DIPLOMÁTICA CONTEMPORÂNEA: UMA ANÁLISE DIALÓGICA COM A PERÍCIA FORENSE DIGITAL

CONTEMPORARY DIPLOMACY: A DIALOGICAL ANALYSIS WITH DIGITAL FORENSIC ANALYSIS

Kevin Vanel Lekika Boucka[1]
Camila Schwinden Lehmkuhl[2]

RESUMO: A Diplomática contemporânea e a perícia forense digital são áreas que se complementam na análise e na preservação de documentos digitais. A diplomática estuda a autenticidade e a integridade dos documentos, enquanto a perícia forense digital utiliza métodos científicos para analisar evidências digitais em investigações. O objetivo da pesquisa foi analisar a relação entre essas áreas, identificando seus elementos, examinando cursos de perícia forense digital e evidenciando as conexões existentes entre elas. Utilizou-se uma pesquisa exploratória e qualitativa, baseada em fontes bibliográficas e em dados do MEC. Os resultados demonstraram que os cursos concentram-se principalmente na camada lógica dos documentos digitais, com ênfase em temas técnicos, como segurança da informação e redes, mas também abordam aspectos da camada conceitual, como autenticidade e cadeia de custódia. A camada física apareceu em poucos tópicos, estando relacionada à infraestrutura de armazenamento. A pesquisa reforça a importância da articulação entre os conhecimentos da diplomática e da perícia digital para a formação de profissionais capazes de compreender os documentos digitais em todos os seus aspectos, desde a estrutura técnica até o valor legal e informacional. Por fim, sugere-se que novas investigações aprofundem o papel dos metadados e da cadeia de custódia nas análises forenses.
Palavras-chave: diplomática contemporânea; perícia forense digital; documentos digitais; análise diplomática.

ABSTRACT: Contemporary Diplomatics and digital forensic investigation are complementary fields in the analysis and preservation of digital records. Diplomatics studies the authenticity and integrity of documents, while digital forensics employs scientific methods to analyze digital evidence in investigative contexts. The objective of this study was to examine the relationship between these fields by identifying their core elements, analyzing digital forensic investigation courses, and highlighting the existing connections between them. An exploratory and qualitative approach was adopted, based on bibliographic sources and data from the Brazilian Ministry of Education (MEC). The results showed that the courses focus primarily on the logical layer of digital records, emphasizing technical topics such as information security and computer networks, while also addressing aspects of the conceptual layer, including

[1] Graduando do curso de Graduação em Arquivologia, Centro de Ciências da Educação (CED), Departamento de Ciências da Informação (CIN), Universidade Federal de Santa Catarina (UFSC). E-mail: vanelkevin02@gmail.com.
[2] Docente na Universidade Federal de Santa Catarina, Centro de Ciências da Educação (UFSC), Departamento de Ciência da Informação (CIN) e no Programa de Pós-graduação em Ciência da Informação – PGCIN/UFSC. E-mail: camila.lehmkuhl@ufsc.br.

authenticity and the chain of custody. The physical layer appeared in only a few topics and was mainly related to storage infrastructure. The study underscores the importance of integrating knowledge from Diplomatics and digital forensics in order to educate professionals capable of understanding digital records in all their dimensions, from technical structure to legal and informational value. Finally, it suggests that future research further explore the role of metadata and the chain of custody in forensic analyses.
Keywords: contemporary diplomatics; digital forensics; digital records; diplomatic analysis.

1 INTRODUÇÃO

A Diplomática é a disciplina que estuda a estrutura formal dos documentos e a sua autenticidade. Seu objeto de análise abrange elementos como formato, suporte, espécie, entre outros. Preocupa-se em informar o que é o documento, quais são as suas características externas (físicas) e internas (conteúdo), atestando, por meio de seu método de análise, a autenticidade dos documentos arquivísticos.

Para Nascimento e Konrad (2016), a propagação das novas tecnologias e a produção acentuada de documentos em ambientes digitais criaram desafios aos arquivistas, como manter e preservar os documentos em meio digital sem prejuízo de sua integridade, fidedignidade e autenticidade nos sistemas em que foram gerados, bem como garantir-lhes o acesso. Nesse contexto, a Diplomática contemporânea surge como um referencial essencial para enfrentar esses desafios, pois amplia seu campo de análise para além dos documentos tradicionais e passa a considerar as estruturas, funções e propriedades dos documentos digitais.

Outro assunto de interesse desta pesquisa, a forense digital, é uma das aplicações da ciência forense e busca analisar provas e evidências digitais para a identificação de possíveis crimes cibernéticos. Segundo Montoya-Mogollón e Troitiño Rodríguez (2019), a Ciência Forense Digital dedica-se à aplicação de métodos cientificamente validados para coletar, verificar, identificar, analisar, interpretar, registrar e apresentar evidências provenientes de fontes digitais, visando à reconstrução de acontecimentos e à prevenção de ações indevidas ou não autorizadas. Assim, a presente pesquisa tem como objetivo geral analisar a relação entre a Diplomática contemporânea e o ensino da perícia forense digital.

A fim de atingir o objetivo geral, definem-se os seguintes objetivos específicos: identificar os elementos constituintes da Diplomática contemporânea; analisar disciplinas e suas ementas em cursos de especialização em perícia forense digital; e apresentar as intersecções identificadas entre a Diplomática contemporânea e o ensino da perícia forense digital.

Para alcançar esses objetivos, serão utilizados como métodos a pesquisa bibliográfica em bases de dados como SciELO e a Base de Dados em Ciência da Informação (BRAPCI), bem como a pesquisa documental realizada no site do Ministério da Educação (MEC) e nas ementas das disciplinas dos cursos de forense digital.

A escolha do presente tema justifica-se pela crescente necessidade de aprofundar os estudos no campo arquivístico, especialmente diante da expansão das demandas por profissionais capacitados para lidar com documentos digitais em processos judiciais e administrativos, bem como pela possível relação com a formação de peritos forenses digitais no Brasil, que também têm como objeto a análise de documentos digitais.

Este trabalho também se justifica por seu valor formativo, uma vez que permite ao pesquisador aprofundar seus conhecimentos em áreas interdisciplinares, como a Arquivologia e a Perícia Forense Digital. O estudo contribui para o desenvolvimento acadêmico e profissional do autor, além de ampliar sua compreensão sobre os desafios e as possibilidades de atuação no campo da perícia digital.

O presente texto apresenta uma abordagem inicial sobre a Diplomática, seguida da discussão acerca da perícia forense digital, da metodologia adotada para a pesquisa, da análise dos dados, das considerações finais e das referências.

2 DIPLOMÁTICA

A Diplomática nasce como uma ciência que tem por objeto os diplomas, as cartas e outros documentos oficiais, com o objetivo de determinar sua autenticidade, sua integridade e a época ou data em que foram produzidos. Também pode ser considerada uma disciplina voltada ao estudo das estruturas formais de documentos solenes, provenientes de atividades governamentais ou notariais.

De acordo com Torrão e Valentim (2020), a Diplomática é uma ciência baseada na análise dos elementos internos e externos dos documentos, evidenciando suas relações com os produtores, com o objetivo de identificar, avaliar e comunicar sua verdadeira natureza.

Para Berwanger e Leal (2008, p. 25), “a palavra diplomática deriva do latim *diploma*, originalmente um escrito dobrado em dois, *diplous* (duplo). Diplomática é, etimologicamente, ‘a ciência dos diplomas”.

