementos técnicos e jurídicos da cadeia de custódia; e sistematizados critérios de validação, confirmação e relato. A convergência entre esses eixos sustenta uma prática baseada em

adequação e rastreabilidade, não em confiança presumida na ferramenta (Almuqren et al., 2024; Hargreaves et al., 2024; SWGDE, 2025, 2026).

A matriz resultante pode ser resumida em sete movimentos: delimitar a pergunta; registrar o estado; preservar oportunidades e riscos; selecionar método proporcional; verificar aquisição e decodificação; interpretar com correlação e hipóteses alternativas; e relatar alcance, limitações e rastreabilidade. Esses movimentos não constituem roteiro rígido para todos os aparelhos, mas critérios de decisão aplicáveis a protocolos institucionais e adaptáveis à evolução tecnológica (ISO, 2015a, 2015c; Stoykova & Franke, 2023).

A síntese produziu seis perguntas de controle: qual era o estado e o contexto; que pergunta orientou a aquisição; qual método foi escolhido e por quê; que mudanças e transferências foram registradas; como funções e achados foram validados; e quais limites foram comunicados. Essas perguntas são aplicáveis em diferentes tecnologias porque descrevem requisitos, não receitas. O modelo resultante funciona como instrumento de planejamento, revisão e relato, devendo ser adaptado às políticas e à legislação do laboratório (ISO, 2015a, 2015b; SWGDE, 2025, 2026).

Como produto aplicado da pesquisa, foram elaborados dois apêndices: uma matriz de decisão para métodos e um checklist de cadeia, validação e relato. Eles não certificam procedimentos; traduzem os achados em perguntas documentáveis. Seu uso exige competência e adaptação. A utilidade está em tornar explícitos critérios que podem permanecer implícitos e, assim, favorecer consistência, revisão e aprendizado institucional (INTERPOL, 2019; ISO, 2017; SWGDE, 2024).

Para a Criminalística, os achados indicam que a capacidade institucional não pode ser medida somente pela posse de ferramentas. Infraestrutura deve ser acompanhada por procedimentos, testes, qualificação, controle de versões, registros e revisão. Sem esses elementos, o aumento da capacidade de aquisição pode ampliar igualmente a produção de resultados incompletos ou mal interpretados. O investimento mais consistente combina tecnologia e governança técnica (ISO, 2017; Lyle et al., 2022; SWGDE, 2024).

A padronização nacional deve estabelecer requisitos mínimos sem congelar técnicas. Protocolos excessivamente vinculados a marcas ou passos imutáveis envelhecem rapidamente. É preferível definir resultados de controle: registrar estado, justificar o método, preservar conjuntos, documentar mudanças, testar funções críticas, confirmar achados relevantes e relatar limitações. Cada laboratório pode implementar esses requisitos conforme

sua estrutura, mantendo evidências de conformidade (ISO, 2012, 2015a; SWGDE, 2025, 2026).

Uma terminologia funcional também contribuiria para a comparabilidade. Laudos deveriam explicar quais dados foram adquiridos, de quais áreas, por qual mecanismo e com quais exclusões, reduzindo dependência de rótulos como lógica, física ou completa. Essa descrição facilita o exame por peritos assistentes, autoridades e julgadores, além de evitar que técnicas diferentes sejam tratadas como equivalentes apenas porque receberam o mesmo nome (Fukami et al., 2021; Lyle et al., 2022).

A qualidade do laudo também depende de comunicação acessível. Termos técnicos precisam ser definidos, incertezas preservadas e limitações ligadas ao efeito concreto sobre a conclusão. Um documento compreensível não simplifica o método de forma indevida; torna visível a cadeia lógica que liga fonte, procedimento, achado e inferência. Esse cuidado favorece controle jurisdicional e uso proporcional da prova (Stoykova & Franke, 2023; Sunde, 2022).

