ELEMENTO DE ANÁLISE DIPLOMÁTICA DIGITAL: OS VERIFICADORES DE ASSINATURA DIGITAL

DIGITAL DIPLOMATIC ANALYSIS ELEMENT: DIGITAL SIGNATURE CHECKERS

André Pavanati[*]
Camila Schwinden Lehmkuhl[**]

RESUMO
O desenvolvimento tecnológico trouxe novas ferramentas e formas para se produzirem documentos. Partindo da necessidade de registrar as informações, os documentos passaram das formas primitivas, como as escritas em argila, materiais duros, pergaminhos, papiro, papel para, por último, o documento digital. Juntamente com os registros documentais, identifica-se a produção de informações falsas ou falsificadas. Nesse sentido, a Diplomática surgiu para identificar a veracidade, autenticidade e possíveis falsificações. Atualmente, com documentos nato digitais, alguns elementos, tais como o *hash* documental e os metadados podem auxiliar a análise diplomática. Isso porque algoritmos criptográficos e técnicas de criptografia são aplicadas aos documentos que carregam uma assinatura digital. Nesse contexto, a presente pesquisa tem como objetivo investigar aspectos da integridade e autenticidade dos documentos arquivísticos nato digitais, na perspectiva da diplomática digital, a partir do hash documental, utilizando verificadores de assinatura. Esse trabalho se caracteriza quanto à natureza como uma pesquisa aplicada, de abordagem qualitativa. Quanto aos procedimentos, se identifica como documental, bibliográfico e estudo de caso. Em relação aos resultados obtidos, foi possível verificar que o *hash* documental, após a cifragem promovida pela assinatura digital, confere grau de integridade e autenticidade. Isso porque, com o verificador de assinatura é possível identificar se houve mudanças no texto do documento ou em algum de seus metadados, por meio da cifragem e decifragem do *hash* embarcado no documento.

Palavras-chave: Arquivologia; Diplomática Digital; Hash; Verificadores de assinatura.

ABSTRACT
Technological development has brought new tools in the way to produce documents. Starting from the need to record information, documents passed from primitive forms, such as writing on clay, hard materials, parchment, papyrus, paper to, finally, the digital document. Along with the documentary records, the production of false or falsified information has been identified. In this sense, Diplomatics emerged to identify the veracity, authenticity and possible falsifications. Nowadays, with born-digital documents, some elements, such as the document hash and metadata can help diplomatic analysis. This is because cryptographic algorithms and encryption techniques are applied to documents that carry a digital signature. In this context, the present research aims to investigate aspects of the integrity and authenticity of natural-born archival documents, from the perspective of digital diplomacy, from the document hash, using signature verifiers. This research is characterized as an applied research, with a qualitative approach. As to the procedures, it is identified as documental, bibliographic and as a case study. As to the results obtained, it was possible to verify that the document hash, after the encryption promoted by the digital signature, confers a degree of integrity and authenticity. This is because, with the signature verifier it is possible to identify whether there have been changes in the document text

[*] Graduando no curso de Arquivologia. Universidade Federal de Santa Catarina. E-mail: andre.p@ufsc.br
[**] Profª. Dra, Orientadora no curso de Arquivologia. Universidade Federal de Santa Catarina. E-mail: camila.lehmkul@ufsc.br

or in any of its metadata, through the encryption and decryption of the hash embedded in the document.

Keywords: Archival science; Digital Diplomatics; Hash; Signature Verifiers.

1 INTRODUÇÃO

A necessidade do registro de informações surgiu, inicialmente, como uma forma de controle de materiais e bens de consumo nas relações sociais. Com o crescimento de economias centralizadas, os funcionários de palácios e templos não podiam mais contar com a memorização de transações comerciais, necessitando, nesse sentido, registrar o que era comercializado tais como suas quantias (HOOKER, 1996). Com a produção e acúmulo documental, surge a preocupação com os registros e sua organização. Nesse sentido, Rousseau e Couture (1998) consideram que a história dos arquivos está ligada à história do suporte cuja informação está registrada, sendo os principais materiais utilizados para registrar a informação, a argila, o pergaminho, o couro, o papiro e posteriormente o papel.

Houve uma mudança cultural no método de criação dos documentos, com o surgimento da imprensa, a produção em massa passa a ser possível, ser padronizada e mais rápida. Mais tarde, de forma mais abrangente, as máquinas de escrever passam a ser adotadas por organizações e pessoas no desenvolvimento de suas atividades cotidianas.

Atualmente, ao recordarmos essa história do suporte para o registro da informação, estamos diante de mais uma mudança, trata-se do suporte eletrônico. A sociedade está em um momento de transição do anteparo dos registros textuais, onde sai do papel e migra para os documentos registrados em editores de textos, por meio de computadores. Primeiramente os documentos são criados nesses editores de texto para, em seguida, serem impressos.

Dessa forma, Moutinho (2011), considera que "a máquina de escrever foi suplantada pela supremacia do computador na era da informática e pela exigência crescente de um ritmo acelerado em que a competitividade e a qualidade estão associadas ao sucesso e ao lucro" (MOUTINHO, 2011, s.p.). Com o surgimento do computador e das facilidades para a produção textual, é possível fazer a digitação da matéria desejada, errando e corrigindo inúmeras vezes até a sua impressão, trazendo assim como no papel, preocupações relacionadas à sua autenticidade, integridade e originalidade e fazendo emergir outro tipo de diplomática, a diplomática digital.

Paralelamente à evolução dos suportes e facilidades com a produção documental, já na Idade Média, o registro das informações começou a ser contestado. Com o aumento da produção

de documentos falsos, que tinham como objetivo provar a propriedade de terras, fez surgir os estudos diplomáticos. Os estudos diplomáticos tinham como foco, naquele momento, reconhecer os diplomas autênticos e identificar os falsos ou falsificados produzidos em períodos passados (TOGNOLI, 2014). Nesse sentido, a diplomática se desenvolveu e auxiliou a identificação de documentos falsos por meio de manuais, normas e tratados criados na Áustria, Alemanha, Itália e França, por estudiosos da área. A diplomática atualmente não se ocupa somente dos documentos em papel, tanto é que é tratada hoje como diplomática digital ou diplomática contemporânea ocupando-se de "[...] tratar os documentos de arquivo digitais afim de garantir e averiguar a autenticidade, bem como garantir a preservação a longo prazo" (VALENTIM, 2020, p. 28).

1.1 TEMA E PROBLEMA DE PESQUISA

Os avanços da tecnologia fizeram com que além da produção, a transmissão de documentos por meio da Web fosse feita também de forma mais dinâmica. Nesse sentido, o tratamento documental precisa agora apontar, também, para os documentos em suporte digital. Muitos documentos começaram a ser digitalizados como forma de dinamizar a transmissão e o acesso à informação, diminuindo o manuseio ao documento em papel. No entanto, além da digitalização, os documentos de arquivo passaram a ser produzidos em ambiente digital os chamados documentos natos digitais, ou seja, aqueles que nascem digitais. A produção, tramitação e circulação dos documentos nato digitais são praticadas por empresas e por instituições públicas em todo o mundo. Contudo, sua validade, assim como no documento em papel, pode ser questionada. Isso porque o documento nato digital é também passível de falsificações.

Com o intuito de garantir a originalidade, autenticidade e integridade aos documentos digitais, surgiu o certificado digital de chaves assimétricas (ou chave pública). O documento assinado por meio desse tipo de certificado passa por um processo de cifragem que garante a sua identidade documental. No entanto, a ABNT ISO 32000-1, relativa ao gerenciamento de documentos em PDF, apresenta como normalização uma regra chamada parâmetro de transformação DocMDP que possui três estágios de permissão de alteração documental, podendo permitir apenas uma ou mais assinaturas, a depender do estágio adotado.

Nesse sentido, a diplomática aplicada aos documentos natos digitais dispõe de mais uma característica para a verificação da veracidade documental, ou seja, a análise da assinatura do documento arquivístico digital. Isso porque, ao assinar digitalmente um documento, existe

um processo de cifragem de um componente documental chamado função resumo ou *hash* que acompanha o documento.

Com o exposto, esta pesquisa apresenta o seguinte questionamento: de que forma o *hash* documental pode ser utilizado como base para a análise diplomática a partir de verificadores de assinatura?

1.2 OBJETIVOS

O objetivo geral deste trabalho é: investigar aspectos da integridade e autenticidade dos documentos arquivísticos nato digitais, na perspectiva da diplomática digital, a partir do *hash* documental, utilizando verificadores de assinatura. Enquanto que os objetivos específicos para a realização desta pesquisa são:

a) Apresentar as características diplomáticas dos documentos arquivísticos nato digitais como garantia da autenticidade;
b) Caracterizar o *hash* no documento nato digital;
c) Analisar as relações entre as características diplomáticas do documento arquivístico nato digital e o *hash* a partir de um verificador de assinaturas.