> Historicamente, a definição de diplomática, esteve intimamente ligada ao conceito de documento que caracteriza seu objeto de estudo. Entendido como peça singular ou integrante de um conjunto, esta concepção vai ser distintiva para explicar as correntes

> teóricas que se formaram em nível internacional e como vai ocorrer sua reaproximação com a arquivística (Rodrigues, 2016, p. 3).

Segundo Tognolli e Guimarães (2009), a diplomática nasceu com a finalidade de estabelecer regras que auxiliassem na comprovação da autenticidade dos documentos produzidos e recebidos pelas igrejas católicas.

Para Tognoli (2014), a Diplomática surgiu no século XVII, a partir da publicação, em 1681, da obra *De Re Diplomatica*, do historiador francês Jean Mabillon, considerada o primeiro tratado a estabelecer critérios específicos para combater a falsificação documental, prática comum na época, especialmente em mosteiros que buscavam comprovar direitos sobre terras e privilégios.

Lima e Flores (2015) afirmam que a diplomática, enquanto área do conhecimento autônoma, também se consolida no século XVII, em decorrência das chamadas guerras diplomáticas, que, segundo Bellotto (2004), tiveram início quando o jesuíta Daniel de Papenbroeck questionou a autenticidade de alguns documentos beneditinos.

Nascimento e Konrad (2016, p. 32) afirmam que:

> Em sua origem, a Diplomática esteve ligada ao estabelecimento de regras para comprovar a autenticidade dos documentos produzidos durante a Idade Média. Nos séculos seguintes, passou por mudanças em relação aos seus métodos, com estreita ligação com outros campos, tais como a Paleografia, a História e o Direito. Essas mudanças culminaram numa ampliação significativa de seu objeto de estudo e do seu campo de ação.

A Diplomática Clássica, na abordagem tradicional, é a ciência que tem como finalidade principal distinguir documentos autênticos de falsificações, sobretudo no âmbito religioso e jurídico. Ela se concentra na análise dos elementos externos do documento, como o suporte, os selos, a caligrafia e os materiais utilizados, bem como dos elementos internos, como fórmulas, assinaturas e estilo de escrita.

Rodrigues (2016, p. 5) afirma que:

> Os documentos diplomáticos, objeto da Diplomática se a disciplina for tomada em sua perspectiva clássica, são os de natureza jurídica, que refletem no ato escrito às relações políticas, legais, sociais e administrativas entre o Estado e os cidadãos, cujos elementos semânticos são submetidos a fórmulas preestabelecidas.

Na visão moderna da Diplomática, a análise dos documentos é reforçada, pois não considera apenas a estrutura e o conteúdo, mas também o contexto de produção, que está vinculado às funções, atividades e competências do órgão produtor, as quais apresentam profundas relações com a Arquivística (Rodrigues, 2016).

Lima e Flores (2015) indicam que, a partir do século XX, a Diplomática pode ser dividida em Diplomática Histórica e Diplomática Arquivística. Esta última, a partir da década

de 1980, passou a auxiliar os arquivistas na difícil tarefa de compreender o processo de criação dos documentos contemporâneos, uma vez que a Diplomática e a Arquivística são duas áreas que possuem o mesmo objeto de estudo, o documento de arquivo, ainda que o tratem de formas distintas. A Diplomática limita-se à análise de sua base interna, voltando-se para a veracidade das informações de maneira singular; já a Arquivística preocupa-se com o documento como um todo. Entretanto, em determinados momentos, ambas acabam necessitando uma da outra para atingir uma análise mais complexa e, consequentemente, alcançar melhores resultados.

Segundo Silva e Flores (2018), é por meio das relações entre a Diplomática e a Arquivística que termos como diplomática arquivística contemporânea, diplomática digital ou simplesmente diplomática contemporânea passaram a ser adotados, sobretudo em publicações de diversos autores, como Paola Carucci, na Itália, e Luciana Duranti, no Canadá. A diplomática contemporânea, derivada da diplomática tradicional, ampliou seu campo de análise para abranger documentos modernos, inclusive os digitais, incorporando conceitos de gênese, forma e contexto em diálogo com a Arquivística.

A diplomática digital aplica esses princípios aos documentos arquivísticos digitais, considerando as dimensões física, lógica e conceitual das três camadas de documentos de arquivo digital, fundamentais para a avaliação da autenticidade e do valor probatório.

Para Tognoli e Guimarães (2009), o arquivista é capaz de reconstruir todo o contexto de produção de um conjunto documental por meio da aplicação do método diplomático, a partir da análise de um único documento, uma vez que as fontes utilizadas para reconstruir o percurso documental, como organogramas e regimentos, por exemplo, nem sempre são suficientes.

Portanto, de acordo com Tognoli e Guimarães (2009), a análise do documento contemporâneo tem como objetivo contribuir para a história da administração, além de adaptar os conhecimentos da diplomática tradicional ao mundo atual, garantindo a autenticidade e a confiabilidade dos documentos produzidos em diferentes formatos e contextos, bem como contribuindo para uma gestão arquivística eficiente e para a preservação da informação.

2.1 ANÁLISE DIPLOMÁTICA CONTEMPORÂNEA

A análise diplomática baseia-se no estudo da estrutura e dos elementos formais dos documentos, com o objetivo de comprovar sua autenticidade, legitimidade e vínculo com o contexto de produção. A prática da diplomática consiste na análise diplomática e na tipologia documental, por meio do protocolo inicial, do texto e do protocolo final (Bellotto, 2002). Nessas

seções, identificam-se fórmulas obrigatórias próprias de cada espécie documental, bem como variações que refletem as particularidades do ato e de seu contexto.

De acordo com Bellotto (2002), o documento diplomático é composto por três partes estruturais que, em conjunto, revelam sua forma, função e autenticidade. Como mencionado anteriormente, encontra-se o protocolo inicial, que contém os elementos de identificação e introdução do documento, como o tipo documental, o emissor, o destinatário, a data e o local de produção, elementos que legitimam a origem e a autoridade do ato. O texto constitui o núcleo do documento, expressando o conteúdo jurídico ou administrativo, que representa a manifestação da vontade do autor, bem como os motivos e os efeitos pretendidos. Já o protocolo final compreende os elementos de encerramento e autenticação, como assinaturas, selos, rubricas ou fórmulas de validação, assegurando a integridade e a veracidade do registro. A análise dessas três partes permite compreender a estrutura formal e a intencionalidade do documento, aspectos fundamentais para avaliar sua autenticidade e seu valor probatório.

Segundo Torrão (2020), o século XXI trouxe profundas transformações nas formas de produzir, acessar e utilizar informações, impulsionadas pelo desenvolvimento tecnológico e pelo surgimento dos objetos digitais. Nesse novo contexto, a Arquivologia passou a enfrentar desafios relacionados aos documentos digitais, sejam eles digitalizados ou natos digitais, recorrendo à diplomática como base teórico-metodológica para compreender e tratar adequadamente essas novas manifestações documentais.

A análise diplomática em ambiente digital segue os mesmos princípios da análise diplomática tradicional, concentrando-se na avaliação dos elementos que garantem a autenticidade e a integridade dos documentos, como a estrutura, a autoria e o contexto. No entanto, no ambiente digital, surgem novos desafios, como a preservação e o rastreamento de metadados, inexistentes na forma tradicional em papel. Enquanto, na análise diplomática tradicional, a autenticidade do documento é mais facilmente verificada pela aparência física e pelos elementos visíveis no próprio documento, na versão digital é necessário considerar como os dados e metadados associados são gerenciados, preservados e acessados ao longo do tempo.