A implementação requer governança: responsáveis por aprovar métodos, controlar versões, manter testes, registrar competência e tratar não conformidades. Adquirir ferramentas sem essa estrutura amplia capacidade de processamento, mas não assegura qualidade. Resultados de ensaios compartilhados podem reduzir duplicação, desde que sejam avaliados para a configuração local. Redes de laboratórios podem cooperar na construção de conjuntos de teste e divulgação de limitações, fortalecendo transparência (National Institute of Standards and Technology, 2026; ISO, 2017).

A principal limitação deste estudo é não ter realizado ensaios laboratoriais com aparelhos e ferramentas. As conclusões sistematizam o que a literatura e os documentos técnicos permitem afirmar, mas não medem desempenho, taxa de recuperação ou erro de produtos específicos. Esse limite foi preservado na linguagem: as recomendações se referem ao processo e precisam ser validadas antes de sua adoção operacional em cada ambiente (Gil, 2022; Lyle et al., 2022).

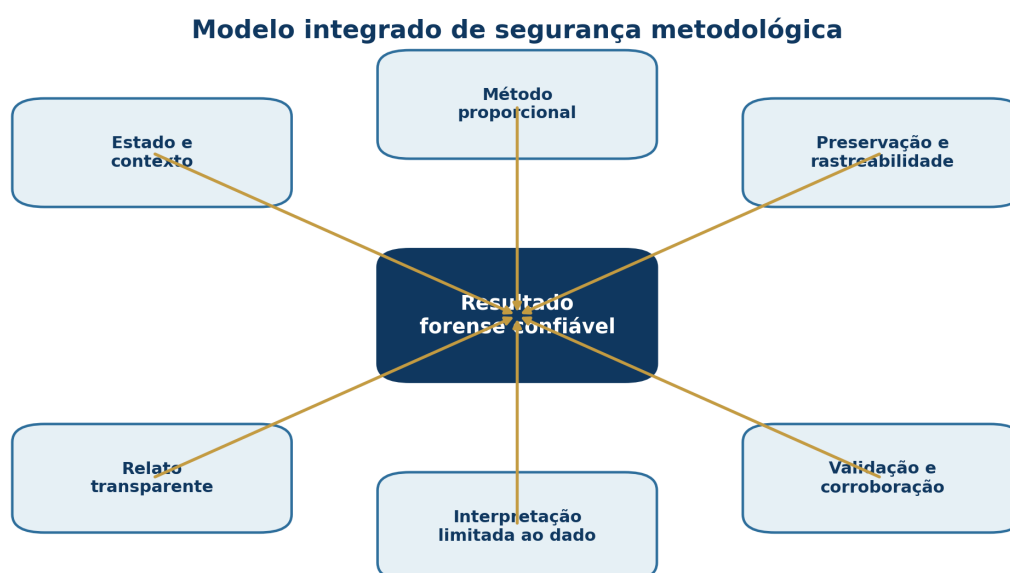
A documentação pública das ferramentas proprietárias constitui outra restrição. Parte das rotinas internas, dos formatos e das condições de exploração não é integralmente divulgada, dificultando comparação independente. A pesquisa compensou essa limitação privilegiando requisitos de verificação e retorno ao dado fonte, mas não elimina a necessidade de testes institucionais controlados e participação em programas de avaliação de ferramentas (National Institute of Standards and Technology, n.d.; SWGDE, 2024).

Como perspectiva empírica, recomenda-se construir conjuntos de teste representativos de versões Android e iOS, documentar estados de bloqueio, executar métodos compatíveis e comparar aquisição, decodificação e relatório entre ferramentas. O estudo deve ser replicável, evitar dados pessoais reais e registrar erros, omissões e diferenças. Esse desenho permitiria transformar a matriz qualitativa desta pesquisa em protocolo avaliado por evidências laboratoriais (ISO, 2017; Hargreaves et al., 2024; SWGDE, 2024).

Outra linha é avaliar aplicabilidade do checklist por revisores independentes. Estudos podem verificar concordância entre avaliadores, campos ambíguos, tempo de uso e falhas detectadas. A matriz também pode ser adaptada a aplicativos específicos, preservando o núcleo geral. Pesquisas sobre mensagens criptografadas, por exemplo, podem testar diferentes versões de banco e chave, correlacionando saídas com a estrutura fonte (Prabowo et al., 2025; Stoykova & Franke, 2023).

