SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS – UEG
COORDENADORIA DE ENSINO – COE
COORDENAÇÃO DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO
ESPECIALIZAÇÃO EM ALTOS ESTUDOS DE SEGURANÇA PÚBLICA

STÉPHANNY RIBEIRO DA SILVA

PROPOSTA DE APRIMORAMENTO DA CADEIA DE CUSTÓDIA DE VESTÍGIOS DIGITAIS DA POLÍCIA CIENTÍFICA DO ESTADO DE GOIÁS

GOIÂNIA – GO

2025

STÉPHANNY RIBEIRO DA SILVA

PROPOSTA DE APRIMORAMENTO DA CADEIA DE CUSTÓDIA DE VESTÍGIOS DIGITAIS DA POLÍCIA CIENTÍFICA DO ESTADO DE GOIÁS

Artigo apresentado como exigência parcial para conclusão do Curso de Especialização em Altos Estudos de Segurança Pública - CAESP, pela Secretaria de Segurança Pública do Estado de Goiás – SSP/GO e pela Universidade Estadual de Goiás - UEG, sob a orientação do Prof. Ma. Francyelle Pereira e Silva Umbelino.

GOIÂNIA – GO

2025

PROPOSTA DE APRIMORAMENTO DA CADEIA DE CUSTÓDIA DE VESTÍGIOS DIGITAIS DA POLÍCIA CIENTÍFICA DO ESTADO DE GOIÁS

PROPOSAL TO IMPROVE CHAIN OF CUSTODY FOR DIGITAL EVIDENCE IN GOIÁS FORENSIC SCIENCE DEPARTMENT

Discente Stéphanny Ribeiro da Silva[1]
Orientadora Ma. Francyelle Pereira e Silva Umbelino [2]

Resumo: A cadeia de custódia de vestígios digitais impõe desafios específicos decorrentes da volatilidade, da facilidade de alteração e da inexistência de normativas nacionais padronizadas aplicáveis ao contexto pericial. Este estudo examinou o fluxo de tratamento de vestígios digitais na Polícia Científica do Estado de Goiás (PCI/GO), com foco nos vestígios derivados de suportes físicos e na forma como são registrados e administrados pelo Sistema ODIN. A pesquisa adotou abordagem qualitativa, combinando revisão bibliográfica e análise documental, estruturadas segundo o método hipotético-dedutivo, a partir do qual se investigou o problema da ausência de fluxos padronizados para a custódia digital na instituição. Foram analisadas normativas, protocolos institucionais, sistemas de gestão utilizados em outros estados e dados obtidos por observação do funcionamento interno do ODIN, buscando identificar lacunas operacionais, tecnológicas e procedimentais. A análise evidenciou limitações que podem comprometer a integridade, a rastreabilidade e a consistência dos registros digitais. A comparação com sistemas estaduais revelou práticas que podem orientar melhorias na infraestrutura goiana. Com base no diagnóstico construído, o estudo propõe medidas de padronização procedimental, aperfeiçoamento do ODIN e qualificação contínua dos profissionais, reforçando a segurança jurídica e a confiabilidade da custódia digital.
Palavras-chave: Cadeia de Custódia; Vestígio Digital; Perícia Criminal; Gestão de Evidências.

Abstract: The chain of custody of digital evidence presents specific challenges arising from its volatility, susceptibility to alteration, and the absence of standardized national regulations establishing minimum requirements for its handling within the forensic context. This study examined the workflow for processing digital evidence in the Goiás Forensic Science Department (PCI/GO), focusing on digital traces derived from physical supports and on how they are recorded and managed in the ODIN System. A qualitative approach was adopted, combining bibliographic review and document analysis, structured according to the hypothetico-deductive method, through which the lack of standardized procedures for digital custody within the institution was investigated. Regulations, institutional protocols, management systems used in other states, and data obtained through observation of ODIN's internal operation were analyzed to identify operational, technological, and procedural gaps. The analysis revealed limitations that may compromise the integrity, traceability, and consistency of digital records. The comparison with systems adopted in other states highlighted practices that may guide improvements to Goiás's infrastructure. Based on this diagnostic assessment, the study proposes measures for

[1] Perita Criminal da Polícia Científica de Goiás. E-mail: stephannyr@gmail.com

[2] Mestra em Engenharia de Produção pela Universidade Federal de Goiás. Perita Criminal e Coordenadora Geral de Controle de Custódia da Polícia Científica do Estado de Goiás.

procedural standardization, enhancement of the ODIN system, and continuous professional training, thereby strengthening legal reliability and the trustworthiness of the digital chain of custody.
Keywords: Chain of Custody; Digital Evidence; Forensic Science; Evidence Management.

1. INTRODUÇÃO

No processo penal, a prova exerce papel fundamental, pois, além de possibilitar a reconstrução dos fatos ou a demonstração dos acontecimentos alegados, constitui elemento de convicção para o magistrado, que a utilizará como fundamento de sua decisão (Pacelli, 2020). A Lei n. 13.964/2019, conhecida como Pacote Anticrime, representou um avanço ao inserir, de forma explícita, a cadeia de custódia de vestígios no Código de Processo Penal brasileiro (CPP) (Borri; Soares, 2020; Giacomolli; Amaral, 2020), suprindo uma lacuna que se limitava a uma construção doutrinária e jurisprudencial (Giacomolli; Amaral, 2020; Chacon; Siqueira, 2025).

Mesmo antes de constar expressamente no CPP, a Secretaria Nacional de Segurança Pública (SENASP), vinculada ao Ministério da Justiça e Segurança Pública (MJSP), já buscava orientar as instituições de segurança pública, por meio de cursos de capacitação, manuais técnicos e Procedimentos Operacionais Padrão (POPs), quanto à aplicação da cadeia de custódia. Ademais, o tema foi objeto da Portaria SENASP n. 82/2014, que estabeleceu regras obrigatórias para a Força Nacional de Segurança Pública e de caráter recomendatório para as demais organizações policiais do país (Umbelino, 2024).

Ressalta-se que a cadeia de custódia é considerada a espinha dorsal da prova pericial e pode ser definida como um conjunto de procedimentos documentados voltados a assegurar a integridade, autenticidade e rastreabilidade da prova penal desde sua coleta até sua apresentação em juízo (Badaró, 2017; Badaró Massena, 2023; Lopes Júnior, 2019). Trata-se, portanto, de um instrumento que contribui para a garantia da imparcialidade e transparência do processo penal (Zaffaroni, 2021). De acordo com o CPP, essa documentação deve acompanhar todas as dez etapas previstas em seu art. 158-A, a saber, reconhecimento, isolamento, fixação, coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte (Brasil, 2021).

Nesse contexto, a prova digital, em contraste com as chamadas provas analógicas, apresenta características singulares. Por não estar necessariamente vinculada a um suporte físico, mostra-se mais frágil, volátil e suscetível a alterações ou perdas, sejam estas voluntárias ou acidentais (Badaró, 2021; Badaró Massena, 2023; Torres, 2022). Tal condição impõe desafios ainda mais complexos no que tange à preservação da cadeia de custódia desse tipo de vestígio, de forma a garantir sua legitimidade e aplicação na esfera penal (Chacon; Siqueira, 2025).

É importante ressaltar que as provas materiais, por existirem de forma autônoma e externa ao processo, também necessitam ser incorporadas aos autos processuais por meio de instrumentos probatórios adequados, como documentos, laudos periciais ou inspeções realizadas em juízo (Silva; Lopes, 2025).

Assim, a prova digital engloba tanto fatos nascidos no mundo virtual quanto aqueles registrados ou documentados por ferramentas digitais. Para tanto, muitas vezes é necessário que esses elementos migrem do campo físico para o digital, por meio de registros como fotografias, digitalizações ou laudos eletrônicos, a fim de possibilitar sua tramitação processual. Em síntese, ao analisarmos o cenário atual em que as provas e documentos probatórios digitais assumem papel de destaque no judiciário, fica evidenciada a necessidade do fortalecimento dos mecanismos de controle e validação dessas evidências (Silva; Lopes, 2025; Vaz, 2023; Chacon; Siqueira, 2025).

Embora o CPP apresente a descrição de todos os passos referentes à preservação da cadeia de custódia, o foco principal aplica-se às evidências físicas, deixando uma lacuna legal no que tange ao vestígio digital (Furlaneto Neto; Santos, 2020; Parodi, 2020). Sua efetividade, portanto, depende da elaboração de protocolos específicos voltados à coleta, preservação e análise de dados digitais, capazes de atender às particularidades desse tipo de evidência (Furlaneto Neto; Santos, 2020). Esse cenário demonstra a complexidade do tema, marcada não apenas pela limitada produção doutrinária, mas também pela inexistência de uma sistematização normativa (Capanema, 2025).

