XXII Encontro Nacional de Pesquisa em Ciência da Informação – XXII ENANCIB

ISSN 2177-3688

GT- 8 – Informação e Tecnologia

O USO DAS ASSINATURAS DIGITAIS PARA AUTENTICAÇÃO DOS REPRESENTANTES DIGITAIS: GARANTIAS LEGAIS A PARTIR DAS PRÁTICAS ARQUIVÍSTICAS.

THE USE OF DIGITAL SIGNATURES FOR AUTHENTICATION OF DIGITAL REPRESENTATIVES: LEGAL GUARANTEES BASED ON ARCHIVISTICAL PRACTICES.

Dalton Garcia do Darmo. UFMG.

Cintia Aparecida Chagas. UFMG.

Modalidade: Resumo Expandido

Resumo: É cada vez mais comum a necessidade das assinaturas digitais para as pessoas físicas e jurídicas, devido à crescente disponibilidade de serviços informatizados, à transformação digital dos órgãos públicos e ao respaldo legal concedido ao processo de digitalização para substituição e, consequentemente, ao representante digital. No entanto, quanto à utilização das assinaturas digitais, existe um problema relacionado à distinção entre os conceitos de autenticação e autenticidade de documentos digitalizados, que afeta diretamente a segurança e a preservação da informação. O objetivo deste trabalho é entender as características técnicas das assinaturas digitais e como garantir a presunção de autenticidade e a validade jurídica para os documentos digitais a partir da teoria arquivística. Esta pesquisa é qualitativa e foi desenvolvida por meio de pesquisa bibliográfica e documental. Os resultados obtidos podem contribuir para o aperfeiçoamento das interações realizadas com a utilização de assinatura digital, distinguindo autenticação de autenticidade e garantindo a integridade e confiabilidade dos representantes digitais e do processo realizado, com o subsídio de sistemas informatizados de gestão arquivística. Observa-se, que a teoria arquivística contribui efetivamente com os procedimentos realizados no ambiente digital, amparando o cumprimento da legislação e a preservação da informação.

Palavras-Chave: Assinatura Digital. Representante Digital. Digitalização para Substituição.

Abstract: *There is an increasing need for digital signatures for individuals and legal entities, due to the increasing availability of computerized services, the digital transformation of public bodies and the legal support given to the common process of digitization for replacement and, respectively, to the digital representative. However, regarding the use of digital signatures, there is a problem related to the distinction between the concepts of authentication and authenticity of digitized documents, which directly affects the security and preservation of information. The objective of this work is to understand the technical characteristics of digital signatures and how to guarantee the presumption of authenticity and legal validity for digital documents based on archival theory. This research is qualitative and was developed through bibliographic and documentary research. The results obtained can contribute to the improvement of the interactions carried out with the use of digital signatures, distinguishing authentication from authenticity and guaranteeing the integrity and reliability of the digital representatives and the process carried out, with the support of computerized archival management*

systems. It is observed that the archival theory effectively contributes to the procedures carried out in the digital environment, supporting compliance with legislation and the preservation of information.

***Keywords*:** *Digital Signature. Digital Representative. Scan for Replacement.*

1 INTRODUÇÃO

Impulsionada pelas inovações da Tecnologias Digitais de Informação e Comunicação (TDIC), a digitalização para substituição está sendo adotada por instituições públicas e privadas com a justificativa de "desburocratização" e melhor eficiência dos processos internos. Em relação aos órgãos públicos, toda uma base legal está sendo constituída desde a Medida Provisória 2.200-2, de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP- Brasil) com o objetivo de garantir a autenticidade, integridade e validade jurídica dos documentos, das aplicações de suporte habilitadas e para a realização de transações eletrônicas. Em 2020, a Lei nº 14.063[1], consentiu a utilização das assinaturas digitais em interações com entes públicos.

As assinaturas digitais são adotadas para autenticação de prontuários médicos eletrônicos por meio de certificação digital[2], para a prescrição médica[3], no projeto do Assentamento Funcional Digital - AFD[4], na conversão para o meio digital dos documentos que compõem o acervo acadêmico[5], para digitalização de documentos relativos a transações de instituições financeiras[6], além de validar documentos e atos processuais digitalizados em

[1] BRASIL, Lei Nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

[2] BRASIL, Lei Nº13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

[3] CONSELHO FEDERAL DE MEDICINA (BRASIL). Resolução CFM Nº 2.299, de 30 de setembro de 2021. Regulamenta, disciplina e normatiza a emissão de documentos médicos eletrônicos.

[4] BRASIL. Ministério do Planejamento, Gestão e Pessoas. Secretaria de Gestão de Pessoas. Portaria nº 9, de 1 de agosto de 2018. Dispõe sobre a criação do Assentamento Funcional Digital – AFD.2018.

[5] BRASIL. Ministério da Educação. Portaria nº 315, de 4 de abril de 2018. Dispõe sobre os procedimentos de supervisão e monitoramento de instituições de educação superior integrantes do sistema federal de ensino e de cursos superiores de graduação e de pós-graduação lato sensu, nas modalidades presencial e a distância.2018.

[6] BRASIL. Ministério da Fazenda. Banco Central do Brasil. Resolução nº 4.474, de 31 de março de 2016. Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente.

instituições públicas[7] e na tramitação de processos judiciais em sistemas informatizados[8], e na produção de representantes digitais para o documento original[9] no suporte papel, sem valor permanente, facultando neste último caso a eliminação do original. Dessa forma, a digitalização de substituição subsidiada somente pela utilização da assinatura digital pode levar à perda de informação e a prejuízos imensuráveis para toda a sociedade.