Para Rondinelli (2005), a análise diplomática em ambiente digital consiste em adaptar os princípios da diplomática tradicional às características dos documentos eletrônicos. Ela envolve o exame dos elementos formais e tecnológicos, como metadados, assinaturas digitais e cadeia de custódia, com o objetivo de verificar a autenticidade, a integridade e a fidedignidade do documento digital ao longo de seu ciclo de vida.

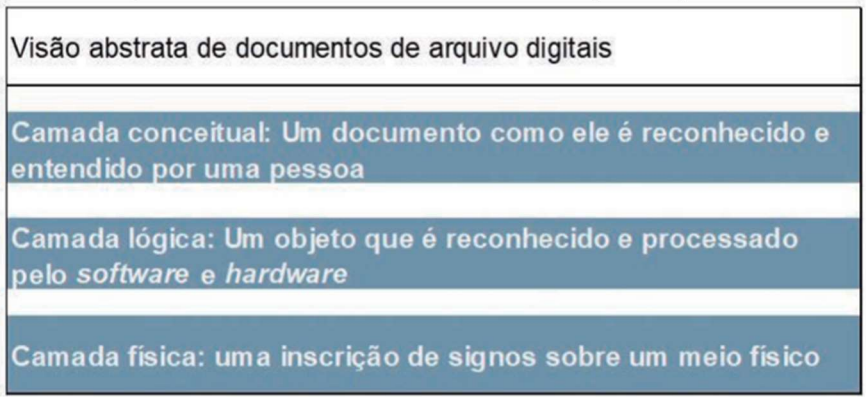
> No mundo do suporte em papel, esses elementos da forma são evidentes simplesmente com uma inspeção visual ao documento de arquivo. No ambiente digital, eles podem

> ser visíveis na manifestação conceitual do documento de arquivo, porém, pode existir também (ou não) na representação lógica do documento de arquivo. Assim, eles podem ser explícitos nos dados do documento de arquivo (conteúdo) ou capturados manualmente ou automaticamente como metadados associados ao documento de arquivo conceitual. Esses metadados podem estar imediatamente visíveis (por exemplo, o nome do arquivo e o caminho), visíveis por meio das funções disponíveis para qualquer usuário do sistema no qual o documento do arquivo é armazenado (por exemplo, o tamanho do arquivo a data de criação ou a última modificação), ou visível por meio simplesmente de uma investigação mais complexa utilizando ferramentas especializadas (forense digital) (Rogers, 2020, p. 100).

Segundo Rogers (2020), a identificação e a verificação da autenticidade de documentos digitais exigem a aplicação dos princípios da diplomática arquivística, com a análise dos elementos formais extrínsecos e intrínsecos presentes nos metadados de identidade e integridade. Esses elementos manifestam-se nas camadas conceitual e lógica do documento, sendo independentes do meio físico em que os dados são armazenados, uma vez que as regras do nível lógico garantem a manutenção da estrutura e da autenticidade do documento, mesmo diante de mudanças no suporte.

Diante do exposto, Rogers (2020) afirma que os documentos arquivísticos digitais são compostos por diferentes tipos de dados e metadados, tanto aqueles gerados pelo usuário quanto os produzidos automaticamente pelos sistemas e aplicativos. Esses metadados registram informações sobre a origem, o formato, o contexto e o funcionamento do documento, sendo fundamentais para sua identificação e preservação. Nesse sentido, a análise diplomática em ambiente digital, ao aplicar os princípios da análise diplomática tradicional, permite reconhecer quais metadados são essenciais para garantir a autenticidade, a integridade e a confiabilidade dos documentos digitais ao longo do tempo.

Imagem 1: Visão abstrata de documentos de arquivo digitais



Fonte: Rogers (2020).

A imagem 1 representa a visão abstrata dos documentos de arquivo digitais. Esses documentos podem ser compreendidos em três níveis de abstração, conforme a perspectiva da autora Rogers (2020). O primeiro nível é a camada conceitual, na qual o documento é reconhecido e compreendido por uma pessoa, sendo representado pelo conteúdo intelectual (texto, imagem, som e vídeo), pelo contexto de produção (quem, quando e por quê) e pelos atributos arquivísticos, tais como autenticidade, integridade, organicidade e unicidade.

Em seguida, tem-se a camada lógica, que corresponde ao objeto digital processado por software e hardware, incluindo estruturas de dados e metadados, formatos de arquivos (por exemplo, PDF, DOCX e XML), além dos sistemas que interpretam esses dados para torná-los legíveis.

Por fim, a camada física representa a inscrição dos signos em suportes materiais, sendo constituída por dados binários (0s e 1s) armazenados em dispositivos como discos rígidos, SSDs, servidores, entre outros, bem como pelos componentes eletrônicos responsáveis pela leitura e gravação desses dados. Os metadados estão presentes nas camadas conceitual e lógica e configuram-se como elementos fundamentais para a análise diplomática de documentos digitais, contribuindo para a identificação e a avaliação da autenticidade e da confiabilidade dos documentos de arquivo. Apesar disso, há desafios, muitas vezes, relacionados ao rastreamento de sua origem e manutenção. Essa visão abstrata demonstra a complexidade dos documentos digitais e a importância de considerar as três camadas para a garantia da autenticidade dos documentos arquivísticos nato-digitais.

A análise desenvolvida permitiu compreender que a Diplomática se adaptou às transformações tecnológicas e continua sendo essencial para garantir a autenticidade e a integridade dos documentos digitais. No contexto atual, sua aplicação na área da perícia forense digital mostra-se indispensável para validar a veracidade das evidências e manter a confiabilidade da cadeia de custódia. Percebe-se que o arquivista e o perito forense digital compartilham responsabilidades semelhantes, uma vez que ambos buscam assegurar que os documentos digitais mantenham seu valor probatório e informacional.

3 FORENSE DIGITAL

A forense digital é um ramo da ciência forense que abrange a recuperação e a investigação de materiais encontrados em dispositivos digitais, geralmente relacionados a crimes computacionais. Ela consiste, basicamente, no uso de métodos científicos para a

preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais com validade probatória em juízo.

Montoya Mogollón e Troitiño Rodríguez (2019) afirmam que a ciência forense digital tem por objetivo aplicar métodos comprovados e desenvolvidos cientificamente para a coleta, validação, identificação, análise, interpretação, documentação e apresentação da prova em ambiente digital, obtida por meio de fontes digitais, com a finalidade de facilitar e otimizar a reconstrução de eventos, bem como prevenir ações não apropriadas ou não autorizadas, como invasões ou adulterações. Para os autores, "a Ciência Forense é considerada uma área de conhecimento relativamente recente. No entanto, a construção dessa ciência tem vários séculos de consolidação" (Montoya Mogollón; Troitiño Rodríguez, 2019, p. 56).

Padilha et al. (2021) definem a ciência forense digital (CFD) como o ramo da Ciência Forense que trata da análise e investigação de conteúdos associados a dispositivos digitais, desde equipamentos de grande porte, como servidores e roteadores de empresas globais, até dispositivos móveis, como celulares e *wearables*.