As pesquisas evidenciam que ainda não há consenso internacional quanto a diretrizes unificadas, tampouco padronização nos procedimentos relacionados à custódia digital, o que aumenta sua vulnerabilidade à adulteração e ao questionamento judicial (Badaró, 2021, 2023; D’Anna et al., 2023; Giacomolli; Eilberg, 2023; Parodi, 2020; Steffen, 2025). No contexto brasileiro, o cenário não é diferente, a falta de normativas e as fragilidades de ordem operacional expõem os dados digitais a maior vulnerabilidade jurídica (Badaró, 2021, 2023; Silva; Lopes, 2025).

No Estado de Goiás, a cadeia de custódia foi normatizada por meio da Portaria n. 325/2022 da Secretaria de Estado da Segurança Pública (SSP), reforçando a necessidade de regulamentar procedimentos de preservação da prova (Goiás, 2022). Nesse ínterim, a Polícia Científica de Goiás (PCI/GO) processa milhares de documentos e vestígios periciais em formato

digital mensalmente, incluindo dispositivos móveis, computadores, mídias de armazenamento e documentos eletrônicos. Isso reforça a necessidade de maior padronização procedimental e de protocolos específicos voltados ao ambiente digital, a fim de assegurar a segurança jurídica das investigações e mitigar eventuais contestações quanto à validade das provas (Badaró, 2021, 2023; Steffen, 2025; Vaz, 2023).

Diante desse cenário, o objetivo geral deste estudo consiste em propor o aprimoramento da cadeia de custódia de vestígios digitais da PCI/GO, por meio da definição de diretrizes que padronizem e qualifiquem os procedimentos relacionados ao tratamento de vestígios digitais e digitalizados, assegurando sua autenticidade, integridade e validade jurídica. Para atingir esse propósito, o trabalho estabeleceu objetivos específicos voltados a mapear o fluxo de evidências na PCI/GO, com ênfase nos vestígios digitais derivados de suportes físicos, bem como identificar as boas práticas adotadas por órgãos periciais nacionais nesse domínio. A investigação envolveu o exame do funcionamento do Sistema ODIN, revisão bibliográfica e a análise documental de normativas, protocolos e experiências consolidadas, permitindo identificar lacunas operacionais, tecnológicas e procedimentais. Esse diagnóstico fundamentou a proposição de medidas de padronização e de aperfeiçoamento do sistema, contribuindo para o fortalecimento da segurança jurídica e da confiabilidade da custódia digital no âmbito da PCI/GO.

2. REVISÃO DA LITERATURA

2.1. Ferramentas aplicáveis à gestão de vestígios digitais

A prova digital, devido às suas características específicas, não se adapta com facilidade às práticas tradicionais de produção e tratamento de evidências próprias do ambiente físico. Embora existam diversas diretrizes e boas práticas internacionais amplamente reconhecidas na literatura especializada (Badaró, 2017; 2021; 2023), ainda não há um padrão único universalmente adotado, tampouco uma regulamentação nacional vinculante que estabeleça parâmetros mínimos para o tratamento desses vestígios no âmbito pericial brasileiro. Nesse cenário, organizações internacionais ocupam papel central na formulação de recomendações técnicas para identificação, coleta, preservação e análise de vestígios digitais, conforme sintetizado no Quadro 1.

Quadro 1 – Principais referências internacionais aplicáveis à gestão de evidências digitais

Instituição / Norma	Descrição
ISO/IEC 27037:2013	Estabelece diretrizes para identificação, coleta, aquisição e preservação de evidências digitais, servindo de base para o Procedimento Operacional Padrão da SENASP.
NIST – *National Institute of Standards and Technology*	Produz guias e recomendações técnicas, incluindo diretrizes para perícia em dispositivos móveis e estudos sobre gerenciamento de evidências.
SWGDE – *Scientific Working Group on Digital Evidence*	Elabora orientações de boas práticas para coleta, preservação, manuseio e aquisição de dados provenientes de dispositivos eletrônicos.
INTERPOL	Disponibiliza orientações internacionais para laboratórios de perícia digital e procedimentos de busca e apreensão de evidências eletrônicas, incluindo drones e consoles de jogos.

Fonte: Elaborado pelos autores (2025).

A preservação da integridade dos dados digitais é um requisito fundamental para assegurar a confiabilidade da prova. Nesse contexto, os algoritmos de integridade (funções *hash*) desempenham um importante papel, pois convertem dados de qualquer tamanho em valores de comprimento fixo, funcionando como identificadores únicos que representam o estado do arquivo no momento do cálculo (Brasil, 2023; Steffen, 2025). O uso de funções *hash* consolidou-se como uma das práticas mais amplamente adotadas no ambiente pericial, uma vez que permite verificar, de maneira objetiva e verificável, se determinado conteúdo permaneceu inalterado ao longo de seu ciclo de custódia.

Nesse sentido, o Procedimento Operacional Padrão da SENASP, por exemplo, recomenda a utilização do algoritmo SHA-512 para a verificação futura de possíveis alterações em dados armazenados (Brasil, 2013), enquanto o NIST IR 8387 indica os algoritmos SHA-256, MD5 e SHA-1 para finalidades específicas de análise forense (Guttman; White; Walraven, 2022). Entretanto, é imprescindível reconhecer que as funções de *hash* apresentam limitações intrínsecas: elas apenas atestam a integridade do dado a partir do instante em que o código foi gerado, não sendo capazes de identificar modificações ocorridas previamente (D'Anna et al., 2023; Guttman; White; Walraven, 2022; Steffen, 2025).

Para mitigar essas fragilidades, alguns autores propõem o uso de técnicas mais avançadas, entre as quais se destaca a *blockchain*, que oferece propriedades como imutabilidade, descentralização, transparência, rastreabilidade, auditabilidade e elevada confiabilidade. Essas características permitem a criação de um registro cronológico de vestígios que é, por natureza, resistente a adulterações, apresentando-se como alternativa promissora para fortalecer a cadeia de

custódia digital (Elgohary et al., 2022; Jaquet-Chiffelle; Casey; Bourquenoud, 2020; Khanji et al., 2022; Steffen, 2025). Apesar de seu grande potencial, a implementação de *blockchain* na cadeia de custódia não está isenta de desafios e críticas. Sua adoção impõe custos significativos, maior complexidade operacional e tempo elevado para sincronização e validação de blocos, especialmente quando novos nós, ou seja, participantes, são inseridos (Guttman; White; Walraven, 2022).

Outra ferramenta discutida pela literatura é o *fuzzy hashing* (ou *hashing* aproximado), uma técnica criptográfica projetada para superar as limitações do *hashing* tradicional, sendo capaz de identificar graus de similaridade entre arquivos. Seu principal propósito é lidar com incertezas decorrentes de alterações benignas ou maliciosas em conteúdos digitais, permitindo comparações mesmo quando os artefatos sofreram modificações, sem comprometer a rastreabilidade (Ali et al., 2022; Elgohary et al., 2022). Essa abordagem, contudo, apresenta limitações relevantes: é vulnerável a ataques antiforenses, nos quais o atacante pode modificar um arquivo para que o *fuzzy hashing* deixe de reconhecê-lo como correspondência de um artefato malicioso (*blacklisted*) ou, ao contrário, manipular um arquivo malicioso para que seu *hash* se aproxime do de um arquivo confiável (*whitelisted*). Além disso, possui maior probabilidade de falsos positivos e é incapaz de realizar comparações semânticas entre arquivos idênticos armazenados em formatos distintos. (Elgohary et al., 2022).

O quadro seguir sistematiza as principais ferramentas empregadas na integridade e autenticidade de vestígios digitais.

Quadro 2 – Tecnologias aplicáveis à cadeia de custódia digital

Ferramenta	**Objetivos**	**Vantagens**	**Limitações**	**Adequação à Cadeia de Custódia**
Hashing Tradicional (SHA-512, SHA-256, e outros)	Verificar se os dados foram alterados após a geração do Código.	- Amplamente aceito no meio jurídico; - Rápido e simples; - Alta confiabilidade para integridade no momento da coleta.	- Não registra histórico; - Não detecta alterações anteriores ao cálculo; - Depende de documentação complementar.	Essencial, mas insuficiente isoladamente. Comum nas práticas periciais atuais.
Blockchain	Registrar de forma imutável e auditável todas as operações realizadas sobre a evidência.	- Registro cronológico imutável; - Alta rastreabilidade e transparência; - Elevada resistência a adulterações; - Auditabilidade por múltiplos atores.	- Alto custo e complexidade; - Infraestrutura especializada; - Tempo elevado de sincronização e validação.	Muito alta. Potencializa a cadeia de custódia, mas exige recursos e maturidade institucional.

Fuzzy Hashing	Identificar similaridade entre arquivos mesmo após modificações.	- Útil para análise de versões modificadas; - Detecta alterações sutis; - Auxilia investigações em cenários dinâmicos.	- Vulnerável a falsos positivos; - Suscetível a ataques antiforenses; - Não garante integridade estrita; - Não compara bem arquivos iguais em formatos diferentes.	Baixa. Ferramenta complementar para investigação. Não adequada como mecanismo de integridade jurídica.

Fonte: Elaborado pelos autores (2025).