1.3 JUSTIFICATIVA

A presente pesquisa se justifica pela crescente produção de documentos nato digitais. Ademais, o pesquisador, além de discente do curso de Arquivologia, também é servidor Técnico Administrativo em Educação (TAE), da Universidade Federal de Santa Catarina (UFSC), lotado na Coordenadoria de Certificação Digital (CCD). Atuou no desenvolvimento intelectual do portal de assinaturas Assina UFSC, responsável pela assinatura digital de documentos, com a utilização de certificado digital de chaves assimétricas e do Verificador de Assinaturas UFSC.

Ainda como justificativa, conforme será apresentado na metodologia, há escassa produção sobre a temática em tela na área de CI. Nesse sentido, entende-se que essa pesquisa sirva como um caminho para levar à comunidade acadêmica, na área da Ciência da Informação, um entendimento de como as características de documentos digitais, produzidos com algoritmos criptográficos por meio do certificado digital, contribuem para a segurança da informação dos documentos arquivísticos a partir da ciência diplomática.

2 METODOLOGIA

A Pesquisa científica busca satisfazer dúvidas existentes sobre um objeto de pesquisa, respondendo às respectivas perguntas. Muitas vezes a busca pela resposta vem seguida por mais questionamentos. Hair *et al* (2005) dizem que a pesquisa tem como foco a verdade. Nesse sentido, as técnicas adotadas para a coleta e análise das informações precisam ser processadas e refletir seus resultados da forma mais clara possível.

A presente pesquisa se caracteriza quanto à natureza como uma pesquisa aplicada, pois segundo Vergara (2012) esse método busca gerar conhecimentos com a finalidade de resolver problemas de ordem prática. Quanto à abordagem, é uma pesquisa qualitativa. Nesse sentido, Triviños (2011) considera que a pesquisa qualitativa, ao se apoiar na fenomenologia, tem viés descritivo, já que tais fenômenos possuem significados impostos pelo ambiente, sendo que tal ambiente é produto de uma visão subjetiva, rejeitando visões quantitativas, mensuráveis ou numéricas. Dessa forma, a pesquisa busca relatar as características necessárias para a análise dos documentos assinados digitalmente por parte dos verificadores.

Quanto aos procedimentos para coleta de dados, esta é uma pesquisa documental e bibliográfica. Roesch (1999) considera a pesquisa bibliográfica a parte mais extensa do trabalho acadêmico, pois consiste em fazer leitura eficiente, analítica e uma análise compreensiva do texto, facilitando o resumo e a interpretação de forma sistemática. Além disso, também se caracteriza como um estudo de caso, visto que, segundo Godoy (1995), o pesquisador se utiliza do estudo de caso para realizar a análise de fenômenos atuais, onde, de forma cronológica, está amarrado à atualidade vivida por ele, utilizando-se de uma variedade de dados coletados para produzir relatórios mais informais.

Foi feita uma pesquisa bibliográfica sobre o tema em bases de dados como Brapci, por se tratar de uma das principais bases de dados no Brasil sobre os temas da Ciência da Informação (CI), com os termos "verificador *and* conformidade" e "verificador *and* assinatura", combinados. Na base Brapci não foi apresentado nenhum resultado para a busca selecionada. Nesse sentido, uma nova busca foi realizada com os termos "hash *and* documentos" combinados, buscando identificar produções nesse sentido, contudo, também não foi apresentado nenhum resultado para a busca selecionada. O termo "hash *and* documentos" foi utilizado para pesquisa no portal Scielo e foram apresentados 77 resultados, sendo que apenas 3 tratam do tema específico. Os outros resultados eram relativos à criptografia em sistemas com Internet das coisas (IoT), criptografias para e-mail e demais outras aplicações com criptografia.

Outras literaturas que tratam do tema documento digital com assinatura digital relatam informações de segurança, mas não explicam exatamente de qual forma a assinatura digital por meio do certificado digital podem conferir esse tipo de segurança.

Com relação à pesquisa documental, para Gil (2008, p. 51), "[...] a pesquisa documental vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetivos da pesquisa". Dessa forma, serão considerados os documentos que possuam dados relevantes para a presente pesquisa, como manuais, legislação e normas.

Quanto à delimitação, esta pesquisa visa analisar os documentos que contenham apenas uma assinatura digital, e que sejam submetidos aos verificadores de assinatura ou conformidade. Devido ao pouco tempo de pesquisa para este trabalho elegeu-se apenas os documentos com uma assinatura, devido à complexidade que documentos com mais assinaturas estão submetidos. Isso porque, de acordo com a norma ABNT ISO 32000-1 (2019), o documento digital pode assumir algumas regras, chamadas DocMDP. O DocMDP assume três opções, sendo o DocMDP1 o que será estudado nessa pesquisa. Segundo a norma ABNT ISO 32000-1 (2019, p. 639), no DocMDP1 "nenhuma alteração ao documento deve ser permitida; qualquer mudança no documento deve invalidar a assinatura".

Será feita uma análise comparativa entre os verificadores, objeto deste estudo, mostrando o que cada um busca verificar em relação ao documento digital.

O quadro abaixo busca apresentar de forma visual, objetiva e resumida os métodos adotados na execução de cada objetivo específico:

Quadro 1: Métodos aplicados aos objetivos

Objetivos	**Como executar**
a) Apresentar as características diplomáticas dos documentos arquivísticos digitais como garantia de integridade e autenticidade;	Pesquisa bibliográfica
b) Caracterizar o *hash* no documento digital;	Pesquisa bibliográfica + documental (manuais, legislação e normas)
c) Analisar as relações entre as características diplomáticas do documento arquivístico digital e o *hash* a partir de um verificador de assinaturas.	Pesquisa bibliográfica + documental + verificador de assinaturas (assina UFSC)

Elaborado pelo autor (2022).

3 DA DIPLOMÁTICA AOS HASHES: A BASE CONCEITUAL DA PESQUISA

Com a finalidade de buscar um melhor embasamento para a presente pesquisa, as seções seguintes irão tratar de temas que pretendem dar suporte ao alcance dos objetivos propostos,

como a diplomática, os algoritmos de resumo ou *hash* criptográfico e as bases do verificador de assinaturas.

3.1 DIPLOMÁTICA

A produção documental é uma atividade inerente ao ser humano, desde que se percebeu que não era mais possível utilizar da memorização para registrar atividades comerciais. Dessa forma, a sociedade passou a fazer registros, reduzindo a escrito as transações comerciais, administrativas e jurídicas, de forma que pudessem ser consultados futuramente, assegurando assim os seus direitos e as possíveis contestações em caso de litígio. No entanto, isso não impediu que registros documentais viessem a nascer falsos ou, mesmo após a sua produção, fossem falsificados. Nesse sentido, uma pessoa leiga não conseguiria identificar a falsidade documental de forma clara, pois é preciso que uma análise minuciosa das características desse documento seja realizada, avaliada e identificada, fazendo surgir a diplomática.

3.1.1 Breve histórico da Diplomática

Nos séculos XIV e XV, os humanistas renascentistas italianos Francesco Petrarca e Lorenzo Valla fizeram uma análise documental dos privilégios concedidos à Áustria por César Augusto e Nero no século I, além da doação feita por Constantino ao Papa Silvestre, no século IV e, nessa análise documental, comprovaram que esses privilégios e doações não passavam de falsificações (DURANTI, 1989). Duranti (1989, p.13, tradução nossa) ainda explica que "a transformação da análise crítica de espécies documentais em uma disciplina completa e autônoma foi determinada pelo o que foi chamado de 'guerra diplomática' (*bella diplomática*)", que ocorreu no século XVII. Fazendo um contexto histórico, Duranti (1989, p. 13, tradução nossa), relata que

> Em 1643, os Bollandistas começaram a publicar o primeiro volume de um trabalho colossal, a *Acta Sanctorum*, em que os testemunhos relativos à vida dos santos eram avaliados com a proposta de separar os fatos das lendas. Seu segundo tomo surgiu em 1675 com uma introdução escrita por Daniel Van Papenbroeck, na qual os princípios gerais para estabelecer a autenticidade de antigos pergaminhos foram rigorosamente enunciados. No entanto, aplicando esses princípios aos diplomas dos reis Francos, Papenbroeck declarou erroneamente um diploma de Dagoberto I como uma falsificação e, ao fazê-lo, desacreditou todos os diplomas Merovíngios, muitos dos quais foram preservados no Mosteiro Beneditino de Saint-Denis. Dom Jean Mabillon, Beneditino da Congregação de Saint-Maur, que havia sido chamado do mosteiro de Saint-Denis para a Abadia de Saint-Germain-des-Prés para publicar a vida dos santos Beneditinos, respondeu à acusação de Papenbroeck seis anos depois, em 1681, em um tratado de seis partes, *De Re Diplomatica Libri VI*, que estabeleceu as regras fundamentais da crítica textual.