Souza (2015) afirma que a forense consiste na aplicação de conhecimentos científicos a questões criminais e que a perícia forense computacional, ou perícia forense digital, é uma fusão entre conhecimentos da área da informática e da área jurídica. Seu objetivo é coletar evidências digitais, analisar dados e apresentar provas em ambiente jurídico, visando sempre à elucidação de um fato. O termo forense digital foi originalmente utilizado como sinônimo de forense computacional, mas expandiu-se para abranger a investigação de todos os dispositivos capazes de armazenar dados digitais. Com raízes na revolução da computação pessoal no final dos anos 1970 e início dos anos 1980, a disciplina evoluiu de maneira desordenada durante a década de 1990, e foi somente no início do século XXI que surgiram as políticas nacionais.

Montoya-Mogollón e Troitiño Rodríguez (2019, p. 56) destacam que:

> O surgimento da perícia forense no Ocidente, remetendo sua origem ao ano 130 da Era Cristã, passando pelo processo romano, a Idade Média e dos séculos XV ao XXI. O trabalho deste autor destaca a evolução da ciência em cada período histórico, até seu desenvolvimento no século XIX e XX, época em que se começa a falar de uma Ciência Forense Moderna.

O perito forense digital é um profissional especializado em investigar e analisar evidências digitais encontradas em dispositivos eletrônicos. Atua na investigação da materialidade e da autoria de fraudes, incidentes e crimes cibernéticos ou virtuais, utilizando metodologias forenses para a coleta, recuperação, preservação e análise de evidências digitais.

Segundo Souza (2015), o processo de perícia forense digital é composto por quatro etapas principais, fundamentais para garantir que as evidências digitais sejam válidas, seguras

e úteis à investigação. O processo inicia-se com a etapa de coleta, na qual são identificadas e coletadas fontes que provavelmente contenham evidências digitais ou que possuam relação com o evento investigado. É fundamental que essa etapa ocorra de maneira rápida, sempre que possível, logo após o conhecimento do incidente, e que siga procedimentos capazes de preservar a integridade do material coletado.

Após a coleta, tem início a etapa de extração das informações contidas nas cópias, com o propósito de identificar e obter dados relevantes para a investigação. As cópias seguras, produzidas na fase de coleta, são reproduções integrais do material apreendido, ou seja, contêm todos os arquivos, dados e configurações existentes no original.

Com os dados extraídos, inicia-se a fase de análise, que consiste em um exame das informações obtidas a partir do material apreendido, buscando a identificação de evidências digitais que possuam relação com o fato investigado.

A apresentação, ou documentação, é a etapa final do processo forense, pois, nessa fase, a tarefa da perícia consiste em documentar as evidências digitais encontradas e apresentá-las às autoridades competentes.

> A Ciência Forense digital encontra-se em um momento ideal (Forensics Readiness) como auxílio em ciências, tais como a Psicologia, a Medicina, as Engenharias e a Criminologia, entre outras. Seus estudos atuais, principalmente no contexto internacional, estão gerando profícuas pesquisas no âmbito da Arquivologia. No entanto, por ser uma ciência relativamente nova, surgida no final do século XX, alguns conceitos continuam sendo aprimorados, tanto no seu próprio corpus teórico e prático, como na adaptação em outras ciências (Montoya-Mogollón; Troitiño Rodriguez, 2022, p. 2-3).

De acordo com Montoya Mogollón e Troitiño Rodríguez (2019), os elementos metodológicos da forense digital oferecem princípios e fundamentos que, quando articulados ao conhecimento da Diplomática — ciência voltada ao estudo dos diplomas, cartas e demais documentos oficiais, com o objetivo de determinar sua autenticidade, integridade e data de produção — e da Arquivologia — área dedicada à organização, preservação, conservação e gestão de documentos em ambientes físicos e digitais —, proporcionam soluções para as complexidades que envolvem os documentos arquivísticos nascidos digitais. Nesse sentido, esta pesquisa busca demonstrar essas relações a partir da análise do ensino da forense digital no Brasil.

Ao concluir a análise sobre a Forense Digital, torna-se evidente que essa área, apesar de sua consolidação recente, desempenha um papel fundamental diante da complexidade dos documentos digitais e das novas dinâmicas de produção e circulação da informação. A leitura

crítica dos autores estudados e o exame dos métodos forenses permitem perceber que a atuação do perito digital não se limita ao domínio técnico, mas exige uma compreensão profunda sobre autenticidade, integridade, proveniência e contexto, princípios que dialogam diretamente com a Diplomática Contemporânea. Nesse sentido, compreende-se que a Forense Digital e a Arquivologia não apenas compartilham preocupações comuns, mas se complementam ao enfrentar os desafios trazidos pelos documentos natos digitais, sobretudo no que se refere à preservação das evidências, à manutenção da cadeia de custódia e à validação probatória. Refletindo sobre esse cenário, reconhece-se que a interseção entre essas áreas revela um campo interdisciplinar em expansão, no qual a formação do perito digital precisa integrar não apenas competências tecnológicas, mas também fundamentos arquivísticos e diplomáticos que sustentem análises mais rigorosas e confiáveis dos documentos digitais no contexto jurídico e investigativo.

4 METODOLOGIA

A metodologia utilizada neste relatório, do ponto de vista de seu objetivo, caracteriza-se como uma pesquisa exploratória, ou seja, uma pesquisa preliminar que visa proporcionar maior familiaridade com o problema exposto, ao prover mais informações sobre o assunto (Rodrigues; Neubert, 2023).

Para a coleta de dados, utilizou-se a pesquisa bibliográfica, realizada por meio de materiais publicados, com o objetivo de proporcionar ao pesquisador contato com o conhecimento produzido, recolher informações e compreender a teoria relacionada ao objeto de pesquisa (Rodrigues; Neubert, 2023). Também foi utilizada a pesquisa documental que, segundo as autoras Rodrigues e Neubert (2023), é elaborada a partir de materiais que não receberam tratamento analítico.

Quanto à abordagem, trata-se de uma pesquisa qualitativa, considerando a relação, a análise e a interpretação subjetivas para a atribuição de significados aos fenômenos estudados. Não requer o uso de métodos e técnicas estatísticas, mas demanda padronização dos registros e das análises (Rodrigues; Neubert, 2023).

Em relação à natureza, é considerada uma pesquisa básica, que objetiva a produção de novos conhecimentos, úteis para o avanço da ciência, sem previsão de aplicação prática. Nesse sentido, envolve interesses universais (Rodrigues; Neubert, 2023).

As bases de dados utilizadas para a pesquisa bibliográfica foram a SciELO e a Base de Dados em Ciência da Informação (BRAPCI). A SciELO foi selecionada por contemplar

diversas áreas do conhecimento, e a BRAPCI por ser uma base de dados de referência na área. Na busca efetuada nas bases identificadas, foram utilizados alguns filtros para delimitar a pesquisa, como idioma (português) e palavras-chave (forense digital; diplomática contemporânea).

Tendo em vista que o objetivo central desta pesquisa é identificar, de forma precisa, elementos dialógicos entre a diplomática contemporânea e a forense digital, optou-se por uma estratégia de busca simples, baseada nessas palavras-chave. Essa delimitação metodológica resultou em uma quantidade considerável de pesquisas recuperadas nas bases consultadas. Contudo, caso se utilizasse uma abordagem combinada das duas palavras-chave, haveria um número reduzido de resultados.