2.2. As normativas brasileiras e a cadeia de custódia de vestígios digitais

Embora existam inúmeras ferramentas para a gestão de vestígios digitais, a incorporação dessas soluções enfrenta barreiras de ordem técnica, normativa e institucional. Além da ausência de regulamentação específica, verifica-se no Brasil uma lacuna doutrinária e a falta de consenso sobre diretrizes uniformes aplicáveis às Polícias Científicas (Capanema, 2025; D'Anna et al., 2023). Isso gera disparidades na condução de procedimentos e pode prejudicar a credibilidade da prova digital em juízo (Badaró, 2017; Badaró M., 2023; Menezes et al., 2018). Nesse ínterim, observa-se que algumas instituições públicas têm se mobilizado para suprir tais demandas, buscando estruturar práticas mais robustas e tecnicamente fundamentadas no tratamento de vestígios, especialmente os digitais.

Um exemplo significativo é a atuação da SENASP/MJSP, que designou, por meio da Portaria n. 282/2021, servidores da segurança pública para integrar Câmaras Técnicas distribuídas em 13 grupos estratégicos, organizados conforme suas áreas de atuação, resultando na publicação de um compilado de relatórios técnicos finais, reunindo estudos e orientações relevantes sobre o tema, a exemplo do Relatório da Câmara Técnica de Vestígios Digitais da SENASP.

O documento destaca que o vestígio digital está presente em praticamente todas as áreas forenses e que, em razão das suas particularidades, como volatilidade, vulnerabilidade a alterações e dependência de suportes e sistemas específicos, a gestão de sua cadeia de custódia demanda procedimentos próprios (Brasil, 2023). Além disso, descreve os problemas críticos identificados em níveis operacional, tático e estratégico que afetam a correta aplicação da cadeia de custódia para vestígios digitais, conforme sintetizado no quadro 3 a seguir.

Quadro 3 – Fatores que comprometem a cadeia de custódia de vestígios digitais

Nível	Problemas identificados
Operacional	- Dificuldades na manutenção constante de suprimentos básicos (etiquetas, lacres, envelopes); - Falta de envolvimento de órgãos externos à perícia nos procedimentos de cadeia de custódia; - Manipulação inadequada dos vestígios por agentes sem conhecimento técnico; - Ausência de mecanismos para efetivar o descarte de vestígios; - Falta de procedimentos padronizados para gestão de registros audiovisuais gerados durante exames periciais.
Tático	- Dificuldade de compreensão de procedimentos informáticos técnicos pelo público leigo; - Apreensões frequentes de versões modificadas de arquivos multimídia (comprimidos por aplicativos de mensageria); - Riscos de perda de conteúdo durante operações de busca e apreensão pela sensibilidade dos vestígios digitais; - Aplicação inadequada dos procedimentos em unidades descentralizadas devido à falta de ferramental, mão de obra e infraestrutura.
Estratégico	- Ausência de um sistema básico de gestão da cadeia de custódia que viabilize o registro completo das etapas e o rastreamento integral dos vestígios; - Ausência de alinhamento institucional para políticas de descarte; - Falta de critérios para armazenamento que equilibrem volume e condições de processamento; - Deficiência na conscientização do Judiciário, Ministério Público e Defensoria Pública sobre a necessidade de preservação de vestígios digitais; - Sistemas judiciários que tratam arquivos multimídia como documentos comuns, provocando perda de metadados e alterações de formato.

Fonte: Brasil, 2023.

O relatório da Câmara Técnica também buscou relacionar as etapas da cadeia de custódia, previstas no CPP), com os requisitos específicos aplicáveis às evidências digitais.

Quadro 4 – Etapas da cadeia de custódia e sua aplicação aos vestígios digitais

Etapa	Prática
Reconhecimento	Consiste em identificar suportes ou fontes de dados relevantes.
Isolamento	Envolve preservar não só o dispositivo, mas também seu conteúdo lógico, evitando perdas de dados voláteis ou acessos remotos.
Fixação	Requer descrição detalhada dos itens ou dados coletados, podendo incluir registros fotográficos ou a identificação por meio de *hashes* quando não houver suporte físico.
Coleta	Compreende tanto a apreensão dos dispositivos quanto a aquisição direta dos dados, priorizando a preservação da integridade física e lógica.
Acondicionamento	Deve proteger os materiais contra impactos, campos magnéticos e conexões de rede.
Transporte	Exige medidas que preservem suas características.
Recebimento	Deve ser formalizado em sistema de gestão.

Processamento	Realizado exclusivamente mediante técnicas forenses que assegurem integridade, auditabilidade e repetibilidade/reprodutibilidade, em conformidade com a ABNT NBR ISO/IEC 27037 e infraestrutura apropriada.
Armazenamento	Pode ser físico, digital ou híbrido, desde que garanta integridade e rastreabilidade.
Descarte	Envolve a destinação adequada dos materiais, seja destruindo o suporte, apagando dados ou restituindo ao proprietário, conforme o caso.

Fonte: Brasil, 2023.

Por fim, o documento propõe a implantação de uma central de custódia dotada de infraestrutura robusta, segura e padronizada, além da adoção de um modelo híbrido de armazenamento, combinando preservação digital e manutenção física do suporte sempre que a custódia totalmente digital se mostrar tecnicamente ou operacionalmente inviável (Brasil, 2023).

De forma convergente, outras instituições federais, como a Polícia Federal e o Ministério Público Federal, também vêm adotando iniciativas estruturantes nesse domínio, demonstrando um esforço mais amplo de profissionalização e padronização das práticas periciais relacionadas a vestígios digitais.

No âmbito da Polícia Federal, existem procedimentos padronizados quanto às etapas da cadeia de custódia de vestígios digitais, reforçando a preservação prioritária dos dados em sua forma e suporte originais, além do registro das ações com detalhamento técnico e *hashes* de integridade. Além disso, é prevista a regulamentação complementar sobre segurança de dados, *backup* e uso de nuvem, evidenciando o compromisso institucional com o tema (Brasil, 2025).

Por sua vez, em 2020 o Ministério Público Federal (MPF) emitiu o guia prático denominado “Orientações para a Preservação da Cadeia de Custódia de Vestígios Digitais”, voltado à preservação da integridade e rastreabilidade desse tipo de vestígio no âmbito institucional, com diretrizes quanto ao registro rigoroso de dados fornecidos por provedores de serviços ou obtidos em ambiente de computação em nuvem (Brasil, 2020). Outras recomendações do guia incluem a necessidade de minimizar o manuseio dos dispositivos, realizar o cálculo de *hash* para assegurar a integridade e autenticidade dos dados e exigir dos provedores a disponibilização desses identificadores (Brasil, 2020).

Paralelamente, no âmbito legislativo, observa-se um movimento convergente de fortalecimento normativo. O Projeto de Lei n. 4.939/2020 foi proposto com o objetivo de padronizar e regulamentar os procedimentos relacionados à cadeia de custódia da prova digital. Ele estabelece regras específicas para a obtenção e admissibilidade de provas digitais, exigindo

metadados e registro do tratamento da evidência. Além disso, determina que a coleta seja feita por perito oficial ou assistente técnico, com espelhamento em duas cópias e preservação imediata da integridade dos dados, priorizando a cópia forense à apreensão física de dispositivos. O documento também regulamenta formas especiais de coleta, como a remota, oculta e forçada, além da infiltração virtual, e prevê a separação de dados pessoais sensíveis em autos próprios, buscando suprir lacunas legais sobre armazenamento e gestão da prova digital (Brasil, 2020).

3. MÉTODO DE PESQUISA

O método pode ser compreendido como o conjunto de etapas sistemáticas e racionais que orienta a produção de informações confiáveis e pertinentes. Seu propósito é definir o percurso investigativo, identificar eventuais falhas no processo e sustentar, de maneira lógica, as proposições do pesquisador. Entre os métodos de raciocínio científico, destaca-se o hipotético-dedutivo, que parte da identificação de um problema e formula hipóteses provisórias a serem testadas e questionadas, em busca de refutar inconsistências. O processo é cíclico, pois a cada verificação surgem novas hipóteses e indagações. Tal método baseia-se, portanto, na observação criteriosa de um fenômeno e na formulação de explicações passíveis de contestação, possibilitando a produção de novos conhecimentos (Marconi; Lakatos, 2017). Com base nessa perspectiva, esta pesquisa tomou como problema a ausência de fluxos padronizados para a cadeia de custódia digital na Polícia Científica de Goiás, levantando hipóteses relacionadas à adaptação ou implantação de ferramentas já descritas na literatura e aplicadas em experiências nacionais e internacionais, de forma a aprimorar o gerenciamento de vestígios digitais na instituição.

Quanto à sua natureza, a literatura classifica as pesquisas em dois grandes grupos: a básica, voltada à ampliação do conhecimento científico sem preocupação imediata com a aplicação prática, e a aplicada, destinada à geração de soluções direcionadas a problemas específicos (Gil, 2017). Este estudo se inseriu no segundo grupo, pois seu resultado esperado não se limitou ao aprofundamento teórico do debate, mas incluiu a proposição de diretrizes e modelos de fluxo aplicáveis à rotina institucional, assegurando maior confiabilidade jurídica às provas digitais e fortalecendo o processo penal.