Nesse sentido, Rondinelli (2005), considera que a guerra diplomática, ocorrida na Igreja Católica, entre beneditinos, jesuítas e dominicanos, foi o que conduziu o que se tem de análise crítica de documentos em disciplinas independentes, como é o caso da paleografia, sigilografia e diplomática. Seguindo na linha da diplomática como ciência documentária, Belloto (2006, p. 47), explica que ela nasceu "da reação do espírito crítico dos homens do século XVII à fidedignidade de certos 'diplomas' medievais. O início da atividade diplomatista liga-se à investigação sobre a falsidade *versus* a veracidade desses papeis". Belloto (2006) enfatiza que em um primeiro momento a nova técnica documental serviria à área do direito eclesiástico, como visto na guerra diplomática, mais do que em qualquer outra seara, mas, posteriormente, os historiadores e arquivistas se beneficiariam dessas técnicas.

Com o passar do tempo, os diplomatistas, arquivistas e historiadores, com o uso da nova técnica documental, ou seja, da aplicação da crítica diplomática, puderam fazer a análise de diplomas antigos escritos em papiros, bulas papais oriundas da Idade Média, além de decretos de lei na França de 1900. Tal prática permitiu a esses profissionais conhecer a gênese documental, tais como a forma, negócio jurídico e das pessoas que participaram da formação desses documentos (TOGNOLI, 2014). Explica Tognoli (2014), que pelo fato dos elementos das formas documentais nem sempre serem os mesmos, os diplomatistas do século XIX focaram em encontrar e analisar mais elementos de documentos antigos, excluindo os documentos contemporâneos da análise diplomática, limitando-se a um recorte de análise de documentos da Idade Média.

Contudo, no início do século XIX surgiu a diplomática moderna, que pode ser dividida em duas: histórica e arquivística. Possui como marco os métodos desenvolvidos por Sickel e com a posterior junção ao método de Ficker. Tal método, de acordo com Tognoli (2014, p. 87), consistia em enunciar o "[...] conceito de documento diplomático e o método de análise baseado no confronto de escrituras, além do estudo das circunstâncias de criação do ato e da sua documentação". Tognoli (2014) discorre sobre a junção desses métodos para a diplomática moderna, dizendo que

> Nesse momento, a arte começa a deslocar seus estudos da simples análise de diplomas falsos/autênticos para a relação dos documentos diplomáticos – ou seja, daqueles redigidos segundo formas determinadas que lhes conferem força probatória e fé pública – e seu contexto de criação. Novos elementos foram incorporados ao estudo dos documentos e à sua partição, expandindo seu uso aos demais países da Europa, como Itália e França (TOGNOLI, 2014, p. 85).

Tognoli (2014) faz uma comparação em que Mabillon está para a diplomática clássica assim como Sickel e Ficker estão para a diplomática moderna. No entanto, assim como houve

uma estagnação após o tratado de Mabillon, também ocorreu após os métodos de Sickel e Ficker.

No século XX, um novo marco da diplomática surge, onde Tognoli (2014) considera se tratar de um terceiro movimento. Tal movimento se destaca pelo fato de autores da escola diplomática francesa aproximarem, cada vez mais, a diplomática aos documentos de arquivo. Nesse momento, se faz importante entender o conceito de documento arquivístico que, de acordo com o a Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivo (CONARQ, 2020, p. 24), é o "documento produzido (elaborado ou recebido), no curso de uma atividade prática, como instrumento ou resultado de tal atividade, e retido para ação ou referência". Tognoli (2014) enfatiza que os autores apresentaram os

> [...] pressupostos para uma mudança na problemática da Diplomática e os autores que contribuíram para um 'descolamento' no foco da disciplina, enunciando a expansão dos limites cronológicos e espaciais da Diplomática e sua aproximação à Arquivística e aos documentos de arquivo; e em seguida 'A consolidação da Diplomática Contemporânea a partir dos estudos de Carucci e Duranti' a partir do final da década de 1980 – quando a disciplina é incorporada aos estudos arquivísticos como uma resposta às novas tecnologias e às novas formas de produção e organização dos documentos arquivísticos, sobretudo aqueles gerados em meio eletrônico, com base nos estudos de Paola Carucci e Luciana Duranti, na Itália e Canadá respectivamente (TOGNOLI, 2014, p. 88).

Os autores franceses que trouxeram contribuições consideráveis para a diplomática contemporânea foram Augusto Dumas com a obra *La Diplomatique et la forme des actes,* 1932, Auguste Dumas com a obra *La Diplomatique*, 1966 e Robert-Henri Bautier com a obra *Leçon d'ouverture du cours de Diplomatique à l'École des Chartes*, 1961. Estes autores deram subsídios para que Carucci e Duranti pudessem desenvolver suas contribuições à diplomática. Percebe-se que no fim da década de 1980 os documentos de arquivo começaram a experimentar uma mudança de suporte. Paola Carucci trouxe uma contribuição à diplomática com a obra *Il documento contemporâneo: Diplomatica e criteri di edizione*, 1987 e Luciana Duranti com a obra *Diplomatics: New uses for an Old Science*, 1989-1992. No entanto, é a obra de Luciana Duranti que traz uma nova perspectiva à diplomática e aos documentos contemporâneos, principalmente por conta da mudança de suporte documental em curso, saindo do físico em papel ou outros materiais, em direção ao digital. Tognoli (2014, p. 119) comenta que "[...] os estudos de Duranti sobre a Diplomática aplicada aos documentos de arquivo se destacam, ainda, por fornecer alguns conceitos e definições fundamentais ao estudo dos documentos eletrônicos, como é o caso do projeto Interpares".

Nessa perspectiva, surge uma nova abordagem para a análise de documentos digitais, a diplomática digital. Silva e Tognoli (2019) identificam produções acadêmicas de Luciana

Duranti em conjunto com Endicott Popovsky e uma outra com Randy Preston, que abordam a diplomática digital. Silva e Tognoli (2019) investigam as produções acadêmicas e consideram que "a Diplomática Digital é compreendida como uma metodologia advinda de um resultado de pesquisas do Projeto InterPARES que visa analisar a integridade, autenticidade, proveniência dos documentos digitais em sistemas eletrônicos (SILVA; TOGNOLI, 2019, p. 104). Dessa forma, a diplomática se desenvolve ao passo que a produção documental se modifica com a tecnologia.

3.1.2 Elementos de análise diplomática

Primeiramente, é válido frisar que "a origem da diplomática está estritamente ligada à necessidade de apurar a autenticidade dos documentos, com um fim último de averiguar a realidade dos direitos ou veracidade dos fatos nele representados" (DURANTI, 1989, p. 21).

Portanto, a análise diplomática de documentos contemporâneos se torna mais complexa. Isso porque está vinculada à estrutura da forma do documento contemporâneo, que reflete o quão complexo são os sistemas jurídicos cujos documentos são produzidos no presente século (TOGNOLI, 2014).

Na diplomática histórica, alguns elementos são identificados no momento em que é feita a análise diplomática do documento em questão. São levadas em conta as características intrínsecas e extrínsecas. As características intrínsecas são as que estão ligadas ao conteúdo do documento e são elas: protocolo inicial, exposição, preâmbulo, dispositivo, sanção, corroboração e protocolo final (BELLOTTO, 2006, p. 66). Afirma ainda Bellotto (2006) que as formas extrínsecas dos documentos são formais e que não estão ligadas ao teor do documento, mas que estão presentes para garantir a autenticidade e podem ser "[...] marcas de validação, como selos ou outros sinais; as subscrições (assinaturas dos responsáveis pelo documento); o suporte; a escrita; a língua e o estilo" (BELLOTTO, 2006, p. 66).

Em relação ao protocolo inicial, Bellotto (2002, p. 39) detalha os seus elementos, quando diz que

> O protocolo inicial ou protocolo, na sequência dos dados, é constituído por: 1) invocação (*invocatio*) que, em geral, só ocorre nos atos dispositivos mais antigos (a expressão "Em nome de Deus" é um exemplo de invocação); 2) titulação (*intitulatio*), formada pelo nome próprio da autoridade (soberana ou delegada) de que emana o ato e por seus títulos; 3) direção ou endereço (*inscriptio*), parte que nomeia a quem o ato se dirige, seja um destinatário individual ou coletivo e; 4) saudação (*salutatio*), parte final do protocolo.