Após a pesquisa bibliográfica, foi realizada a leitura dos títulos, sendo analisadas e selecionadas as pesquisas que mais se adequavam ao objetivo deste estudo, qual seja, a identificação de uma relação dialógica entre ambos os conceitos centrais da pesquisa, frente à propagação das novas tecnologias e à produção acentuada de documentos em ambientes digitais.

O Quadro 1 apresenta o resultado compilado da pesquisa bibliográfica realizada, indicando a base utilizada, as palavras-chave, os resultados recuperados e os selecionados para a pesquisa em tela.

Quadro 1 - Resultados de buscas nas bases de dados

Base	**Palavra-chave**	**Recuperado**
SCIELO	Forense Digital	2
	Diplomática Contemporânea	2
BRAPCI	Forense Digital	15
	Diplomática Contemporânea	49
Total		68

Fonte elaborada pelo autor (2025)

No total, foram recuperadas, nas duas bases de dados (SciELO e BRAPCI), por meio das duas palavras-chave, 68 pesquisas. Além dessas, foram identificados outros artigos por meio de pesquisas livres em bases de dados como o Google, bem como textos utilizados ao longo da disciplina de Introdução à Diplomática Contemporânea. A partir da leitura dos títulos e resumos, foram selecionadas 13 pesquisas diretamente relacionadas ao tema do estudo, as quais foram utilizadas na elaboração do presente trabalho.

A pesquisa documental foi realizada por meio da plataforma oficial e-MEC, utilizando como filtro principal a palavra-chave “Forense Digital”, aplicada aos cursos de especialização oferecidos por Instituições de Ensino Superior (IES) da Região Sul, nas modalidades a distância e presencial. Inicialmente, o escopo da busca contemplava exclusivamente os estados da Região Sul (Paraná, Santa Catarina e Rio Grande do Sul), sobretudo por estarem localizados na região de residência do autor. Contudo, devido à dificuldade de encontrar dados necessários para a elaboração do trabalho — como matrizes curriculares, disciplinas e ementas —, bem como à quantidade limitada de cursos específicos na área nessa região, justificou-se a ampliação da busca para o estado de São Paulo, que concentra um número elevado de instituições privadas e uma oferta significativa de cursos de especialização relacionados à perícia forense.

Dessa forma, no total, foram recuperados 16 cursos. Após a análise, três deles foram excluídos por não apresentarem vínculo com as questões digitais, resultando em um total de 13 cursos a serem analisados.

Após a análise das áreas relacionadas e da denominação dos cursos, foram selecionados, para a pesquisa, 13 cursos vinculados a questões digitais, especialmente às três camadas do documento de arquivo digital. Assim, o Quadro 2 apresenta o conjunto final das instituições identificadas, totalizando três ofertas, todas vinculadas à rede privada, na modalidade a distância (EaD), a qual se destaca como a principal forma de oferta na área.

Quadro 2 –Resultado dos cursos selecionados para a pesquisa, de acordo com dados do e-MEC

Instituição (IES)	Sigla	UF de Oferta	Curso	Categoria	Modalidade
Centro Universitário UNIFATEB	-	PR	Perícia Forense aplicada à Informática	Privada	Educação a Distância
Faculdade Iguaçu	FI	PR	Perícia forense aplicada à informática	Privada	Educação a Distância
Faculdade Iguaçu	FI	PR	Perícia forense aplicada a informática (360 h)	Privada	Educação a Distância
Faculdade Iguaçu	FI	PR	Perícia forense computacional	Privada	Educação a Distância
Faculdade Iguaçu	FI	PR	Perícia forense computacional (360h)	Privada	Educação a Distância
Faculdade Norte-sul	FANS	SC	Perícia forense aplicada a informática	Privada	Educação a Distância
Faculdade Norte-sul	FANS	SC	Perícia forense computacional	Privada	Educação a Distância

Universidade do Oeste Paulista	UNOESTE	SP	Perícia forense	Privada	Educação Presencial
Minas Faculdade	MFMG	SP	Perícia forense aplicada a informática	Privada	Educação a Distância
Universidade Cruzeiro do Sul	UNICSUL	SP	Perícia forense computacional	Privada	Educação a Distância
Minas Faculdade	MFMG	SP	Perícia forense computacional	Privada	Educação a Distância
Minas Faculdade	MFMG	SP	Perícia forense computacional	Privada	Educação a Distância
Universidade Cruzeiro do Sul	UNICSUL	SP	Perícia forense computacional 360h	Privada	Educação a Distância

Fonte elaborada pelo autor (2025)

O Quadro 2 apresenta os resultados obtidos por meio das pesquisas realizadas no site do e-MEC, totalizando 13 ofertas de cursos, majoritariamente relacionados à Perícia Forense Digital ou à Perícia Forense Computacional, distribuídos entre seis instituições privadas brasileiras. A maioria dos cursos está sendo ofertada na modalidade de Educação a Distância. As formações abrangem áreas como Perícia Forense Aplicada à Informática e Perícia Forense Computacional, entre outras, incluindo também cursos complementares, como Fisioterapia em Perícia Forense e Gestão em Perícia Forense e Criminologia, sobretudo em áreas correlatas à forense digital.

Depois o levantamento dos cursos, o passo seguinte consistiu na busca pelas disciplinas e ementas ofertadas por essas formações.

Após o contato com todas as instituições, foi possível identificar que algumas possuíam o curso aprovado pelo e-MEC, porém não haviam aberto turmas de formação até o momento; outras não forneceram as ementas, tampouco responderam aos e-mails ou às ligações realizadas com o objetivo de solicitar informações a respeito dos cursos encontrados no site do e-MEC. Por se tratarem de instituições privadas, não há obrigatoriedade de disponibilização das informações, e o contato, muitas vezes realizado exclusivamente por meio do WhatsApp, direcionava a chatbots automatizados, nos quais não era possível solicitar as grades curriculares e suas respectivas ementas.

Após esse percurso, obteve-se um total de três instituições participantes da pesquisa, as quais forneceram matrizes curriculares completas.

Para finalizar o percurso metodológico da pesquisa, o Quadro 3 apresenta, de forma sintética, as abordagens e a classificação da metodologia utilizada.

Quadro 3 – Abordagens e classificações das pesquisas

Forma de classificação	**Tipo de método adotado**
Quanto à natureza	Pesquisa básica
Quanto aos objetivos	Pesquisa exploratória
Quanto à abordagem	Pesquisa qualitativa
Quanto aos procedimentos técnicos	Pesquisa bibliográfica
	Pesquisa documental

Fonte: elaborado pelo autor (2025), baseado em: Rodrigues; Neubert (2023).

O Quadro 3 representa as abordagens e classificações das pesquisas utilizadas para a elaboração do presente trabalho. Nessa tabela, encontram-se as formas de classificação quanto à natureza, aos objetivos, à abordagem e aos procedimentos técnicos da pesquisa. Em relação aos objetivos do trabalho, foram escolhidos os seguintes tipos de pesquisa: pesquisa básica, quanto à natureza; pesquisa exploratória, quanto aos objetivos; pesquisa qualitativa, quanto à abordagem; e pesquisa bibliográfica e documental, quanto aos procedimentos técnicos.

A rigorosa delimitação das bases de dados (SciELO e BRAPCI) e das palavras-chave permitiu a seleção criteriosa do material mais relevante para a análise, resultando em um corpus fundamentado e alinhado ao objetivo proposto.