Em relação aos objetivos, as pesquisas podem ser exploratórias, quando têm como meta proporcionar maior familiaridade com um problema, ou descritivas, quando buscam detalhar e

caracterizar fenômenos observados (Gil, 2017). O presente trabalho conjugou ambas as finalidades: foi exploratório, ao ampliar o conhecimento sobre a problemática, identificar lacunas normativas e mapear experiências bem-sucedidas em outros contextos (Gil, 2002), e foi descritivo, na medida em que registrou e analisou práticas e normativas já existentes, sistematizando informações sobre fluxos, ferramentas e protocolos utilizados em diferentes instituições periciais brasileiras. Essa dupla classificação justificou-se pela complexidade do objeto, que demandou tanto o mapeamento inicial do campo quanto a descrição aprofundada das práticas em vigor.

A abordagem adotada foi qualitativa, uma vez que privilegiou a interpretação crítica dos documentos e textos examinados, promovendo a compreensão de processos, fluxos e práticas institucionais. Essa estratégia permitiu acompanhar como as atividades se desenvolveram até sua etapa final, priorizando a avaliação do contexto e da complexidade envolvida (Cauchick-Miguel, 2018). O tratamento dos dados foi feito por meio da técnica de análise de conteúdo, que possibilitou organizar o material em categorias temáticas, tais como: fundamentos legais da cadeia de custódia; protocolos existentes para provas digitais; ferramentas aplicáveis à rastreabilidade; práticas normativas estaduais; e propostas de padronização. Essa categorização permitiu confrontar a teoria com a realidade normativa e operacional, evidenciando convergências, lacunas e potenciais soluções (Cauchick-Miguel, 2018).

No tocante às técnicas de pesquisa, foram utilizadas a revisão bibliográfica e a análise documental. A primeira permitiu apresentar os marcos normativos e conceituais, examinando o problema com base em material já publicado em um arcabouço teórico sólido, como livros, artigos científicos, teses, dissertações e relatórios técnicos, proporcionando bases teóricas e discussões atualizadas sobre cadeia de custódia digital e ferramentas tecnológicas correlatas (Marconi; Lakatos, 2017). Nesse sentido, foram analisadas obras clássicas do processo penal e manuais de direito, bem como artigos recentes nacionais e internacionais que discutiram os desafios da custódia de provas digitais e as ferramentas emergentes aplicadas ao tema. A pesquisa bibliográfica foi conduzida em bases acadêmicas como Scielo, *Google Scholar*, Periódicos CAPES e repositórios institucionais, garantindo amplitude e diversidade na coleta das informações.

De forma complementar, o estudo adotou a dimensão documental, recorrendo a fontes primárias que ainda não haviam recebido tratamento científico (Marconi; Lakatos, 2017). Foram

examinadas leis, regulamentos, portarias federais e estaduais, documentos institucionais e Procedimentos Operacionais Padrão (POPs), incluindo normativas da SSP/GO e da SENASP. Também foram analisadas publicações institucionais disponíveis em sites oficiais de Polícias Científicas de diversos estados, as quais forneceram informações relevantes sobre o desenvolvimento e uso de sistemas voltados ao gerenciamento de vestígios digitais e à cadeia de custódia.

Além dessas fontes institucionais, foram realizadas buscas sistemáticas no Portal Nacional de Contratações Públicas (PNCP), com o objetivo de identificar processos de aquisição de *softwares*, plataformas e dispositivos tecnológicos relacionados ao tema da cadeia de custódia digital. As buscas foram conduzidas mediante o uso das seguintes palavras-chave: cadeia de custódia, vestígio digital, vestígio virtual, sistema de gerenciamento de perícia, câmeras corporais, sistema de criminalística e sistema forense. Esses levantamentos possibilitaram mapear tendências tecnológicas contratadas por órgãos de segurança pública, bem como identificar ferramentas efetivamente empregadas em diferentes estados brasileiros.

A integração dessas diversas fontes científicas, normativas, documentais e institucionais, aliada à observação participante, permitiu compreender de forma ampla e comparativa como diferentes Polícias Científicas vêm estruturando seus fluxos digitais, adotando sistemas de informação e regulamentando a cadeia de custódia de vestígios digitais. Tal levantamento subsidiou a análise crítica das práticas existentes e contribuiu para a identificação de lacunas e oportunidades de aprimoramento.

4. RESULTADOS E DISCUSSÕES

4.1. Panorama das Polícias Científicas quanto à Gestão de Evidências Digitais

O panorama nacional da gestão de evidências digitais é marcado pela busca por padronização procedimental e pelo desenvolvimento e adoção de sistemas informatizados robustos, essenciais para garantir que a prova seja tratada com o devido rigor técnico-científico. Nesse contexto, a Polícia Científica do Estado de São Paulo desenvolveu o Sistema Gestor de Laudos (GDL), que reúne funcionalidades automatizadas para otimizar o trabalho pericial, reduzir esforço manual e minimizar erros. O Módulo Escritório permite redigir laudos

diretamente no sistema, criando e reutilizando modelos e rascunhos. Já os Módulos de Entorpecentes e Vistoria geram laudos automaticamente a partir das informações da requisição. O GDL também registra todo o histórico de alterações feitas em cada vestígio, indicando autor e data da modificação, o que garante rastreabilidade e fortalece a cadeia de custódia (São Paulo, 2019; 2023).

O estado do Paraná tem se destacado pela gestão de seus sistemas periciais e pela infraestrutura física da custódia. Após receber, da Polícia Científica de São Paulo, o código-fonte original do GDL, em 2013, a Polícia Científica do Paraná (PCI/PR) desenvolveu uma versão customizada que se tornou um dos melhores sistemas de gestão de laudos do país, incorporando funcionalidades como assinatura digital, anexos eletrônicos para computação forense e emissão de laudos automáticos. O sistema transformou a gestão da instituição, proporcionando economicidade ao eliminar o uso de papel, tornando o fluxo totalmente digital e centralizado em todo o estado, além de acelerar a tramitação dos laudos (Paraná, 2014). A PCI/PR está trabalhando em projetos para integrar o GDL com outros sistemas estaduais, como os da Polícia Civil, Polícia Militar e TJPR (Paraná, 2023). Embora a instituição não disponha de uma central de custódia digital para armazenamento, a contraprova consiste na própria mídia mantida fisicamente na Central de Custódia destinada a vestígios materiais. Essa central conta com procedimentos claramente definidos para a extração de dados, incluindo a abertura do lacre em ambiente monitorado por câmeras, garantindo o devido registro de todo o processo (Brasil, 2023).

O Ceará, por sua vez, destaca-se pela criação do aplicativo Galileu, desenvolvido pela Perícia Forense do Estado do Ceará (Pefoce) em 2019. A ferramenta foi um dos destaques nacionais na 1ª Exposição On-line de Boas Práticas Tecnológicas da SENASP. O Galileu integra todas as etapas do trabalho pericial, desde a coleta de dados no local do crime até a elaboração do laudo, abrangendo tanto atividades operacionais quanto administrativas. Entre suas funcionalidades, destaca-se o rastreamento completo dos vestígios ao longo da cadeia de custódia e a agilização da produção dos laudos, graças à automação de processos e ao registro de informações em tempo real. O sistema permite ainda coletar dados, capturar imagens, gravar áudio e gerar o laudo no final do procedimento, viabilizando, por exemplo, que o perito registre fotografias de impressões papilares e as envie direto do local de crime para o banco de dados da Pefoce (Brasil, 2023; Ceará, 2024).

O estado de Alagoas desenvolveu o *software* Forensis, criado pela Chefia de Desenvolvimento de Programas de Informatização da SSP/AL e implantado em julho de 2021. O Forensis é um canal de comunicação totalmente digital que otimiza o tempo das forças policiais e possibilita a solicitação de exames periciais e o envio de laudos para as instituições do sistema de persecução penal. Ele cria um canal direto de comunicação entre a Perícia e as delegacias, permitindo o acesso em tempo real às solicitações e laudos (Xavier, 2024). O sistema utiliza boas práticas de segurança da informação e consistência de dados, incluindo a implementação de um registro histórico de acesso para controle de segurança (Teodósio, 2021; Xavier, 2024). O *software* exige a autenticação física da entrega e recebimento de material no mundo real por meio da senha do usuário destino, documentando a movimentação do vestígio (Alagoas, [s.d], p. 15).