Em relação ao texto, ou exposição, Bellotto (2002, p. 40) apresenta as suas características sendo:

> 1) preâmbulo (*prologus* ou *exordium*), no qual se justifica (por razões de ordem moral, jurídica ou material) a criação do ato; 2) notificação (*notificatio* ou *promulgatio*), que pode ser entendida na expressão "tenho a honra de comunicar a vós"; 3) exposição (*narratio*), na qual são explicitadas as causas do ato, o que o originou, quais as necessidades administrativas, políticas, jurídicas, econômicas, sociais ou culturais que o tornaram necessário; 4) dispositivo (*dispositio*), que é a substância do ato, seu "assunto" propriamente dito, em que se determina o que se quer (iniciado por um verbo na primeira pessoa, como "ordeno", "mando", "estabeleço", "sou servido ..." etc; 5) sanção (*sanctio* ou *minatio*), na qual se assinalam as penalidades, no caso do não cumprimento do dispositivo e; 6) corroboração ou cláusulas finais (*valoratio* ou *corroboratio*), em que se dispõe sobre os meios morais ou materiais que asseguram a execução do dispositivo (alguns autores classificam essa parte final do texto segundo suas variantes: cominatórias, que podem ser penais ou espirituais, de garantia, de renúncia ou de corroboração).

Por fim, na análise de Bellotto (2002, p. 40-41), as características do protocolo final iniciam-se após a corroboração, ou chamadas de cláusulas finais, sendo:

> 1) subscrição/assinatura (*subscriptio*), isto é, a assinatura do emissor/autor do documento ou quem o faça por sua ordem; 2) datação (*datatio*). É preciso distinguir a data tópica da data cronológica, ou o elemento topográfico do elemento cronológico. A primeira é referente à forma como está designado no documento o local onde ele foi assinado. Aí cabe, muitas vezes, não o nome de uma cidade, e sim a denominação de um palácio, de uma sala ou de um logradouro. Isto deve ser obedecido, sem que se acrescente a cidade na qual estejam situados. A segunda corresponde ao dia, mês e ano; 3) precação (*apprecatio*), onde, por meio de dois elementos (assinatura de testemunhas e sinais de validação, como carimbos e selos), reitera-se a legalidade do documento. Nos atos normativos mais freqüentes, as testemunhas incluem os ministros ou secretários das pastas com as quais têm a ver os assuntos tratados.

Esclarece ainda Bellotto (2002) que nem todas as partes diplomáticas estão presentes de forma padrão nos documentos, pois isso vai depender da espécie documental e da natureza jurídica dos documentos que estão sendo analisados.

O objeto dos modernos estudos da Diplomática é a unidade arquivística elementar, analisada enquanto espécie documental, servindo-se dos seus aspectos formais para definir a natureza jurídica dos atos nela implicados, tanto relativamente à sua produção, como a seus efeitos (CARUCCI, 1987). Concentra-se na gênese, na constituição interna, na transmissão e na relação dos documentos entre seu criador e o seu próprio conteúdo, com a finalidade de identificar, avaliar e demonstrar a sua verdadeira natureza (DURANTI, 1995). Hoje, este é o objetivo da Diplomática, muito mais do que simplesmente a autenticidade formal dos documentos.

A partir da análise diplomática é possível identificar se o documento é íntegro e autêntico. No entanto, a Diplomática Digital leva em conta a análise do documento de arquivo, por meio dos seus metadados. Nesse sentido,

> [...] a diplomática digital, baseada nos princípios da diplomática tradicional, pode subsidiar na identificação de documentos de arquivos digitais por meio de seus metadados e determinar quais metadados são necessários para serem capturados, gerenciados e preservados (ROGERS, 2020, p. 105).

A ação de assinar digitalmente um documento nato digital faz com que um requisito de segurança seja incluído. Dessa forma, é possível dizer que, após a assinatura digital, o documento é considerado íntegro, pois qualquer modificação pode ser detectada com a análise do *hash*, como será abordado adiante. Sobre a integridade, Silva *et al* (2008, p.10), falam que se trata da "proteção contra modificações, duplicação, inserção, remoção ou re-ordenamento de mensagens". Já a autenticidade de um documento, segundo Rondinelli (2005, p. 66),

> [...] está diretamente ligada ao modo, à forma e ao *status* de transmissão desse documento, bem como às condições de sua preservação e custódia. Isso quer dizer que o conceito de autenticidade refere-se à adoção de métodos que garantam que o documento não foi adulterado após a sua criação e que, portanto, continua sendo tão fidedigno quanto era no momento em que foi criado.

Ainda sobre a autenticidade dos documentos eletrônicos, MacNeil (*apud* Rondinelli, 2005, p. 67), diz que "um documento eletrônico arquivístico autêntico é aquele que é transmitido de maneira segura, cujo *status* de transmissão pode ser determinado, que é preservado de maneira segura e cuja proveniência pode ser verificada". Nesse sentido, é possível entender que a autenticidade está diretamente relacionada com os requisitos de segurança do documento e a sua forma de manuseio e transmissão, preservando a sua estrutura e informações, incluindo seus metadados, desde o momento em que foi criado.

A garantia da autenticidade do documento digital parte da cadeia de custódia ininterrupta, que envolve desde o processo produtivo do documento até a guarda permanente para os documentos assim classificados, indo ao encontro do que diz o Modelo OAIS (*Open Archival Information System*) (FLORES, 2016). Destarte, o Conarq (2012), elenca três aspectos importantes relativos à autenticidade dos documentos de arquivo, sendo eles: legal, diplomático e histórico. Com relação a esses aspectos e suas definições, segundo o Conarq (2012, p. 3),

> Legalmente autênticos são aqueles que dão testemunho sobre si mesmos em virtude da intervenção, durante ou após a sua produção, de uma autoridade pública representativa, garantindo sua genuinidade. Documentos diplomaticamente autênticos são aqueles que foram escritos de acordo com a prática do tempo e do lugar indicados no texto e assinados pela pessoa (ou pessoas) competente para produzi-los. Documentos historicamente autênticos são aqueles que atestam eventos que de fato aconteceram ou informações verdadeiras.

O Conarq complementa ainda que os três aspectos de autenticidade são independentes entre si, sendo que um documento pode ser legalmente e historicamente autêntico, mas diplomaticamente não. Ou pode ser diplomaticamente e historicamente autêntico, mas legalmente não (CONARQ 2012).

Nesse sentido, os três tipos de autenticidade podem não ser garantidos pela cadeia de custódia, ou seja, ela não é suficiente para garantir os três tipos de autenticidade elencados pelo Conarq, pois dependem das características anteriormente elencadas, além do seu processo produtivo e no contexto em que estão inseridos.

3.2 ALGORÍTMOS DE RESUMO OU *HASH*

Para que seja possível analisar os documentos contemporâneos, é válido ressaltar que existem documentos em suportes diferentes ao papel, como é o caso do documento digital, que está contido na categoria de documentos eletrônicos. Nesse sentido, Rondinelli (2005, p. 56) considera que "hoje, documentos convencionais e eletrônicos apresentam os mesmos elementos constitutivos dos documentos estudados pelos primeiros diplomatas, sendo apenas um pouco mais elaborados".

O Arquivo Nacional, por meio do Conselho Nacional de Arquivos (Conarq), aprovou a resolução nº 38 de 9 de julho de 2013, que estabelece diretrizes ao produtor sobre a elaboração e manutenção de materiais digitais, mais precisamente aos documentos arquivísticos digitais. Nesse sentido, o Conarq (2013), considerou que pela facilidade a qual os documentos digitais podem ser editados, precisam apresentar fixidez, forma fixa e conteúdo estável. Para o Conarq (2013, p. 6), a fixidez é a "qualidade de um documento arquivístico que assegura a forma fixa e o conteúdo estável". Já a forma fixa é a "qualidade de um documento arquivístico que assegura a mesma aparência ou apresentação documental cada vez que o documento é recuperado". Por fim, a definição de conteúdo estável é a "característica de um documento arquivístico que torna a informação e os dados nele contidos imutáveis e exige que eventuais mudanças sejam feitas por meio de acréscimo de atualizações ou da produção de uma nova versão" (CONARQ, 2013, p. 6).