A evolução de serviços em nuvem, inteligência artificial e ambientes conectados tende a ampliar a distribuição da evidência. Trabalhos posteriores devem examinar proveniência de dados sincronizados, decisões automatizadas e validade de classificadores. O princípio permanece: cada transformação precisa ser explicada e validada para o uso pretendido. A incorporação de novas técnicas não dispensa competência, rastreabilidade e possibilidade de contestação (Lyle et al., 2022; ISO, 2015a, 2015b).

Figura 3 – Modelo integrado de segurança metodológica para a evidência móvel



Fonte: elaboração própria a partir da síntese dos resultados.

5 Conclusão

A pesquisa alcançou o objetivo geral de analisar os principais desafios técnicos envolvidos na extração, preservação e validação de evidências digitais em dispositivos móveis. A revisão demonstrou que a confiabilidade não é produzida por uma etapa isolada, mas pela coerência do percurso completo. Estado do aparelho, escolha da técnica, controle de alterações, validação das funções utilizadas, interpretação contextual e relato transparente precisam convergir para que o resultado possa ser tecnicamente examinado e juridicamente valorado (ISO, 2012, 2015b; Lyle et al., 2022).

Quanto aos métodos de extração, conclui-se que não existe técnica universalmente superior. Aquisições lógicas, seletivas, de sistema de arquivos, físicas e avançadas apresentam alcances e riscos distintos. A opção adequada é aquela que responde à pergunta pericial com intervenção proporcional, preserva oportunidades relevantes e permite explicar o conteúdo efetivamente obtido. Profundidade nominal não deve ser confundida com completude, sobretudo quando criptografia e proteção de chaves mantêm dados brutos inacessíveis (Fukami et al., 2021; Google, 2026b; SWGDE, 2026).

Os desafios mais relevantes foram a criptografia, os bloqueios de acesso, a fragmentação de modelos e versões, as atualizações, a dependência de ferramentas proprietárias, a contaminação e a distribuição de dados entre dispositivo e serviços associados. Esses fatores tornam o exame dependente de contexto e reduzem a validade de generalizações. A resposta técnica consiste em registrar combinações específicas, preservar o estado, atualizar testes e declarar limites, em vez de pressupor que resultados anteriores permanecerão aplicáveis (Almuqren et al., 2024; Gruber et al., 2023; Hargreaves et al., 2024).

A cadeia de custódia mostrou-se inseparável da metodologia. Identificação, documentação de transferências, hashes, logs, cópias mestres, derivados e registros de acesso formam um sistema de rastreabilidade. O hash é indispensável para verificar cópias, mas não substitui a narrativa técnica sobre origem, alcance e mudanças. Em aparelhos ativos, integridade significa controlar, registrar e avaliar alterações relevantes, e não prometer uma imobilidade incompatível com o funcionamento do sistema (Brasil, 1941; ISO, 2012; SWGDE, 2025).

A validação deve abranger aquisição, decodificação, interpretação e relato. Funções críticas precisam ser testadas com dados conhecidos e reavaliadas após mudanças relevantes de versão ou configuração. Achados centrais devem ser confirmados por procedimento independente, sempre que possível, e submetidos a revisão técnica. A confiabilidade se fortalece quando o examinador consegue explicar tanto o resultado quanto as possibilidades de erro e as hipóteses alternativas (ISO, 2017; Stoykova & Franke, 2023; SWGDE, 2024).

Para a prática criminalística, recomenda-se que laboratórios adotem protocolos baseados em requisitos de controle, mantenham registros de competência e versão, definam níveis de validação proporcionais ao risco e preservem os conjuntos fonte para auditoria. Os laudos devem separar dado, processamento e inferência, evitando expressões absolutas quando o alcance for parcial. Essas medidas aumentam a consistência sem impedir adaptação a novas tecnologias (Lyle et al., 2022; Sunde, 2022; SWGDE, 2026).