No Piauí, o DRIVE.PI foi criado como repositório oficial da Polícia Científica para armazenar e compartilhar vestígios digitais com segurança, garantindo integridade, rastreabilidade e controle de acesso (Piauí, 2025b). Operado pela Central de Custódia de Vestígios (CCV), o sistema exige credenciais institucionais, mantém registros centralizados de operações e organiza os dados por unidades periciais. Todo material digital deve ser inserido na pasta da demanda, sendo recomendado o uso do *Nextcloud* para grandes volumes. O compartilhamento é restrito a usuários autorizados, sem links públicos, e deve ser mencionado nos laudos. A exclusão de arquivos só ocorre mediante solicitação formal à CCV. Órgãos externos precisam fornecer e-mail institucional para o recebimento de arquivos e, quando necessário, realizar cadastro prévio. Os acessos concedidos expiram em 60 dias (Piauí, 2025a).

Por fim, o Espírito Santo ganhou destaque por meio do Perito Oficial Rafael Pereira de Souza, responsável por liderar o desenvolvimento e a implantação do Gestor de Criminalística, Identificação Humana e Medicina Legal (GCRIM), solução integrada da plataforma Sinesp (Espírito Santo, 2025). O sistema foi concebido com base nas melhores práticas adotadas por ferramentas consolidadas em outros estados, como o Forensis (Alagoas), o GDL e o Galileu (Ceará) (Alagoas, 2025). O GCRIM representa um avanço significativo para a padronização e o fortalecimento da gestão da cadeia de custódia, garantindo maior segurança e transparência na tramitação de procedimentos periciais. A ferramenta permitirá o rastreamento em tempo real de todo o percurso dos materiais coletados, eliminando a necessidade de comprovantes em papel. Cada entrega será acompanhada de confirmação enviada por e-mail, assinada digitalmente pelas partes e certificada eletronicamente. Alagoas também contribuiu com a experiência do Forensis

para o desenvolvimento dessa solução nacional, sendo selecionado, juntamente ao Espírito Santo, para conduzir o projeto-piloto do GCRIM. Após essa fase, o sistema será disponibilizado aos demais órgãos periciais (Alagoas, 2025; Espírito Santo, 2025).

Além das soluções mencionadas, alguns estados brasileiros também têm incorporado tecnologias de registro audiovisual por meio de câmeras corporais voltadas ao policiamento ostensivo. Elas introduzem recursos estruturados de documentação automática, como gravação contínua, transcrição automática, registro georreferenciado, transmissão em tempo real e autenticação integrada a plataformas de gerenciamento de evidências digitais. Embora não estejam direcionadas ao contexto pericial, essas tecnologias exercem impacto indireto, pois permitem registrar de forma imediata e fidedigna as condições encontradas pelos primeiros respondentes na cena, contribuindo para a preservação do estado inicial dos fatos e reforçando etapas essenciais da cadeia de custódia, como a fixação, a documentação e a rastreabilidade das circunstâncias do atendimento policial (Leite; Acayaba, 2025; Paraná, 2025). As boas práticas identificadas nacionalmente estão resumidas no quadro 5.

Quadro 5 – Boas práticas de gestão da cadeia de custódia no Brasil

Instituição	**Prática**	**Características principais relacionadas à cadeia de custódia**
Polícia Científica do Estado de São Paulo (SP)	Criação do Sistema Gestor de Laudos (GDL)	- Automatização de processos periciais; - Módulo Escritório para criação e reutilização de laudos e modelo; - Módulos de Entorpecentes e Vistoria com geração automática de laudos; - Registro completo do histórico de alterações em vestígios (quem alterou e quando); - Alta rastreabilidade e controle das etapas da cadeia de custódia.
Polícia Científica do Paraná (PCI/PR)	Adaptação do GDL – versão customizada	- Assinatura digital e anexos eletrônicos para computação forense; - Emissão automática de laudos e fluxo totalmente digital; - Gestão centralizada e integração planejada com sistemas estaduais (PC, PM, TJPR); - Custódia física estruturada para mídias e vestígios materiais, com extração registrada em ambiente monitorado por câmeras.
Perícia Forense do Estado do Ceará (Pefoce)	Desenvolvimento do Sistema Galileu	- Rastreamento completo dos vestígios ao longo da cadeia de custódia; - Registro de informações em tempo real; - Automação na criação de laudos e integração com a Polícia Civil; - Coleta de dados, fotografia e gravação de áudio dentro do sistema; - Agilidade e confiabilidade no fluxo criminalístico.
Secretaria de Segurança Pública de Alagoas (SSP/AL)	Desenvolvimento do Sistema Forensis	- Canal totalmente digital para solicitação e envio de laudos; - Acesso em tempo real a solicitações e relatórios; - Boas práticas de segurança da informação e consistência de dados; - Registro histórico de acessos para controle e auditoria; - Exige autenticação física da entrega/recebimento por senha do usuário destino (materialidade da cadeia de custódia).

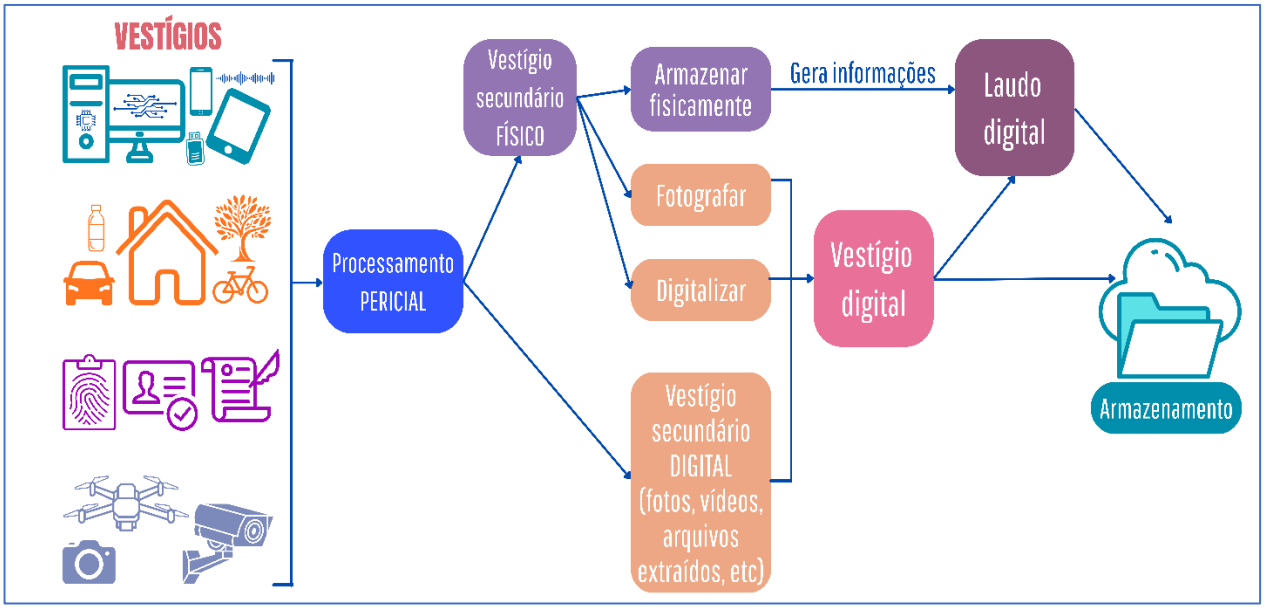
Instituição	Prática	Características principais relacionadas à cadeia de custódia
Polícia Científica do Piauí (PC-PI / DEPOC)	Utilização do DRIVE.PI (Piauí Box)	- Repositório digital para vestígios digitais com controle de integridade; - Acesso apenas com credenciais institucionais e registro centralizado de operações; - Organização por unidades periciais e setores técnicos; - Proibição de *links* públicos; compartilhamento apenas com usuários autorizados (acessos com prazo de 60 dias); - Necessidade de mencionar no laudo o armazenamento no repositório; - Exclusão de arquivos somente mediante solicitação formal.
Polícia Científica do Espírito Santo (ES)	Desenvolvimento do GCRIM – Gestor de Criminalística, Identificação Humana e Medicina Legal (Sinesp)	- Rastreabilidade em tempo real de materiais coletados; - Padronização nacional do fluxo da cadeia de custódia; - Eliminação de comprovantes em papel, substituídos por confirmações digitais assinadas; - Segurança e transparência no trâmite pericial; - Projeto piloto nacional com ES e AL antes da implementação nacional.

Fonte: Elaborado pelos autores (2025).

4.2 O caminho percorrido pelo vestígio

Para propor melhorias na cadeia de custódia de vestígios digitais, é indispensável compreender previamente o caminho percorrido pelo vestígio até adquirir esse formato, nos casos em que deriva de um suporte físico, considerando cada etapa de transformação, registro e tratamento que antecede sua digitalização.

Figura 1 – Percurso do vestígio físico até a sua conversão digital



Fonte: Elaborado pelos autores (2025).

O fluxograma apresentado na Figura 1 ilustra a dinâmica operacional da perícia criminal, evidenciando que, ainda que a maioria dos vestígios seja inicialmente apresentada ao perito em suporte físico, tais como computadores, mídias de armazenamento, dispositivos eletrônicos, documentos, objetos diversos, veículos ou cenas de crime, grande parte desses elementos invariavelmente migra para o ambiente digital ao longo do processamento técnico-científico, de modo a possibilitar a análise forense.