A ampliação da pesquisa documental, por meio da plataforma e-MEC, para instituições da Região Sul e do estado de São Paulo reforçou a abrangência e a representatividade dos dados, apesar das limitações enfrentadas quanto à obtenção das matrizes curriculares junto às instituições de ensino. Tal metodologia garantiu a produção de conhecimentos sólidos, técnicos e teóricos, que sustentam as análises subsequentes da pesquisa, demonstrando a importância do rigor metodológico em estudos interdisciplinares na área de documentos digitais e perícia forense.

5 RESULTADOS

A partir da análise dos resultados dos cursos selecionados para a pesquisa com base nos dados do e-MEC, foi possível reunir as informações apresentadas no Quadro 4. Esse quadro sintetiza os cursos e disciplinas oferecidos pelas instituições que forneceram suas matrizes curriculares. A seleção dessas disciplinas considerou especificamente aquelas cujas ementas apresentavam relação direta com as três camadas do documento arquivístico digital e com práticas forenses aplicadas ao ambiente digital.

Quadro 4 –Resultado dos cursos e disciplinas relacionadas à pesquisa

Universidades	Cursos	Disciplinas
Minas Faculdade	Perícia Forense Aplicada à Informática	Análise Forense em Sistemas Operacionais
		Laudo Pericial e Parecer Técnico
		Análise Forense em Redes de Computação
Minas Faculdade	Perícia Forense Computacional	Métodos e Técnicas de Investigação
		Vulnerabilidade de Sistemas Operacionais e Redes de Computadores
		Perícia Forense Computacional
		Laudo Pericial e Parecer Técnico
Unoeste	Perícia Forense	Computação Forense

Fonte: elaborado pelo autor (2025).

O Quadro 4 apresenta um panorama das instituições brasileiras que disponibilizaram as matrizes curriculares dos cursos na área de forense digital, destacando os três cursos que forneceram essas informações detalhadas. Essas instituições são a Faculdade Minas, com os cursos de Perícia Forense Aplicada à Informática e Perícia Forense Computacional que possuem cargas horárias diferentes, e a Unoeste, com o curso de Perícia Forense. As disciplinas destacadas representam aquelas cujos conteúdos ou ementas se relacionam mais diretamente com as três camadas do documento arquivístico digital. Essa escassez de dados sobre as matrizes curriculares demonstra um desafio para a análise aprofundada da formação acadêmica na área, enquanto os cursos disponíveis indicam uma ênfase relevante em aspectos investigativos e técnicos essenciais para a atuação pericial em ambientes digitais.

A partir da identificação das disciplinas que possuem relação com a pesquisa em tela, o Quadro 5 apresenta suas ementas e as relações dialógicas observadas com a diplomática contemporânea. Essas relações foram identificadas com base nas três camadas utilizadas na análise diplomática contemporânea conceitual, lógica e física, apresentadas no referencial teórico anterior.

Quadro 5 –Relação dos conteúdos das ementas das disciplinas com a diplomática contemporânea

Sigla	Disciplina	Ementa	Relação dialógica com a Diplomática Contemporânea
MFMG	Análise Forense em Sistemas Operacionais	Investigação Criminal; Tipos de Investigação; Métodos de Raciocínio na Investigação Policial; Meios Dinâmicos da Investigação; Penetração e Infiltração; Atuação da Perícia Digital; Computação Forense; **Preservação e Aquisição de Evidências Digitais;** Técnicas de Análise Forense; Sistemas Biometria e AFIS; Recognição Visuográfica de Local de Crime; Ferramentas de Investigação Forense Computacional; Sistema IPED; EnCase; FTK; UFED Touch; DFF; Xplico; Legislação e Competências da Polícia Judiciária; Técnicas de Inquérito Policial; Direitos do Advogado e Garantias Constitucionais; Competência do Ministério Público e Polícia Judiciária; Desafios da Investigação Criminal Contemporânea.	O processo de preservação e aquisição de evidências digitais pode se relacionar de forma integrada às três camadas do documento arquivístico digital. Ele pode atuar primeiramente na camada física, garantindo a integridade dos dados binários e a proteção dos suportes de armazenamento; pode envolver também a camada lógica, ao preservar os formatos, metadados e sistemas que asseguram a legibilidade e autenticidade do documento; e pode se estender à camada conceitual, ao manter o valor probatório e o contexto original das informações, assegurando que elas possam ser interpretadas e utilizadas como evidências confiáveis em investigações ou processos administrativos e jurídicos.
	Laudo Pericial e Parecer Técnico	Termo Forense; Forense Computacional; Procedimentos e Métodos Aplicados à Perícia Forense Computacional; Perícia e Conceitos Fundamentais; Perito Criminal e Perito Nomeado; Análises Físicas; **Análises de Sistemas de Arquivos; Elaboração de Laudo e Parecer Técnico**; Contestação e Apoio do Parecer Técnico do Assistente; Crimes Relacionados ao Uso de Computadores; Tipos de Exames Forenses Computacionais; Aspectos Técnicos e Legais da Perícia Forense; Fases da Perícia Forense Computacional; **Cadeia de Custódia**; Papel do Laudo Pericial no Código de Processo Penal; Responsabilidade e Revisão do Laudo Pericial; Importância do Parecer Técnico como Prova Judicial.	A análise de sistemas de arquivos, elaboração de laudo e parecer técnico e cadeia de custódia podem se relacionar diretamente às três camadas dos documentos arquivísticos digitais, pois atuam de forma integrada na garantia da autenticidade e integridade da informação digital. A análise de sistemas de arquivos está ligada principalmente à camada lógica, pois envolve o exame das estruturas e metadados que organizam os dados digitais. A cadeia de custódia transita entre a camada física e a lógica, assegurando o controle, a rastreabilidade e a preservação dos suportes e das informações ao longo do tempo. Já a elaboração de laudo e parecer técnico pode situar-se na camada conceitual, onde o perito interpreta as informações obtidas e as transforma em conhecimento técnico validado, conferindo valor probatório ao documento digital.