O estudo também evidencia que limitações declaradas não enfraquecem automaticamente a prova. Ao contrário, delimitam o campo em que a conclusão permanece válida e permitem que terceiros avaliem sua força. A omissão de incertezas cria aparência de segurança, mas reduz a transparência. A comunicação tecnicamente responsável preserva a utilidade do achado e impede que uma ausência, uma correlação ou um dado derivado receba significado superior ao permitido pelo método (Stoykova & Franke, 2023; Sunde, 2022).

Por se tratar de pesquisa bibliográfica e documental, as conclusões não equivalem à certificação de ferramentas ou à comprovação experimental de desempenho. O trabalho oferece uma síntese fundamentada e uma matriz de decisão que podem orientar protocolos e futuras pesquisas. A etapa seguinte mais adequada é a validação empírica dessa matriz em conjuntos controlados, com aparelhos, versões e estados documentados, respeitando integridade, legalidade e proteção de dados (Gil, 2022; Hargreaves et al., 2024; SWGDE, 2024).

Em resposta final ao problema, garantir evidências móveis íntegras e confiáveis diante de criptografia, bloqueios e limitações técnicas exige combinar competência, proporcionalidade, rastreabilidade e verificação. Nenhuma ferramenta elimina a necessidade de raciocínio pericial, e nenhum controle isolado assegura a validade do conjunto. A solidez decorre da possibilidade de reconstruir as decisões, compreender as transformações e relacionar cada conclusão ao dado que efetivamente a sustenta (ISO, 2015a, 2015b; Lyle et al., 2022; SWGDE, 2026).

Em termos aplicados, recomenda-se que cada exame produza uma declaração de alcance, uma trilha entre fonte e achado e uma justificativa das verificações executadas. Laboratórios devem manter testes por função e versão, revisar resultados críticos e registrar não conformidades. Quando uma limitação persistir, ela deve ser incorporada à conclusão de modo proporcional. A prova digital se fortalece quando seu percurso pode ser compreendido, repetido no nível possível e criticado com base em registros, e não quando apresenta certeza maior do que o método sustenta (ISO, 2017; Lyle et al., 2022; Stoykova & Franke, 2023).

Referências

- AL-DHAQM, A. et al. **A review of mobile forensic investigation process models**. IEEE Access, v. 8, p. 173359–173375, 2020. DOI: <https://doi.org/10.1109/ACCESS.2020.3014615>.
- ALMUQREN, A. et al. **A systematic literature review on digital forensic investigation on Android devices**. Procedia Computer Science, v. 235, p. 1332–1352, 2024. DOI: <https://doi.org/10.1016/j.procs.2024.04.126>.
- APPLE. **Data Protection overview**. Apple Platform Security, 2024. Disponível em: <https://support.apple.com/guide/security/data-protection-overview-secf6276da8a/web>. Acesso em: 21 jul. 2026.
- AYERS, R.; BROTHERS, S.; JANSEN, W. **Guidelines on mobile device forensics**. Gaithersburg: National Institute of Standards and Technology, 2014. (NIST Special Publication 800-101 Rev. 1). DOI: <https://doi.org/10.6028/NIST.SP.800-101r1>.
- BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941: Código de Processo Penal**. Brasília, DF: Presidência da República, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 21 jul. 2026.
- FUKAMI, A.; STOYKOVA, R.; GERADTS, Z. **A new model for forensic data extraction from encrypted mobile devices**. Forensic Science International: Digital Investigation, v. 38, art. 301169, 2021. DOI: <https://doi.org/10.1016/j.fsidi.2021.301169>.
- GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. São Paulo: Atlas, 2022.
- GOOGLE. **File-based encryption**. Android Open Source Project, 2026a. Disponível em: <https://source.android.com/docs/security/features/encryption/file-based>. Acesso em: 21 jul. 2026.
- GOOGLE. **Hardware-wrapped keys**. Android Open Source Project, 2026b. Disponível em: <https://source.android.com/docs/security/features/encryption/hw-wrapped-keys>. Acesso em: 21 jul. 2026.
- GRUBER, J.; HARGREAVES, C. J.; FREILING, F. C. **Contamination of digital evidence: understanding an underexposed risk**. Forensic Science International: Digital Investigation, v. 44, supl., art. 301501, 2023. DOI: <https://doi.org/10.1016/j.fsidi.2023.301501>.
- HARGREAVES, C.; NELSON, A.; CASEY, E. **An abstract model for digital forensic analysis tools: a foundation for systematic error mitigation analysis**. Forensic Science