Nesse sentido, as características elencadas pelo Conarq aos documentos digitais garantem que o documento não sofra mudanças inadvertidamente. Além de fixidez, forma fixa e conteúdo estável, Rondinelli (2005), considera que os documentos eletrônicos arquivísticos possuem os seguintes elementos:

a) Suporte: anteparo que carrega a informação do documento, sendo imprescindível, pois sem ele o documento não existe;

b) Conteúdo: é a mensagem a qual o documento busca transmitir.;

c) Forma (ou estrutura): são as regras de representação do conteúdo contido no documento arquivístico sendo que por meio delas ocorre a manifestação na sua forma física e intelectual;

d) Ação: é a característica central do documento, ou seja, o ato ou a ação que deu origem a sua existência;

e) Pessoas: são as entidades físicas ou jurídicas envolvidas na geração do documento arquivístico;

f) Relação orgânica: é a coexistência com demais documentos em que ele se interrelaciona com os demais;

g) Contexto: é considerado o elemento que se traduz no ambiente na qual a ação geradora do documento ocorre. Esse contexto se subdivide em quatro: jurídico-administrativo, contexto de proveniência, contexto de procedimentos e contexto documentário. (RONDINELLI, 2005).

Outro apontamento relativo aos documentos eletrônicos apontados por Rondinelli (2005, p. 59), diz respeito aos metadados, cujo termo é utilizado pela área de "[...] tecnologia da informação para designar as informações necessárias para dar significado aos dados armazenados num sistema de computador". Rondinelli (2005, p. 60) ainda salienta que "hoje, o conceito de metadado foi totalmente assimilado pela arquivologia, sendo o mesmo considerado elemento fundamental para a garantia da capacidade testemunhal do documento eletrônico arquivístico". Rondinelli (2005, p. 61) ainda traz mais uma contribuição sobre o metadado, dizendo que

> Em termos de análise diplomática, o chamado *perfil do documento* (ou metadado) é considerado uma *anotação* e, portanto, compõe a forma intelectual do documento arquivístico. Trata-se de um conjunto de informações anexadas ao documento eletrônico no momento em que o sistema recebe uma ordem para enviá-lo ou salvá-lo. Seu objetivo é identificar o documento individualmente e estabelecer a sua relação com os demais documentos integrantes do dossiê.

Com o documento digital finalizado, uma característica que não fica visível aos usuários, mas que confere uma identidade ao documento é o chamado *hash* ou algoritmo de resumo do documento. Antes de tratar a respeito do algoritmo de resumo é válido frisar que ele é uma parte da criptografia. Carvalho (2001) considera que a criptografia é a arte e ciência de se estabelecer uma comunicação secreta com a finalidade de tornar uma mensagem

incompreensível para algum adversário que tente interceptá-la. Nesse sentido, Hintzbergen *et al* (2018), apontam que o objetivo maior é tornar uma informação confidencial e mantê-la dessa forma. No construto da criptografia encontramos, como partes integrantes, os criptossistemas, algoritmos criptográficos, chaves criptográficas, criptoanálise e dificuldade computacional. No entanto, abordaremos apenas os conceitos de criptossistemas, algoritmos criptográficos e chaves criptográficas, que de acordo com Silva et al (2008, p. 14) são:

> a) Criptossistemas: técnicas de embaralhamento ou cifragem com o objetivo de, em um sentido, tornar ilegível uma mensagem e, no sentido oposto, ser possível transformá-la novamente em sua mensagem original; b) Algoritmos criptográficos: os criptossistemas têm como base três algoritmos criptográficos: chave secreta, chave pública e resumo. O resumo faz o mapeamento de um texto de tamanho diverso e o transforma em um texto cifrado de tamanho fixo. Os textos de tamanho fixo não possuem chave e recuperar a informação original a partir dele é computacionalmente inviável. O algoritmo de chave secreta utiliza uma chave secreta para cifrar os textos que possuem tamanho fixo. É computacionalmente inviável tentar recuperar o texto a partir do que está cifrado sem a chave secreta e é utilizado para cifrar grandes quantidades de textos. O algoritmo de chaves públicas é similar ao de chave secreta, no entanto o de chaves públicas é composto por um par de chaves, sendo uma pública e outra privada, equivalentes, e consistem na entrega de chaves secretas aos interessados. c) Chaves criptográficas: são valores matemáticos que carregam a função de criptografar textos plenos e poder fazer o sentido inverso, que seria o da recuperação da informação original a partir do texto criptografado. O tamanho das chaves em bits é o que determina o quanto podem ser seguras. A segurança dos criptossistemas está atrelada ao tamanho que as chaves possuem assim como o poder computacional empregado para que sejam quebradas.

As chaves assimétricas, também conhecidas como chaves públicas, consistem em um par de chaves, sendo uma delas pública, distribuída abertamente e outra chave privada que é entregue apenas ao interessado, além disso, esse tipo de chaves assimétricas, ou públicas, é o que possibilita algumas operações, dentre elas a criptografia e a assinatura digital (FERREIRA; ARAÚJO, 2008).

Nesse sentido, o texto produzido no ambiente digital é submetido a processos matemáticos, além de receber a inserção de informações relevantes ao documento que está sendo gerado. O algoritmo de resumo ou *hash* do documento é então um produto gerado a partir de um algoritmo matemático que transforma um texto de tamanho variado em um resumo de tamanho fixo (SILVA et al, 2008).

3.3 VERIFICADORES DE DOCUMENTOS DIGITALMENTE ASSINADOS

Receber um documento digital assinado e visualizar a existência de uma assinatura digital no documento em questão, não é elemento suficiente para identificar a veracidade do documento e da sua assinatura. Com isso os verificadores de documentos digitais têm como objetivo dar validade às assinaturas digitais contidas em seus documentos. Alguns verificadores

se limitam a verificar apenas a qualidade das assinaturas digitais. Outros verificadores, além de verificar as questões da assinatura, também verificam a estrutura do documento.

Os verificadores de documentos digitais assinados podem assumir diferentes funções. A UFSC, ao desenvolver o portal de assinaturas digitais chamado Assina UFSC, disponibilizou um verificador de assinaturas. No entanto, esse documento só faz a verificação da qualidade das assinaturas. O portal esclarece que:

> O verificador de assinaturas digitais identifica automaticamente assinaturas realizadas com Certificados Digitais de cadeias de certificação reconhecidas pela UFSC, conforme portaria normativa 276/GR/2019 e legislações vigentes (ICP-Brasil, ICP-Edu e GOV.BR). Aceitar ou não o documento assinado, compete àquele cuja responsabilidade é de confirmar se a assinatura digital encontrada pelo verificador corresponde de fato ao signatário envolvido no texto do documento. O Verificador de Assinaturas Digitais não analisa o teor ou o texto dos documentos (UFSC, 2022, s.p).

Já o verificador do Instituto Nacional de Tecnologia da Informação (ITI) tem como objetivo verificar a conformidade das assinaturas e do documento de acordo com o DOC ICP-15 do ITI. O DOC ICP-15 "faz parte de um conjunto de normativos criados para regulamentar a geração e verificação de assinaturas digitais no âmbito da ICP-Brasil" (ITI, 2021, s.p.). Segundo o ITI (2021, p. 15), "toda assinatura digital ICP-Brasil deve ser passível de validação". Segue ainda o ITI (2021, p. 15), afirmando que,

> [...] para verificar a validade de uma assinatura digital ICP-Brasil o verificador deve utilizar: a) o documento eletrônico para o qual a assinatura digital ICP-Brasil foi criada; b) a assinatura digital ICP-Brasil do documento eletrônico; c) o certificado digital do signatário e sua correspondente cadeia de certificação; d) os status de revogação referentes aos certificados dos caminhos de certificação do usuário e, quando houver carimbo do tempo, da ACT; e) a política de assinatura, cujo identificador encontra-se na assinatura digital ICP-Brasil; f) um dos algoritmos definidos no DOC-ICP-01.01 [2].