Tal transição ocorre tanto por meio de procedimentos de extração e aquisição forense de dados quanto pela produção de registros documentais e de imagem, como fotografias, vídeos, arquivos digitais derivados de escaneamentos tridimensionais, medições georreferenciadas e o próprio laudo pericial, geralmente elaborado e armazenado em formato digital.

Esse processo transforma o vestígio físico em um vestígio digital secundário ou subproduto pericial digital, que passa a integrar o conjunto probatório, adquirindo valor jurídico e necessidade de preservação autônoma. Assim, não apenas os vestígios digitais armazenados em algum suporte, como discos rígidos ou telefones celulares, demandam tratamento especializado; mas também aqueles inicialmente físicos, cuja materialidade é capturada, analisada, representada ou ampliada por meios digitais, tornando-se igualmente sujeitos às regras de cadeia de custódia digital (Brasil, 2023).

Em síntese, a expansão do espectro digital na atividade pericial criminal evidencia que a cadeia de custódia digital não constitui uma exceção, mas sim uma extensão essencial da cadeia de custódia probatória moderna, devendo ser tratada como eixo estruturante da garantia da confiabilidade e legitimidade da prova técnico-científica.

4.3 Sistema ODIN e a Cadeia de Custódia Digital na Polícia Científica de Goiás (PCI/GO)

O Sistema de Informações de Criminalística – ODIN, implantado pela PCI/GO no segundo semestre de 2018, gerencia o fluxo pericial desde a requisição até a emissão do laudo, registrando formalmente todas as etapas da cadeia de custódia. Ele centraliza vestígios, exames, laudos e anexos digitais, no intuito de garantir a rastreabilidade e padronização dos processos (Goiás, 2018). Uma funcionalidade recentemente adotada foi o alerta sonoro para novas requisições criadas, o que reduz o risco de solicitações não serem recebidas prontamente. O sistema está em fase de integração com o PROJUDI, o que facilitará a tramitação direta de

documentos com o Poder Judiciário, preservando a cadeia de custódia digital. Em relação às Delegacias de Polícia, o Sistema ODIN permite a realização de requisições e o acompanhamento dessas demandas por meio do número do Registro de Atendimento Integrado (RAI), além de disponibilizar o *download* dos laudos periciais (Silva, 2018).

Um dos principais desafios identificados refere-se ao limite máximo de 7 MB para anexar arquivos individuais na plataforma (Silva, 2018), sem diretrizes padronizadas, pela instituição, para o tratamento ou a tramitação de arquivos volumosos. Essa restrição impacta diretamente o envio de fotografias periciais em alta resolução, vídeos e outros arquivos essenciais ao fluxo do trabalho. Outra dificuldade encontrada é a impossibilidade de realizar as extrações de dados e arquivos diretamente pelo ODIN.

Além disso, identificou-se uma limitação na comunicação entre as Delegacias de Polícia e a PCI/GO, uma vez que o sistema ainda não disponibiliza funcionalidades adicionais que permitam a troca de informações ou o envio de documentos diversos, incluindo cobranças judiciais. Diante dessa lacuna, torna-se necessária a utilização de sistemas auxiliares, como o Sistema Eletrônico de Informações (SEI), o que fragmenta o fluxo documental e compromete a centralização das informações no próprio ODIN.

4.4 Proposta de Aprimoramento da Cadeia de Custódia Digital em Goiás

A proposta de aprimoramento da cadeia de custódia de vestígios digitais na PCI/GO é apresentada como um conjunto estruturado de recomendações que se fundamentaram na análise do trajeto dos vestígios, no diagnóstico do Sistema ODIN, e na comparação com modelos consolidados utilizados por outras Polícias Científicas do país.

Para tanto, recomenda-se a elaboração de uma regulamentação específica voltada à custódia de evidências digitais, estabelecendo requisitos técnicos, responsabilidades institucionais e procedimentos mínimos para todas as fases da custódia, como a identificação, coleta, extração, registro, armazenamento e descarte, em conformidade com padrões internacionais como ISO/IEC 27037, NIST e SWGDE. Além de orientar a prática profissional, essa regulamentação deve ser incorporada à própria cultura organizacional, garantindo uniformidade e continuidade na execução dos procedimentos.

Também se faz necessário instituir fluxos padronizados para vestígios digitais nativos, vestígios derivados de suportes físicos e vestígios híbridos, definindo de maneira clara os trâmites entre laboratórios e setores da instituição. Para assegurar a rastreabilidade e a integridade desses vestígios, sugere-se ainda a implantação de um registro documental completo e obrigatório de todas as etapas da cadeia de custódia, incluindo usuários envolvidos, horários, equipamentos utilizados e, quando aplicável, o cálculo de *hash*.

No que se refere aos registros realizados durante as perícias, recomenda-se, em um cenário ideal, que a instituição se prepare estruturalmente para a aquisição de tablets e para a adaptação do ODIN em formato de aplicativo, permitindo sua utilização diretamente em locais de crime. Assim como ocorre com o sistema Galileu, essa versão móvel possibilitaria ao perito coletar dados e realizar registros audiovisuais no próprio sistema, fortalecendo a integração e a rastreabilidade do fluxo pericial.

Como alternativa, propõe-se que todos os registros sejam obrigatoriamente realizados em dispositivos fornecidos pela instituição, acompanhados da criação de diretrizes que vedem a exclusão de fotografias ou quaisquer registros produzidos durante ou após a perícia, assegurando a confiabilidade, a rastreabilidade e a integridade desses elementos documentais. Ao retornar à base, o perito criminal deve efetuar o descarregamento integral dos arquivos em computadores institucionais, garantindo sua imediata incorporação ao fluxo da cadeia de custódia. Para viabilizar esse procedimento, é essencial que a instituição invista em infraestrutura apropriada, disponibilizando câmeras fotográficas e equipamentos audiovisuais, além de cartões de memória e soluções de armazenamento em nuvem, preferencialmente em repositório que seja exclusivo da PCI/GO, com backup redundante, de modo a assegurar a guarda segura e contínua dos registros produzidos.

No âmbito tecnológico, o Sistema ODIN requer aprimoramentos que assegurem maior eficiência e rastreabilidade no tratamento de vestígios digitais. Entre as medidas sugeridas, destaca-se a necessidade de ampliar o tamanho máximo permitido para anexos, atualmente limitado a 7 MB, ou, alternativamente, incorporar à plataforma mecanismos de compressão automática capazes de adequar arquivos volumosos a esse limite, preservando metadados e garantindo a integridade dos registros. Essa funcionalidade possibilitaria o envio seguro e rastreável de arquivos de grande porte diretamente pelo sistema, reduzindo a dependência de

soluções externas e reforçando a utilização exclusiva de soluções institucionais, o que fortalece a cadeia de custódia digital.

Outra melhoria sistêmica essencial consiste em restringir o uso do campo de anexos apenas à inclusão de documentos informativos, uma vez que esse ambiente registra apenas o usuário e o momento da inserção, sem possibilitar a rastreabilidade completa nem a formalização da troca de custódia. Nesse sentido, recomenda-se a implementação de uma ferramenta que permita a anexação de arquivos diretamente ao vestígio cadastrado, para os casos de vestígios digitais, vinculando automaticamente cada arquivo ao vestígio correspondente, ao usuário responsável, à data e ao setor de destino.

Para otimizar o fluxo interno entre peritos e laboratórios, sugere-se ainda a criação de um mecanismo que possibilite a migração, transferência, desmembramento ou cópia controlada de vestígios, físicos e digitais, entre diferentes Registros Gerais (RGs), preservando os metadados originais do vestígio “pai”. Tal funcionalidade reduziria inconsistências, como a anexação equivocada em RGs distintos e permitiria a análise concomitante em múltiplos laboratórios sem gerar duplicações desnecessárias e mantendo a integridade e a rastreabilidade da cadeia de custódia.

Recomenda-se, ainda a ampliação de funcionalidades do Sistema ODIN para facilitar a comunicação, o envio de cobranças e o compartilhamento de arquivos entre as Delegacias de Polícia e a PCI/GO, de modo a centralizar o fluxo informacional e evitar a fragmentação documental, duplicidades e inconsistências. Paralelamente, é fundamental fortalecer a integração com o Judiciário por meio do PROJUDI, cuja implementação já está em andamento, assegurando a tramitação eletrônica segura de laudos, anexos e mídias.

No aspecto operacional, é fundamental promover a capacitação contínua por meio de treinamentos regulares, de modo a incorporar à cultura organizacional a correta preservação da cadeia de custódia de vestígios digitais. Esses treinamentos devem abarcar o uso adequado do Sistema ODIN, a aplicação de técnicas de criptografia voltadas à garantia de integridade dos dados e as boas práticas de extração, assegurando que todos os profissionais envolvidos atuem de maneira adequada e tecnicamente alinhada.