	Análise Forense em Redes de Computação	Computação Forense; História da Computação Forense; Processo Forense; Técnicas de Análise Forense em Redes; Crimes Eletrônicos e a Atuação da Perícia Digital; Malware e Principais Ameaças Digitais; Metodologias de Resposta a Incidentes; **Coleta de Evidências;** Análises Live, Network e Post Mortem; Ferramentas de Investigação Forense; Aspectos Legais e Competências da Polícia Judiciária; **Aplicações em Crimes Cibernéticos** como Fraudes, Espionagem Industrial, Crimes Contra a Honra e Pedofilia; Desafios da Investigação Digital; Importância da Segurança da Informação para Prevenção de Incidentes.	A coleta de evidências e as aplicações em crimes cibernéticos, como fraudes, podem se relacionar diretamente às três camadas dos documentos arquivísticos digitais, pois envolvem desde o registro até a interpretação conceitual das informações. Na camada física, concentram-se os dados binários e os suportes digitais onde as evidências são coletadas, como discos rígidos ou servidores. Na camada lógica, ocorre o processamento e a análise técnica desses dados por meio de softwares forenses, que organizam e revelam informações relevantes ao caso investigado. Já na camada conceitual, as evidências são interpretadas e contextualizadas pelo perito, que transforma a informação técnica em prova compreensível e válida juridicamente, permitindo a identificação de fraudes e outros crimes cibernéticos.
MFMG	Métodos e Técnicas de Investigação	Perícia Forense Computacional; Definição e Fundamentos da Perícia Forense; Métodos de Investigação; **Coleta de Dados Digitais;** Cadeia de Custódia e Preservação de Evidências; Etapas de Exame, Análise e Formalização; Técnicas de Recuperação e Indexação de Dados; Análises de Vestígios Digitais; **MACtimes e Sistemas de Arquivos;** Métodos de Preservação de Evidências Digitais; Uso de Funções Hash e Mídias Ópticas; Dificuldades da Investigação: Anti Forense, Criptografia, Esteganografia e Wipe; Desafios Tecnológicos e Jurídicos; Marco Civil da Internet; Projeto de Lei Azeredo; Importância da Legislação Atualizada e da Atuação do Perito Forense Computacional.	A camada física abrange as etapas de coleta de dados digitais, MACtimes[3] e sistemas de arquivos, pois envolvem o registro e a leitura dos dados diretamente nos suportes e dispositivos. A camada lógica relaciona-se à recuperação e indexação de dados e às análises de vestígios digitais, já que trata da organização, interpretação e estruturação das informações pelos sistemas e softwares. Por fim, a camada conceitual corresponde à cadeia de custódia e aos métodos de preservação de evidências digitais, pois é nesse nível que se garante o valor probatório, a autenticidade e o significado das informações no contexto arquivístico e pericial.
	Vulnerabilidade de Sistemas Operacionais e Redes de Computadores	Vulnerabilidade de Sistemas; Ataques a Sistemas Operacionais e Redes; Malware e Suas Categorias; Exploits e Ferramentas de Ataque; Spywares, Rootkits, Backdoors e Ransomwares; Infraestrutura de Segurança; Base Computacional Confiável (Trusted Computing Base); **Autenticação, Controle de Acesso e Auditoria;** Segurança	A autenticação, controle de acesso e auditoria podem estar diretamente relacionados às três camadas dos documentos arquivísticos digitais, pois garantem sua segurança e confiabilidade em cada nível. Na camada física, atuam na proteção dos suportes e dispositivos que armazenam os dados, prevenindo acessos ou alterações indevidas. Na camada

[3] *Modified*, *Accessed* e *Changed* (modificação, acesso e alteração de metadados) são campos de metadados que registram a data e hora de eventos importantes de um arquivo.

		em Sistemas Operacionais; Redes de Computadores; História da Comunicação em Redes; Arquiteturas e Topologias de Rede; Protocolos de Comunicação e Padrões IEEE; Modelos OSI e TCP/IP; Classificação de Redes (LAN, MAN, WAN, PAN, CAN, SAN); Tecnologias de Transmissão; Hardware de Rede (Switches, Roteadores, Firewalls); Desafios Contemporâneos de Segurança.	lógica, asseguram que apenas usuários autorizados possam abrir, editar ou processar os arquivos, mantendo o registro das ações realizadas nos sistemas. Já na camada conceitual, contribuem para validar a autenticidade e a integridade do documento, permitindo comprovar sua origem, autoria e histórico de uso, elementos essenciais para a preservação da confiabilidade arquivística em ambiente digital.
	Perícia Forense Computacional	Introdução à Forense Computacional; Conceitos Fundamentais; Contexto Histórico da Computação e Evolução Tecnológica; Importância da Forense Computacional; Dinâmica, Materialidade e Autoria de Crimes Digitais; Crimes que Necessitam de Investigação Forense Computacional; Principais Ferramentas de Investigação (IPED, EnCase, FTK, UFED Touch, DFF, Xplico); Atuação do Perito Computacional; Técnicas Anti Forense; Criptografia e Criptoanálise; **Assinatura Digital; Certificado Digital**; **Preservação de Evidências; Cadeia de Custódia;** Desafios Tecnológicos e Jurídicos; Legislação Brasileira e Internacional Aplicada à Perícia Forense.	A assinatura digital e o certificado digital podem operar principalmente na camada lógica, onde validam a origem e a integridade dos dados por meio de algoritmos criptográficos e sistemas de verificação. Já a preservação de evidências e a cadeia de custódia abrangem as camadas física e conceitual, assegurando, respectivamente, a proteção dos dados armazenados e a manutenção do contexto, da proveniência e da rastreabilidade do documento ao longo do tempo. Assim, esses mecanismos complementam as três camadas, garantindo que o documento digital permaneça autêntico e confiável tanto do ponto de vista técnico quanto arquivístico.
UNOESTE	Computação Forense	**Análise, interpretação e procedimentos** relacionados ao conhecimento da Computação, como sistemas operacionais, redes de computadores, segurança da informação, banco de dados, entre outras.	A análise, interpretação e procedimentos relacionados ao conhecimento da computação, como sistemas operacionais, redes, segurança da informação e bancos de dados — se inserem principalmente na camada lógica dos documentos arquivísticos digitais. Essa camada é responsável por organizar e processar os dados por meio de softwares, protocolos e sistemas tecnológicos, garantindo que o documento possa ser reconhecido, estruturado e interpretado corretamente. Em outras palavras, é nessa camada que as ferramentas e conhecimentos da computação atuam para transformar os dados físicos em informações legíveis e seguras, servindo de base para que, na camada conceitual, o ser humano atribua sentido e valor arquivístico ao documento.

Fonte: Elaborado pelo autor (2025).

O Quadro 5 apresentou os resultados da análise das ementas das disciplinas selecionadas dos três cursos de perícia forense ministrados em instituições de ensino brasileiras, correlacionando-as com as três camadas do documento arquivístico digital: camada física, camada lógica e camada conceitual, conforme modelo arquivístico.

A análise revelou que os conteúdos das disciplinas apresentam forte relação com essas camadas. Por exemplo, o processo de preservação e aquisição de evidências digitais atua na camada física, garantindo a proteção dos dados binários e dos suportes físicos de armazenamento. Ele se estende à camada lógica, que assegura o formato, os metadados e a autenticidade, e à camada conceitual, que mantém o valor probatório e o contexto original das informações para uso em investigações ou processos judiciais.

Além disso, tópicos como a análise forense de sistemas de arquivos vinculam-se fortemente à camada lógica, enquanto a cadeia de custódia transita entre as camadas física e lógica, garantindo a rastreabilidade e a preservação das informações.

A elaboração de laudos e pareceres técnicos insere-se na camada conceitual, onde o conhecimento técnico é interpretado e validado para conferir valor probatório aos documentos digitais.

As disciplinas voltadas para coleta de evidências e aplicações em crimes cibernéticos abrangem as três camadas, desde a captura física dos dados, passando pelo processamento lógico e culminando na interpretação conceitual.

Em termos numéricos, a análise contemplou ementas de 3 cursos, demonstrando uma integração consistente entre a formação acadêmica ofertada e os princípios arquivísticos digitais. Esse alinhamento assegura a confiabilidade, a integridade e a utilidade jurídica das evidências digitais trabalhadas nesses cursos, traduzindo a importância da interdisciplinaridade entre ciência da computação, direito e arquivologia na formação do perito forense.

6 CONSIDERAÇÕES FINAIS

Considera-se que a pesquisa atingiu plenamente os objetivos propostos, ao identificar os elementos constituintes da Diplomática contemporânea, analisar as disciplinas e ementas dos cursos de perícia forense digital e apresentar as intersecções existentes entre essas duas áreas. A investigação evidenciou que a diplomática contemporânea e a perícia forense digital mantêm

uma relação dialógica sólida, sobretudo no que se refere à análise, verificação e preservação de documentos arquivísticos digitais.