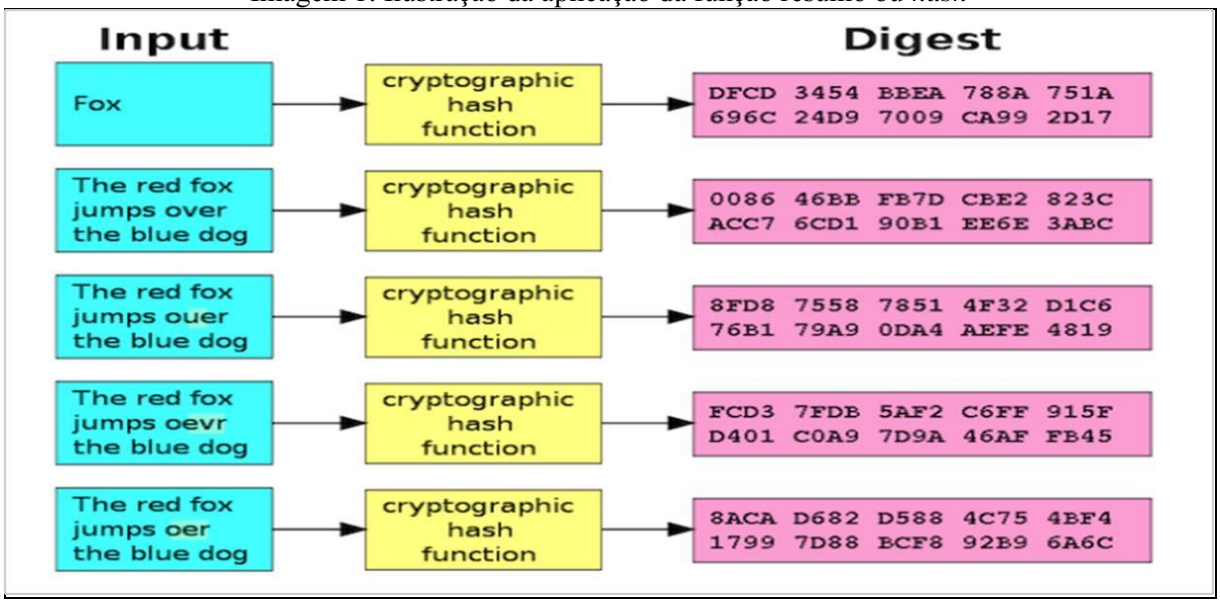
O DOC-ICP-01.01 regulamenta os algoritmos e parâmetros criptográficos utilizados na ICP-Brasil, incluindo, "a) geração de chaves criptográficas; b) solicitação, emissão e revogação de certificados digitais; c) geração e verificação de assinaturas digitais; d) cifração de mensagens; e) autenticação com certificados digitais" (ITI, 2019, p. 6). Nesse sentido, o DOC-ICP-01.01 define as características mínimas necessárias relativas no que tange às técnicas criptográficas adotadas na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

4 ANÁLISE DOS RESULTADOS

Verificou-se que os documentos arquivísticos digitais são produzidos de diversas formas, normalmente por meio de editores de texto, em formatos variados. Pode-se dizer que possuem uma espécie de identidade, como uma impressão digital biométrica. Essa identidade é conferida por meio da função resumo, ou *hash* documental. Cada documento digital possui um

hash que o identifica. Como nos informam Silva *et al* (2008), a função resumo ou *hash* faz a transformação de um documento de tamanho variado em um resumo de tamanho fixo. É possível visualizar seu funcionamento na ilustração abaixo:

Imagem 1: Ilustração da aplicação da função resumo ou *hash*



Fonte: Kapersky Daily (2022).

Na imagem que ilustra a aplicação do *hash*, podemos verificar que um texto qualquer de tamanho variável é identificado pelo sistema no *input*. Em seguida, é aplicada a função criptográfica no texto, de forma que ele produza uma identidade, ou seja, o *hash* documental, que podemos identificá-lo na coluna *digest*. A coluna *digest* é o resultado da aplicação criptográfica do texto de tamanho variável, em um texto de tamanho fixo.

Ao analisar a imagem percebe-se que o resumo documental ou *hash* não se limita ao tamanho do texto. Mesmo em um texto curto é possível identificar o *hash* em um tamanho fixo. Outro ponto que fica evidente é a alteração substancial da função resumo quando o texto sofre a alteração de um único caractere, onde o *hash* documental mudou de forma considerável, não identificando similaridade com o anterior.

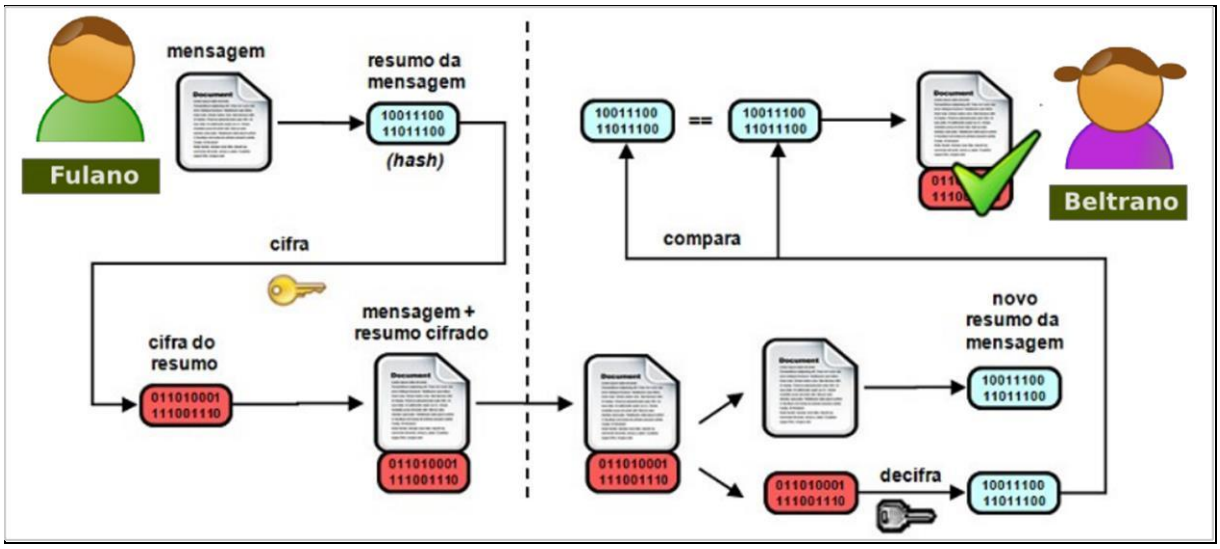
Partindo para a assinatura digital dos documentos nato digitais, é importante compreender que o *hash* é utilizado em combinação com a chave privada do certificado digital de quem deseja assinar o documento. Reforça-se a teoria de que o certificado digital é composto de um par de chaves assimétricas, sendo uma chave pública de domínio público e outra privada de domínio exclusivo do usuário, diferentes entre si, mas matematicamente equivalentes (FERREIRA; ARAÚJO, 2008).

Dessa forma, no momento em que um documento for assinado digitalmente, o sistema utiliza o *hash* do documento digital e o submete à cifragem utilizando a chave privada do usuário que é de domínio exclusivo desse usuário. Feita a cifragem do *hash*, é obtida uma nova função resumo criptografada com a chave privada do usuário. Esse resumo criptografado acompanha o documento original em seus metadados. Quando o destinatário desse documento recebe o arquivo, poderá submetê-lo a um verificador de assinaturas. Nesse momento, o sistema procederá da seguinte forma:

a) Executa a separação do texto do documento e do *hash* cifrado;
b) Extrai o *hash* do documento que deve ser igual ao original antes da cifragem;
c) Decifra o *hash* que acompanhou o documento, utilizando a chave pública do usuário, extraindo o *hash* original;
d) Compara os *hashes* obtidos da extração do texto e o da decifragem;
e) Apresenta resultados sobre a validade documental.

A integridade das informações do documento deverá ser validada pelo sistema, que vai apresentar a informação dizendo se o documento está válido ou se foi corrompido. Lembrando que qualquer alteração no documento, após a assinatura, altera substancialmente o seu *hash*. A imagem a seguir apresenta a forma como o sistema processa a assinatura e como faz a análise:

Imagem 2: Processo de assinatura digital



Fonte: VALCY (2017, p. 18).

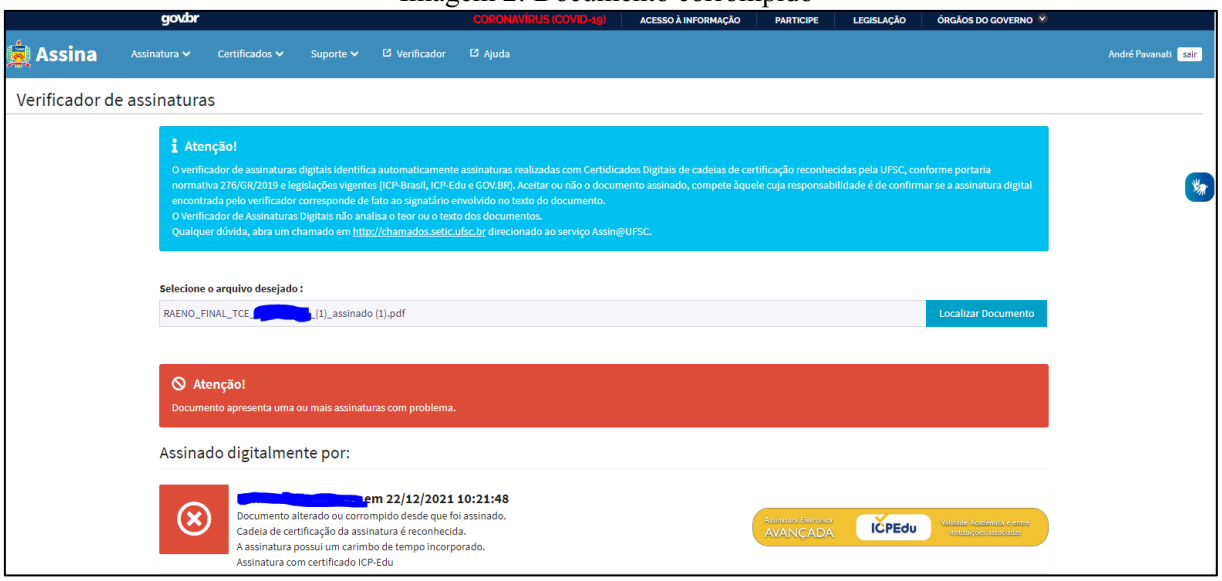
Na UFSC, o portal Assina UFSC é uma ferramenta que foi desenvolvida para a assinatura de documentos digitais, com o objetivo de dar integridade aos documentos nato digitais. Isso porque, assina digitalmente os documentos utilizando certificados digitais assimétricos (par de chaves pública e privada). Tais assinaturas nos documentos digitais, assim