International: Digital Investigation, v. 48, supl., art. 301679, 2024. DOI: <https://doi.org/10.1016/j.fsidi.2023.301679>.

INTERNATIONAL CRIMINAL POLICE ORGANIZATION. **INTERPOL global guidelines for digital forensics laboratories**. Lyon: INTERPOL, 2019. Disponível em: https://www.interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf. Acesso em: 21 jul. 2026.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27037:2012: Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence**. Geneva: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27041:2015: Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method**. Geneva: ISO, 2015a.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27042:2015: Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence**. Geneva: ISO, 2015b.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27043:2015: Information technology — Security techniques — Incident investigation principles and processes**. Geneva: ISO, 2015c.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 17025:2017: General requirements for the competence of testing and calibration laboratories**. Geneva: ISO, 2017.

KUMAR, M. **Mobile phone forensics: a systematic approach, tools, techniques and challenges**. International Journal of Electronic Security and Digital Forensics, v. 13, n. 1, p. 64–87, 2021. DOI: <https://doi.org/10.1504/IJESDF.2021.111725>.

LYLE, J. R. et al. **Digital investigation techniques: a NIST scientific foundation review**. Gaithersburg: National Institute of Standards and Technology, 2022. (NISTIR 8354). DOI: <https://doi.org/10.6028/NIST.IR.8354>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Mobile devices**. Computer Forensics Tool Testing Program, [s. d.]. Disponível em: <https://www.nist.gov/itl/csd/secure-systems-and-applications/computer-forensics-tool-testing-program-cftt/cftt-7>. Acesso em: 21 jul. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Mobile forensics: federated testing**. 2026. Disponível em: <https://csrc.nist.gov/projects/mobile-forensics/federated-testing>. Acesso em: 21 jul. 2026.

PRABOWO, W. A.; MOHSEN, F.; SELAMAT, S. R. **WhatsApp mobile applications in the lens of digital forensics: deciphering the Msgstore.db.crypt14 file**. Journal of Cyber Security and Mobility, v. 14, n. 4, p. 823–848, 2025. DOI: <https://doi.org/10.13052/jcsm2245-1439.1443>.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. **Minimum requirements for testing tools used in digital and multimedia forensics**. SWGDE 18-Q-001-2.1, 2024. Disponível em: <https://www.swgde.org/documents/published-complete-listing/>. Acesso em: 21 jul. 2026.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. **Best practices for mobile device evidence collection and preservation, handling, and acquisition.** SWGDE 18-F-003-2.0, 2025. Disponível em: <https://www.swgde.org/documents/published-complete-listing/18-f-003-2/>. Acesso em: 21 jul. 2026.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. **Best practices for mobile device forensic analysis.** SWGDE 20-F-005-2.0, 2026. Disponível em: <https://www.swgde.org/documents/published-complete-listing/20-f-005-swgde-best-practices-for-mobile-device-forensic-analysis/>. Acesso em: 21 jul. 2026.

STOYKOVA, R.; FRANKE, K. **Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations.** Forensic Science International: Digital Investigation, v. 45, art. 301554, 2023. DOI: <https://doi.org/10.1016/j.fsidi.2023.301554>.

SUNDE, N. **Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations.** Forensic Science International: Digital Investigation, v. 40, art. 301317, 2022. DOI: <https://doi.org/10.1016/j.fsidi.2021.301317>.