A implementação coordenada dessas medidas resultará na padronização do fluxo da cadeia de custódia digital, no aumento da rastreabilidade e confiabilidade dos registros, na eliminação de práticas inseguras de transferência de arquivos, na redução de erros e

inconsistências documentais, culminando na integração efetiva e segura entre a PCI/GO, as Delegacias e o Judiciário.

5. CONSIDERAÇÕES FINAIS

A análise empreendida confirma que a cadeia de custódia digital impõe desafios significativamente distintos daqueles enfrentados no tratamento de vestígios físicos, exigindo procedimentos especializados, infraestrutura tecnológica compatível e normatização própria. No contexto da PCI/GO, o Sistema ODIN representa um avanço importante ao registrar formalmente etapas da cadeia de custódia; entretanto, persistem limitações estruturais e operacionais que afetam a integridade e a rastreabilidade dos vestígios digitais, tais como restrições de anexação, ausência de padronização para grandes volumes de dados, falhas na vinculação entre vestígios e arquivos e a necessidade de mecanismos seguros de migração entre registros.

A comparação com experiências de outros estados demonstra que a adoção de sistemas robustos e integrados contribui diretamente para a confiabilidade da custódia digital. Exemplos como GDL, Galileu, Forensis, DRIVE.PI e GCRIM evidenciam que soluções bem projetadas reduzem erros operacionais, fortalecem a auditoria e padronizam fluxos, servindo de referência aplicável à realidade goiana. Além disso, tecnologias externas ao ambiente pericial, como câmeras corporais vinculadas a plataformas de gerenciamento de evidências digitais, mostram que a rastreabilidade pode ser fortalecida desde a chegada dos primeiros respondentes.

Diante desse cenário, a proposta de aprimoramento apresentada reúne um conjunto de medidas essenciais para qualificar a cadeia de custódia digital na PCI/GO, contemplando a elaboração de regulamentação específica; a modernização do Sistema ODIN; a criação de funcionalidades voltadas à anexação e à migração segura de arquivos, bem como ao aprimoramento da comunicação e do compartilhamento documental com instituições externas; e a necessidade de capacitação contínua dos profissionais envolvidos. A implementação articulada dessas ações fortalece o tratamento dos vestígios digitais, amplia a segurança jurídica das provas e aproxima a instituição dos padrões nacionais e internacionais de excelência em gestão de evidências digitais.

REFERÊNCIAS

ALAGOAS. Polícia Científica. Instituto de Criminalística Perito Dely Ferreira da Silva. **FORENSIS – Apresentação do Sistema**. Versão 1.0. Maceió, AL, [s.d.]. Disponível em: <https://policiacientifica.al.gov.br/documentos/category/326-manuais>. Acesso em: 01 nov. 2025.

ALAGOAS. **Polícia Científica promove capacitação para nova ferramenta nacional de gestão de perícia: Plataforma GCRIM promete unificar e otimizar o gerenciamento da cadeia de custódia e a requisição de exames**. [S.l.]: Ascom Polícia Científica, 5 ago. 2025. Disponível em: <https://alagoas.al.gov.br/noticia/policia-cientifica-promove-capacitacao-para-nova-ferramenta-nacional-de-gestao-de-pericias>. Acesso em: 07 nov. 20025.

ALI, M.; ISMAIL, A.; ELGOHARY, H.; DARWISH, S.; MESBAH, S. ***A procedure for tracing chain of custody in digital image forensics: A paradigm based on grey hash and blockchain***. *Symmetry*, v. 14, 334, 2022. Disponível em: <https://doi.org/10.3390/sym14020334>. Acesso em: 10 out. 2025.

BADARÓ, G. **A cadeia de custódia e sua relevância para a prova penal**. *In:* Temas atuais da investigação preliminar no processo penal. Belo Horizonte: Editora D´Plácido, 2017. Cap 25, p. 517-538.

BADARÓ, G. **A cadeia de custódia da prova digital**. Direito probatório. Londrina: Thoth, 2023.

BADARÓ, G. **Os *standards* metodológicos de produção na prova digital e a importância da cadeia de custódia**. Boletim IBCCRIM, São Paulo, v. 29, n. 343, p. 7–9, 2021. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/1325>. Acesso em: 03 set. 2025.

BADARÓ M., C. **A propósito da cadeia de custódia das provas digitais no Processo Penal: breves notas sobre lógica da desconfiança, assimetria informacional e direito de defesa**. Boletim IBCCRIM, São Paulo, v. 31, n. 368, 2023. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/506>. Acesso em: 03 set. 2025.

BORRI, L. A.; SOARES, R. J. Da ilicitude da prova em razão da quebra da cadeia de custódia. **Revista da Faculdade de Direito da FMP**, v. 15, n. 1, p. 73-82, 11 set. 2020.

BRASIL. Instrução Normativa DG/PF Nº 299, de 24 de fevereiro de 2025. **Regulamenta a cadeia de custódia de elementos de interesse em formato digital no âmbito da Polícia Federal**. Brasília, DF: Ministério da Justiça e Segurança Pública, Polícia Federal, 24 fev. 2025. Disponível em: < https://pfgovbr.sharepoint.com/sites/intranet/normativosinternos/Instrução Normativa/2025/in-299-2025-dg-pf.aspx>. Acesso em: 25 out. 2025

BRASIL. Lei n. 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal; altera o Decreto-lei n. 3.689, de 3 de outubro de 1941, Código de Processo Penal. **Diário Oficial da União**, 30 abr 2021.

BRASIL, Ministério da Justiça e Segurança Pública. **Relatório final: câmaras técnicas de cadeia de custódia:** discussão, diagnóstico e recomendações pós Lei n. 13.964/2019. Secretaria Nacional de Segurança Pública. Brasília, 2023.

BRASIL. **Procedimento operacional padrão: perícia criminal**. Brasília, DF: Ministério da Justiça, Secretaria Nacional de Segurança Pública, 2013. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/pop/procedimento_operacional_padrao-pericia_criminal.pdf>. Acesso em: 13 out. 2025.

CAPANEMA, W. A. **Manual de direito digital teoria e prática**. 2ª Edição – 2025, Editora JUSPODIVM.

CAUCHICK-MIGUEL, P. A. **Metodologia de Pesquisa em Engenharia de Produção e Gestão de Operações.** 3. ed. Rio de Janeiro-RJ: Editora GEN LTC, 2018.

CEARÁ. Secretaria da Segurança Pública e Defesa Social. ***Software* Galileu, desenvolvido pela Pefoce, completa cinco anos de criação**. 02 abr. 2024. Disponível em: <https://www.pefoce.ce.gov.br/2024/04/02/software-galileu-desenvolvido-pela-pefoce-completa-cinco-anos-de-criacao/>. Acesso em 03 out. 2023.

CHACON, M. M.; SIQUEIRA, M. de. **A validade da prova digital no processo judicial brasileiro: requisitos técnicos e jurisprudenciais**. Revista Foco, [S. l.], v. 18, n. 6, p. e9017, 2025. Disponível em: <https://ojs.focopublicacoes.com.br/foco/article/view/9017>. Acesso em: 19 set. 2025.

D'ANNA, T.; PUNTARELLO, M.; CANNELLA, G.; SCALZO, G.; BUSCEMI, R.; ZERBO, S.; ARGO, A. ***The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data***. *Healthcare (Switzerland)*, *11*(5). 2023. Disponível em: <https://doi.org/10.3390/healthcare11050634>. Acesso em: 09 set. 2025.

ELGOHARY, H. M.; DARWISH, S. M.; ELKAFFAS, S. M. ***Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications***. IEEE *Access*, 2022. DOI: 10.1109/ACCESS.2022.3147809. Disponível em: <https://doi.org/10.1109/ACCESS.2022.3147809>. Acesso em: 21 out. 2025.

ESPÍRITO SANTO. Polícia Científica (PCIES). **Perito da Polícia Científica do Espírito Santo lidera desenvolvimento e implantação do sistema que integrará perícias ao SINESP**. [S.l.]: Assessoria de Comunicação da Polícia Científica, 15 ago. 2025. Disponível em: <https://pci.es.gov.br/Not%C3%ADcia/policia-cientifica-do-espirito-santo-lidera-desenvolvimento-e-implantacao-do-sistema-que-vai-integrar-pericias-ao-sinesp>. Acesso em: 02 nov. 2025.

FURLANETO NETO, M.; SANTOS, J. E. L. dos. **Apontamentos sobre a cadeia de custódia da prova digital no brasil**. Revista Em Tempo, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3130>. Acesso em: 02 set. 2025.

GIACOMOLLI, N. J.; AMARAL, M. E. A. **A cadeia de custódia da prova pericial na Lei nº 13.964/2019**. Duc In Altum – Cadernos de Direito, Recife, v. 12, n. 27, p. 123-145, 2020. Disponível em: <https://revistas.faculdadedamas.edu.br/index.php/cihjur/article/view/1305>. Acesso em: 11 set. 2025.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2010, p. 42.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo-SP: Atlas, 2017.