como funcionam nos documentos em papel, são a manifestação de vontade do autor do documento. No Assina UFSC também está disponível aos usuários um verificador de assinaturas. Esse verificador busca apresentar a validade do documento tanto da sua assinatura, quanto se o documento carrega a qualidade da integridade, ou seja, se não sofreu alterações no meio em que foi transmitido.

Na análise da assinatura digital o sistema faz a verificação do documento com base na avaliação e comparação do *hash* documental, conforme explicado anteriormente. Com isso, é possível identificar se o documento possui as qualidades e informações da sua elaboração no momento em que foi assinado.

A seguir serão apresentados dois exemplos, onde um documento sofreu alteração em alguma de suas informações e, em seguida, um documento que se apresenta íntegro:

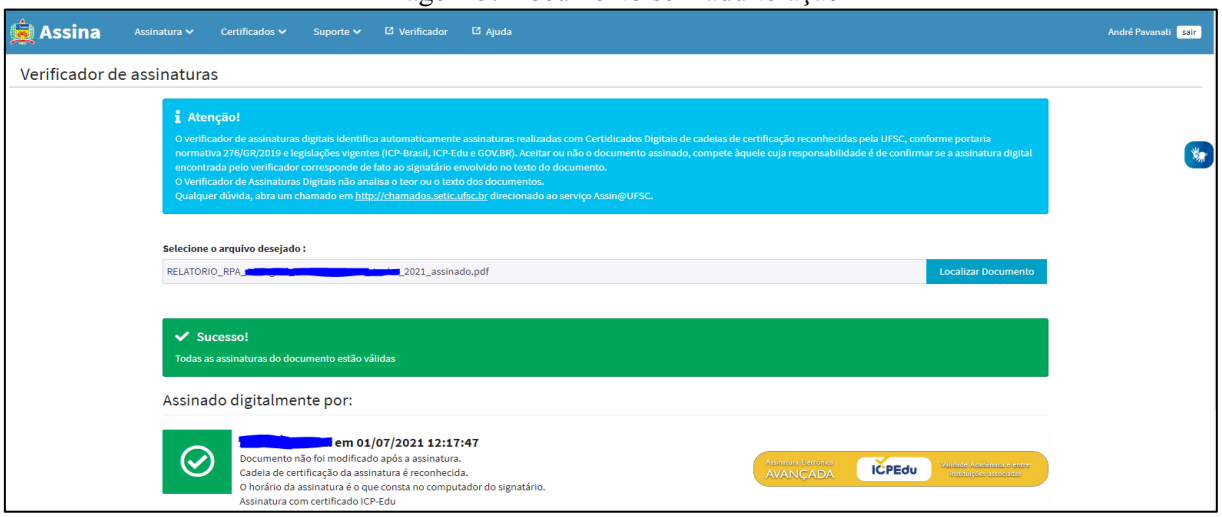
Imagem 2: Documento corrompido



Fonte: Extraído do verificador do Assina UFSC (2022)

Na imagem anterior, o sistema fez o procedimento de separação do texto do documento e do *hash* cifrado, extraindo novo *hash* do texto (que deve ser igual ao extraído originalmente), e fez a decifragem do *hash* cifrado que acompanhou o documento, utilizando a chave pública embarcada no PDF. Após fazer a comparação dos *hashes* o sistema identificou que eles eram diferentes entre si, ou seja, o sistema identifica que houve alteração em alguma das informações do documento desde que ele foi assinado, portanto, trata-se de um documento adulterado. Em seguida, será apresentado um documento sem alterações:

Imagem 3: Documento sem adulteração



Fonte: Extraído do verificador do Assina UFSC (2022).

Recordando a lógica do sistema de verificação, para que se chegasse a esses resultados, as funções resumo ou *hash* passaram pelo processo de cifragem, decifragem e comparação, de forma que o sistema pudesse identificar a sua integridade.

A verificação das assinaturas dentro da diplomática traz uma reflexão, Rondinelli (2013) aborda, quanto aos documentos digitais, que "[...] um documento dessa natureza implica necessariamente ação, contexto, pessoas, inter-relacionamento (relação orgânica), forma fixa e conteúdo estável" (RONDINELLI, 2013, p. 244-245). Segue ainda a reflexão de Rondinelli (2013), onde a autora diz que "deve-se perguntar como, de fato, as características de forma fixa e conteúdo estável, as quais, do ponto de vista da diplomática, são consideradas essenciais, se aplicam aos documentos arquivísticos digitais" (RONDINELLI, 2013, p. 245). Dessa forma, apesar dos documentos digitais serem um conjunto de bits que serão processados e lidos por um sistema, composto por uma infraestrutura de hardware e software, são os metadados que serão responsáveis por dar a forma fixa e fixidez do documento apresentado em tela, assim como a sua autoria, data de produção, software produtor, hash documental, cifragem documental, dentre outras informações que sejam relevantes para a recuperação, processamento e apresentação do documento na forma que ele foi definitivamente produzido, para a análise diplomática.

Apesar da análise diplomática aplicada à produção documental, Bellotto (2006) considera que a gênese documental, assim como a tipologia documental são o cerne do entendimento e da motivação pela qual o documento foi criado e estruturado no momento da sua produção. Como se encarrega da estrutura documental, significa que os elementos tais como protocolo inicial, texto e protocolo final são objetos de análise. No entanto, a forma fixa,

conteúdo estável e fixidez documental são garantidos nos documentos digitais por meio dos seus metadados, como citado anteriormente. Esses metadados, no momento da assinatura digital e cifragem do hash, garantem que o documento não seja alterado após sua gênese definitiva.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa buscou identificar a integridade e autenticidade dos documentos natos digitais, utilizando como base elementos da diplomática tradicional e da diplomática digital ou contemporânea. Além da análise dos elementos intrínsecos e extrínsecos, foi possível observar que, nos documentos natos digitais, os elementos que dão sustentabilidade aos documentos estão vinculados aos seus metadados, de forma que funcionem como um conjunto de regras para a visualização documental por meio da infraestrutura de hardware e também do software, envolvidos na apresentação documental. Além disso, o *hash* documental em conjunto com os algoritmos criptográficos, associados à assinatura digital, se apresenta como um elemento de análise de integridade documental e, também de autenticidade, visto que é possível identificar adulterações que tenham ocorrido no documento após a sua assinatura, seja logo após a produção, seja no meio de transmissão. Nesse sentido, o *hash* documental pode ser utilizado como um elemento de análise da diplomática digital, por apresentar características suficientemente robustas para identificar a adulteração documental, visto que a alteração de um único caractere no texto faz com que a composição do *hash* seja substancialmente modificada.

Nesse sentido, os verificadores de assinatura de documentos natos digitais se apresentam como uma ferramenta que busca auxiliar a identificação da adulteração documental, visto que ele mesmo faz a análise dos metadados do documento no que se refere ao *hash* e à decifragem do mesmo, com base no texto original.

Essa discussão se faz relevante para que, frente à crescente produção de documentos natos digitais, a classe arquivística possa se munir de ferramentas de análise, buscando validar somente os documentos que sejam íntegros e autênticos. Receber um documento digitalmente assinado e visualizá-lo em um PDF como documento assinado não é o suficiente para considera-lo válido, íntegro ou verdadeiro. Com isso, acredita-se que a presente pesquisa possa colaborar para as análises de documentos natos digitais com assinaturas eletrônicas de chaves públicas.

Nesse caso, verificar as assinaturas não é somente saber se foi aquela pessoa que assinou como era no papel. A verificação de assinaturas em documentos digitais traz outras confirmações: se o texto foi alterado ou se algo foi inserido ou suprimido após a sua assinatura.