A análise das ementas obtidas demonstrou que os conteúdos se concentram majoritariamente na camada lógica dos documentos digitais, com forte presença de assuntos relacionados à segurança da informação, redes de computadores, bancos de dados e sistemas operacionais, revelando o caráter técnico predominante na formação forense.

Contudo, constatou-se também a presença relevante de disciplinas ligadas à camada conceitual, abordando temas como autenticidade, cadeia de custódia e contexto de produção documental aspectos que reforçam o diálogo entre Arquivologia, diplomática e ciência forense.

A camada física, ainda que menos explorada, surgiu pontualmente em conteúdos relacionados à infraestrutura tecnológica e aos suportes de armazenamento.

Esses resultados demonstram que uma abordagem interdisciplinar, integrando fundamentos arquivísticos e diplomáticos às práticas forenses, é essencial para formar profissionais capazes de compreender documentos digitais em sua totalidade, desde sua estrutura técnica até seu valor probatório e informacional.

Conclui-se que o fortalecimento do diálogo entre a Diplomática Contemporânea e a Perícia Forense Digital representa não apenas um avanço teórico, mas uma necessidade prática diante dos desafios contemporâneos de produção, preservação e validação de documentos digitais em ambientes administrativos e judiciais.

Como sugestões para pesquisas futuras, o escopo de aplicação pode ser alargado para cursos em todo o Brasil, destacando o papel dos metadados.

REFERÊNCIAS

BELLOTTO, Heloísa Liberalli. A análise diplomática e a crítica diplomática: elementos para a sua aplicação em arquivos. In: **Arquivos permanentes:** tratamento documental. 2. ed. Rio de Janeiro: FGV, 2002. p. 111-134. Disponível em: https://www.arqsp.org.br/arquivos/oficinas_colecao_como_fazer/cf8.pdf. Acesso em: 25 out. 2025.

BERWANGER, Ana Regina; LEAL, João Eurípedes Franklin. **Noções de Paleografia e de Diplomática.** 2. ed. rev. ampl. Santa Maria: Ed. UFSM, 2008. Acesso em: 22 jun. 2025.

MONTOYA-MOGOLLÓN, Juan Bernardo; RODRIGUEZ, Sonia Maria Troitiño. Integrando Funções Forenses e Arquivísticas: um diálogo **po**ssível. **Ágora:** Arquivologia em Debate, v. 32, n. 65, p. 1-16, 2022. Disponível em: https://agora.emnuvens.com.br/ra/article/view/1119. Acesso em: 22 jun. 2025.

MONTOYA-MOGOLLÓN, Juan Bernardo; TROITIÑO RODRÍGUEZ, Sonia Maria. Diplomática forense: revisão histórica para a abordagem do documento nato-digital de arquivo. **Investigación Bibliotecológica**: archivonomía, bibliotecología e información, v. 33, n. 78, p. 47-62, 2019. Disponível em: https://doi.org/10.22201/iibi.24488321xe.2019.78.57928. Acesso em: 17 jun. 2025.

NASCIMENTO, Maiara de Arruda; KONRAD, Glaucia Vieira Ramos. Da diplomática tradicional para a diplomática contemporânea: trajetória e convergências com a arquivística. **Ágora:** Arquivologia em Debate, v. 26, n. 53, p. 31-59, jul./dez. 2016. Disponível em: https://agora.emnuvens.com.br/ra/article/view/1156. Acesso em: 21 jun. 2025.

PADILHA, Rafael et al. A inteligência artificial e os desafios da ciência forense digital no século XXI. **Estudos Avançados,** v. 35, n. 101, p. 111-138, 2021. Disponível em: https://doi.org/10.1590/s0103-4014.2021.35101.009. Acesso em: 17 jun. 2025.

RODRIGUES, Ana Célia. Diplomática e arquivística: diálogos para a construção do método de identificação da tipologia documental. In: **Encontro Nacional de Pesquisa em Ciência Da Informação (Enancib),** 17., 2016, Salvador. Anais [...]. Salvador: ANCIB, 2016. Disponível em: https://www.enancib2016.sites.ufba.br/. Acesso em: 22 jun. 2025.

RODRIGUES, Ana Célia. **Diplomática contemporânea como fundamento metodológico da identificação de tipologia documental em arquivos.** In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO (ENANCIB), 17., 2016, Salvador. Anais [...]. Salvador: ANCIB, 2016. Disponível em: https://www.enancib2016.sites.ufba.br/. Acesso em: 22 jun. 2025.

RODRIGUES, Rosângela Schwarz; NEUBERT, Patricia da Silva. **Introdução à pesquisa bibliográfica.** Florianópolis: Editora da UFSC, 2023. Disponível em: https://doi.org/10.5007/978-65-5805-082-7. Acesso em: 16 jun. 2025.

ROGERS, Corrine. **Diplomática de Documentos Nato Digitais: a consideração da forma documental no ambiente digital.** 2020. Disponível em: http://arquivistica.fci.unb.br/wp-content/uploads/tainacan-items/476350/836109/Diplomatica-de-documentos-nato-digitais-a-consideracao-da-forma-documental-no-ambiente-digital.pdf. Acesso em: 25 out. 2025.

SILVA, William; FLORES, Daniel. **A diplomática contemporânea: reflexões sobre sua aplicabilidade na era digital.** Informação & Informação, v. 23, n. 1, p. 351-370, jan./abr. 2018. DOI: 10.5433/1981-8920.2018v23n1p351. Disponível em: http://www.uel.br/revistas/informacao/. Acesso em: 28 ago. 2025.

SOUZA, Paulo Francisco Cruz de. **Perícia forense computacional: procedimentos, ferramentas disponíveis e estudo de caso.** 2015. 83 f. Trabalho de Conclusão de Curso (Tecnologia em Redes de Computadores) – Universidade Federal de Santa Maria, Santa Maria, 2015. Disponível em: https://www.ufsm.br/app/uploads/sites/495/2019/05/2015-Paulo-Souza.pdf. Acesso em: 18 jun. 2025.

TOGNOLI, Natália Bolfarini. **A construção teórica da Diplomática: em busca de uma sistematização de seus marcos teóricos como subsídio aos estudos arquivísticos.** São Paulo: Cultura Acadêmica, 2014. Disponível em: /https://repositorio.unesp.br/server/api/core/bitstreams/1dfff8fd-6db1-40ba-adb6-15ebf61d71c4/content. Acesso em: 21 jun. 2025.

TOGNOLI, Natália Bolfarini; GUIMARÃES, José Augusto Chaves. **A diplomática contemporânea como base metodológica para a organização do conhecimento arquivístico: perspectivas de renovação a partir das ideias de Luciana Duranti.** Scire: Representación y Organización del Conocimiento, v. 15, n. 1, p. 23-34, 2009. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=2921994. Acesso em: 16 jun. 2025.

VALENTIM, Raquel Torrão; TOGNOLI, Natalia Bolfarini. **Convergências e divergências entre a Diplomática Digital e a Ciência Forense Digital.** Brazilian Journal of Information Science: Research Trends, v. 14, n. 4, set.–dez. 2020. Disponível em: https://doi.org/10.36311/1940-1640.2020.v14n4.10528. Acesso em: 22 jun. 2025.