GOIÁS. Polícia Científica do Estado de Goiás. **Lançamento do novo Sistema de Informações ODIN**. Goiânia, 2018. Disponível em: <https://goias.gov.br/policiacientifica/lancamento-do-novo-sistema-de-informacoes-odin/>. Acesso em: 8 nov. 2025.

GOIÁS. **Portaria n. 325, de 12 de abril de 2022. Estabelece diretrizes sobre os procedimentos a serem observados pelas forças de segurança pública do Estado de Goiás no tocante à cadeia de custódia da prova**. Diário Oficial do Estado, Goiânia, n. 23.779, p. 21, 18 abr. 2022.

GUTTMAN, B.; WHITE, D. R.; WALRAVEN, T. ***Digital evidence preservation: considerations for evidence handlers***. *Interagency Report* NIST (IR) NIST IR 8387, 2022. Disponível em: <https://doi.org/10.6028/NIST.IR.8387>. Acesso em: 02 nov. 2025

JAQUET-CHIFFELLE, D. O.; CASEY, E.; BOURQUENOUD, D. ***Tamperproof timestamped provenance ledger using blockchain technology.*** *Forensic Science International: Digital Investigation*, v. 32, p. 300926, 2020. Disponível em <https://doi.org/10.1016/j.fsidi.2020.300977>. Acesso em: 29 ago. 2025.

KHANJI; S.; Alfandi, O.; Ahmad, L.; Kakkengal, L.; Al-kfairy, M. ***A systematic analysis on the readiness of blockchain integration in IoT forensics.*** *Forensic Science International: Digital Investigation*, v. 42-43, p. 301472, 2022. Disponível em <https://doi.org/10.1016/j.fsidi.2022.301472>. Acesso em: 29 ago. 2025.

LAKATOS, E. M.; MARCONI, M. de A. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017, p. 85-90.

LEITE, I.; ACAYABA, C. **Com quase 3 mil equipamentos, PM inicia implantação de novas câmeras a partir de junho**. g1 SP, São Paulo, 30 maio 2025. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2025/05/30/com-quase-3-mil-equipamentos-pm-inicia-implantacao-de-novas-cameras-a-partir-de-junho.ghtml>. Acesso em: 29 out. 2025.

LOPES JÚNIOR, A. **Direito processual pena**l. 16. ed. São Paulo: Saraiva Educação, 2019.

MENEZES, I. A. de; BORRI, L. A.; SOARES, R. J. **A quebra da cadeia de custódia da prova e seus desdobramentos no processo penal brasileiro.** Revista Brasileira de Direito Processual Penal, Porto Alegre, v. 6, n. 1, p. 209-238, 2020. Disponível em: <https://revista.ibraspp.com.br/RBDPP/article/view/128>. Acesso em: 11 set. 2025.

PACELLI, E. **Curso de Processo Penal**. 24. ed. São Paulo: Atlas, 2020.

PARANÁ. Polícia Científica. **Novo Sistema de Gestão de Laudos é implantado na Polícia Científica do Paraná**. 16 mai. 2014. Disponível em: Disponível em: <https://www.policiacientifica.pr.gov.br/Noticia/Novo-Sistema-de-Gestao-de-Laudos-e-implantado-na-Policia-Cientifica-do-Parana>. Acesso em 20 out. 2025.

PARANÁ. Polícia Científica. **10 anos do primeiro laudo inserido no Sistema Gestor de Laudos**. 12 dez. 2023. Disponível em: <https://www.policiacientifica.pr.gov.br/Noticia/10-anos-do-primeiro-laudo-inserido-no-Sistema-Gestor-de-Laudos#:~:text=A%20Pol%C3%ADcia%20Cient%C3%ADfica%20do%20Paran%C3%A1%20comemorou%20em,S%C3%A3o%20Paulo%20para%20conhecer%20o%20sistema%20GDL%2C>. Acesso em 20 set. 2025.

PARANÁ. Secretaria de Segurança Pública. **Paraná será 1º estado da América Latina a testar câmeras corporais com IA e tradução simultânea**. 23 mai. 2025. Disponível em: <https://www.seguranca.pr.gov.br/Noticia/Parana-sera-1o-estado-da-America-Latina-testar-cameras-corporais-com-IA-e-traducao#:~:text=Paran%C3%A1%20ser%C3%A1%201%C2%BA%20estado%20da,simult%C3%A2nea%20%7C%20Secretaria%20da%20Seguran%C3%A7a%20P%C3%BAblica>. Acesso em 02 nov. 2025.

PARODI, L. **A cadeia de custódia da prova digital à luz da Lei 13.964/2019**. Consultor Jurídico, [S. l.], 18 jun. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-18/lorenzo-parodi-cadeia-custodia-prova-digital?utm_source=dlvr.it&utm_medium=twitter>. Acesso em: 19 set. 2025.

PIAUÍ. Polícia Civil. Departamento de Polícia Científica. Central de Custódia de Vestígios. **Ofício Nº 14816/2025/PC-PI/DEPOC/CCV.** Implantação do protocolo de envio e armazenamento digital de vestígios – DRIVE.PI. Teresina, 24 jul. 2025a. 3 p. Documento eletrônico assinado por Charles da Costa Cunha.

PIAUÍ. Polícia Civil. Departamento de Polícia Científica. Gabinete do Perito Geral. **Portaria N. 187/2025 – Gabinete do Perito Geral do Departamento de Polícia Científica da PC/PI**, de 29 de maio de 2025. Dispõe sobre a utilização do DRIVE.PI (Piauí Box) como repositório oficial de vestígios digitais no âmbito do Departamento de Polícia Científica da Polícia Civil do Estado do Piauí. Teresina, PI, publicado no Diário Oficial do Piauí, n. 101/2025b, p. 62-63. Disponível em: <https://www.diario.pi.gov.br/doe/files/diarios/anexo/12e1e223-adea-4801-bd9b-8baf02117172/DOEPI_101_2025.pdf>. Acesso em 27 out. 2025.

SANTOS, Juarez Cirino dos. **Direito Penal: Parte Geral**. 6. ed. Curitiba: ICPC, 2020.

SÃO PAULO (Estado). Polícia Científica. **Manual de Operação GDL–IC**. São Paulo: Polícia Científica, 2019.

SÃO PAULO (Estado). Superintendência da Polícia Técnico-Científica. Instituto de Criminalística. **Manual de Operação do Módulo do GDL-IC para Solicitação de Relatório de Análise**. Elaborado por Melina Guerreiro Rodrigues. São Paulo: IC/SPTC, 2023.

SILVA, D. A. M. da. **Manual de Utilização ODIN: Sistema de Informações de Criminalística**. Goiás: Polícia Científica de Goiás, 2018. Disponível em: <https://odin.ssp.go.gov.br/sistemas/odin/ajuda/ger_documento.php>. Acesso em: 21 out. 2025.

STEFFEN, C. **Cadeia de custódia da prova digital no Brasil: o que se precisa, o que se tem e por que pensar em *blockchain*?** Revista da EMERJ, v. 27, e643, p. 1-15, 2025. Disponível em: <https://ojs.emerj.com.br/index.php/revistadaemerj/article/view/643>. Acesso em: 02 set. 2025.

TEODÓSIO, Vinícius. **Novo *software* reduz tempo-resposta do trabalho entre peritos e policiais**. [Alagoas]: Governo do Estado de Alagoas, 15 jul. 2021. Disponível em: <https://alagoas.al.gov.br/noticia/novo-software-reduz-tempo-resposta-do-trabalho-entre-peritos-e-policiais>. Acesso em 29 out. 2025.

TORRES, P. R. **Desafios contemporâneos do direito à prova:** obtenção de dados digitais armazenados no exterior. Revista Fac. Dir. | Uberlândia, MG, v. 50, n. 1, p. 229-252, jan./jun. 2022. Disponível em: <https://doi.org/10.14393/RFADIR-50.1.2022.65264.229-252>. Acesso em: 05 ago. 2025.

UMBELINO, F. P. E. S. **Proposta de aprimoramento da cadeia de custódia em Goiás**. Maio-2025.

VAZ, M. F. **A preservação da cadeia de custódia como pressuposto de admissibilidade da prova digital**. Revista da ESMESC, [S. l.], v. 30, n. 36, p. 323–350, 2023. Disponível em: <https://revista.esmesc.org.br/re/article/view/406>. Acesso em: 19 ago. 2025.

XAVIER, Roberison. **Sistema criado pela SSP dá agilidade em ações processuais contra a criminalidade em Alagoas:** Requisição de equipes e envio de laudos têm sido otimizados com a utilização do Forensis. [Alagoas]: Governo do Estado de Alagoas, 08 mai. 2024. Disponível em: <https://alagoas.al.gov.br/noticia/sistema-criado-pela-ssp-da-agilidade-em-acoes-processuais-contra-a-criminalidade-em-alagoas>. Acesso em 29 out. 2025

ZAFFARONI, E. R. **Manual de Direito Penal Brasileiro**. 10. ed. São Paulo: Revista dos Tribunais, 2020.