No entanto, a verificação do documento por meio do verificador de assinaturas, garante apenas a informação de integridade e autenticidade documental ou se o documento sofreu alguma alteração após a assinatura. Nesse sentido, não garante se o documento foi produzido com informação verdadeira ou falsa. Portanto, os documentos que refletem a realidade, de acordo com o acontecimento natural dos fatos, podem ter a sua integridade e autenticidade garantidas. Dessa forma, essas qualidades trazem revoluções no contexto da Arquivologia e da Diplomática Digital.

Como recomendação para pesquisas futuras, outras análises podem ser realizadas, há um longo caminho a ser explorado pelos arquivistas nessa área no Brasil, que conforme observado, ainda possui poucas produções. Há de mencionar ainda, trabalhos como o apresentado aqui de Corinne Rogers (2020) da University of British Columbia, que traz contribuições para a Diplomática Digital, trazendo análises da camada conceitual, lógica e física dos documentos digitais, que poderão também ser explorados por pesquisadores brasileiros. Além disso, com relação à autenticidade do documento digital, pesquisas mais aprofundadas podem ser realizadas com outras tecnologias disponíveis como, por exemplo, o blockchain, que pode ser capaz de aumentar a rastreabilidade fortalecendo a segurança e confiança da informação.

Por fim, é válido frisar que os arquivistas podem não conseguir impedir adulterações documentais, mas podem ajudar a identificá-las e esta pesquisa buscou apresentar uma das formas possíveis para isso.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO 32000-1**: gerenciamento de documentos – portable document format – Part 1: PDF 1.7. Rio de Janeiro. 2019.

BELLOTTO, Heloísa Liberalli. **Como fazer análise diplomática e análise tipológica de documento de arquivo**. São Paulo: Arquivo do Estado: Imprensa Oficial, 2002.

_____. Arquivos permanentes: tratamento documental. 4 ed. Rio de Janeiro: Editora FGV. 2006.

CARVALHO, Daniel Balparda de. **Segurança de dados com criptografia**: métodos e algoritmos. 2 ed. Rio de Janeiro: Book Express, 2001.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Glossário Documentos Arquivísticos Digitais**. Câmara Técnica de Documentos Eletrônicos. 8 ed. 2020. Disponível em:

<https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf>. Acesso em: 06 fev. 2022.

_____. A elaboração e a manutenção de materiais digitais: diretrizes para indivíduos. **Diretrizes do Produtor**. 2013. Disponível em: <https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_diretrizes_produtor_preservador_resolucao_38.pdf>. Acesso em: 02 mar. 2022.

DURANTI, Luciana. **Diplomatics**: new uses for an old Science, Part I. Archivaria. Canadá, n.28, p. 7-27. 1989. Disponível em: <https://archivaria.ca/index.php/archivaria/article/view/11567/12513>. Acesso em: 03 fev. 2022.

_____. Diplomática: **novos usos para uma antiga ciência**. Tradução de Lara Monteiro. Revista de fontes, v. 07, n. 13. Guarulhos, 2020. Disponível em: <https://periodicos.unifesp.br/index.php/fontes/article/view/11968/8430>. Acesso em: 23 fev. 2022.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação**: guia prático para elaboração e implementação. Rio de Janeiro: Editora Ciência Moderna Ltda. 2008.

FLORES, D.; ROCCO, B. C. B.; SANTOS, H. M. D. **Cadeia de custódia para documentos arquivísticos digitais**. Acervo - Revista do Arquivo Nacional, v. 29, n. 2, p. 117-132, 2016. Disponível em: <http://hdl.handle.net/20.500.11959/brapci/40511>. Acesso em: 22 jun. 2022.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6 ed. São Paulo: Editora Atlas. 2008.

GODOY, Arilda Schmidt. **Introdução à pesquisa qualitativa e suas possibilidades**. RAE - Revista de Administração de Empresas, São Paulo, v. 35, n. 2, p. 57-63, 1995.

HAIR JÚNIOR, J. F. et al. **Fundamentos de métodos de pesquisa em administração**. Porto Alegre: Bookman, 2005.

HINTZBERGEN, Jule et al.**Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

HOOKER, J. T. **Lendo o passado - do cuneiforme ao alfabeto**: a história da escrita antiga. São Paulo: Melhoramentos, 1996. 473 p.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Padrões e algoritmos criptográficos da ICP-Brasil**: DOC ICP-01.01 – Versão 4.2. 2019. Disponível em: <https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-01-01-v-4-2-padroes-e-algoritmos-criptograficos-da-icp-brasil-copy-pdf>. Acesso em: 25 fev. 2022.

_____. **Requisitos para geração e verificação de assinaturas digitais na ICP-Brasil**: DOC-ICP-15.01 – Versão 4.0. 2021. Disponível em: <https://www.gov.br/iti/pt-

br/assuntos/legislacao/instrucoes-normativas/IN012021_DOC_15.01_assinada.pdf>. Acesso em: 25 fev. 2022.

MACNEIL, Heather. **Trusting records**: legal, historical and diplomatic perspectives. Dordrecht, Kluwer Academic, 2000 *apud* RONDINELLI, Rosely Curi. 2005.

MOUTINHO, Célia. O tempo da máquina de escrever: sobre a coleção de máquinas de escrever da Caixa Geral de Depósitos. **Gabinete do Patrimônio Histórico da Caixa Geral de Depósitos**. Caixa Geral de Depósitos. Lisboa, 2011. Disponível em: <https://www.cgd.pt/Institucional/Patrimonio-Historico-CGD/Estudos/Documents/Maquinas-de-escrever.pdf>. Acesso em: 13 dez. 2021.

ROESCH, Sylvia Maria Azevedo. **Projetos de estágio e de pesquisa em administração**: guia para estágios, trabalhos de conclusão, dissertações e estudos de caso. 2. ed. São Paulo: Editora Atlas, 1999.

ROGERS, Corinne. **Diplomática de documentos nato digitais**: a consideração da forma documental no ambiente digital. Tradução: Juan Bernardo Montoya Mogollón. São Paulo: Revista do arquivo, ano v, nº 10, p. 93-108, 2020. Disponível em: <http://www.arquivoestado.sp.gov.br/revista_do_arquivo/10/pdf/versao.pdf>. Acesso em: 22 jun. 2022.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos**. 4.ed. Rio de Janeiro: Editora FGV, 2005.

ROUSSEAU, Jean-Yves; COUTURE, Carol. Introdução e Cap. 1 Os arquivos, os arquivistas e a arquivística. Considerações históricas. In: **Os fundamentos da disciplina arquivística**. Lisboa: Publicações Dom Quixote, 1998. p.23-42.

SILVA, L. G. C. da et al. **Certificação digital**: conceitos e aplicações. Rio de Janeiro: Ciência Moderna, 2008.

SILVA, Anelise Barbosa da; TOGNOLI, Natália Bolfarini. Diplomática digital: uma nova abordagem? In: BARROS, Thiago Henrique Bragato; SANTOS JÚNIOR, Roberto Lopes dos; CÂNDIDO, Gilberto Gomes (org.). **A pesquisa e o ensino da Arquivologia**: perspectivas na era digital. Belém: Editora da UFPA. 2019.

TOGNOLI, Natália Bolfarini. **A Construção Teórica da Diplomática**: Em busca da sistematização de seus marcos teóricos como subsídio aos estudos arquivísticos. São Paulo: Editora UNESP, 2014.

TRIVIÑOS, A. N. S. **Introdução a pesquisa em ciências sociais**: a pesquisa qualitativa em educação. 1. ed. 20. reimpr. São Paulo: Atlas, 2011.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. **E-UFSC**: Portal de serviços digitais. 2022. Disponível em: < https://e.ufsc.br/>. Acesso em: 01 mar. 2022.

VALCY, Italo. **Entendendo a criptografia e como ela pode ser usada na prática.** Superitendência de Tecnologia da Informação. UFBA, 2017. Disponível em:

<https://eventos.rnp.br/sites/default/files/activity/activity-presentation/palestra_01_disi17_italovalcy.pdf>. Acesso em: 18 maio 2022.

VALENTIM, Raquel Torrão. **A diplomática digital e a ciência forense digital**: aspectos convergentes e divergentes entre disciplinas. Niteói: UFF, 2020. Disponível em: <https://app.uff.br/riuff/bitstream/handle/1/22801/TCC%20Raquel%20Torr%c3%a3o.pdf?sequence=3&isAllowed=y>. Acesso em 22 jun. 2022.

VERGARA, Sylvia Constant. **Métodos de pesquisa em Administração**. 5. Ed. São Paulo: Atlas, 2012.