A proposta deste trabalho é distinguir os termos autenticação e autenticidade, caracterizar os padrões e tipos de assinaturas digitais existentes e os procedimentos para a presunção de autenticidade a partir dos conceitos arquivísticos. Por meio de pesquisa bibliográfica e documental, propõe-se de uma forma exploratória, apresentar maiores características de uma assinatura digital e os atributos relacionados a esta, em especial as normativas e procedimentos da ICP-Brasil.

2 AUTENTICAÇÃO E AUTENTICIDADE

Por vezes, a assinatura digital é apresentada como mecanismo suficiente para a garantia de autenticidade de um documento. Para a Arquivologia e para a Diplomática é possível aferir apenas a autoria e a integridade do documento a partir dessa ferramenta, tornando-se necessários a adoção do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos (SIGAD), de repositório arquivístico digital confiável (RDC-Arq) e a inclusão de metadados para garantir a autenticidade, gestão e preservação do documento digitalizado.

Dessa forma, conforme o e-ARQ Brasil (CONARQ, 2022), autenticação é a:

> Declaração de que um documento original é autêntico – ou que uma cópia reproduz fielmente o original – feita por uma pessoa jurídica com autoridade para tal (servidor público, notário, autoridade certificadora) num determinado momento, por meio da adição de elementos ou afirmações. (CONARQ, 2022).

---

[7] BRASIL. Lei Nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017.

[8] BRASIL. Lei Nº 11.419, de 19 de dezembro de 2016. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

[9] BRASIL. Decreto Nº 10.278, de 18 de março de 2020. Regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais.

Por sua vez, a autenticidade é a:

> Credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção. A autenticidade é composta de identidade e integridade. [...] identidade e integridade são constatadas à luz do contexto (jurídico-administrativo, de proveniência, de procedimentos, documental e tecnológico) no qual o documento arquivístico foi produzido e usado ao longo do tempo (CONARQ, 2022).

Como visto, uma assinatura digital afere autenticação ao documento. Observa-se, ainda, que uma assinatura digital é adicionada ao documento sem alterar a informação nele contida, por meio da criptografia[10].

3 ASSINATURA ELETRÔNICA OU ASSINATURA DIGITAL?

Segundo a Lei nº 14.063/2020, assinatura eletrônica são dados em formato eletrônico que se ligam ou estão logicamente associados a outros dados em formato eletrônico e que são utilizados pelo signatário para assinar, observados os níveis de assinaturas apropriados para os atos previstos na referida lei, sendo classificadas e caracterizadas como:

- Assinatura eletrônica simples: os registros e controles são normatizados pela entidade que mantém o sistema. Não requer certificado. Utilizável em situações de baixo risco, devido à alta probabilidade de fraude. Exemplos: acesso via cadastro de usuário e senha e IP de rede.
- Assinatura eletrônica avançada: utiliza certificados não emitidos pela ICP-Brasil ou outro meio de comprovação da autoria e da integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. Possui baixo risco de fraude. São exemplos: a biometria, as senhas, os certificados corporativos, o pix e o *pin*[11].
- Assinatura eletrônica qualificada: a que utiliza certificado digital, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Garante a integridade e autoria do documento. Possui nível alto de segurança, pois faz o uso de certificado digital e da assinatura digital, ou seja, de criptografia nas transações (chave privada e chave pública).

[10] Método de codificação de dados segundo algoritmo específico e chave secreta, de forma que somente os usuários autorizados possam restabelecer sua forma original (CONARQ, 2022).
[11] *Personal identificator number* ou Número de identificação pessoal.

Por sua vez, a assinatura digital é uma assinatura eletrônica, do tipo avançada ou qualificada, associada a um par de chaves criptográficas e a certificados digitais. O Glossário ICP-Brasil (BRASIL, 2020), define assinatura digital como:

> Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um e mail ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente.

Para o e-ARQ Brasil (CONARQ, 2022), a assinatura digital permite aferir a origem e a integridade do documento, deve ser única para cada documento, comprovar a autoria e assegurar ao destinatário o "não repúdio" do documento digital, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura.

Destaca-se que em virtude de acordos internacionais, parceria entre países e por manifestação e vontade das partes, as assinaturas eletrônicas qualificadas não emitidas pela ICP-Brasil devem ser reconhecidas. Segundo o portal Consultor Jurídico (2021), é importante nesta situação garantir a identidade dos signatários e os requisitos da Lei nº 14.063/2020. A Para a Adobe (2022), ainda que os países possuam leis diferentes, três princípios básicos garantem validade legal da assinatura eletrônica: a autenticação do signatário, a intenção e o consentimento, e a prova final evidenciado que um documento foi assinado e quem assinou.

4 ASSINATURA DIGITAL: PADRÕES E PERFIS

Neste estudo, será considerado como assinatura digital o conceito normatizado pela ICP-Brasil. Atualmente, existem disponíveis três padrões de assinaturas digitais, conforme apresentado nos requisitos das políticas de assinatura digital na ICP-Brasil (ITI, 2021):

- CMS *Advanced Electronic Signatures* (CAdES): É usado para descrever estrutura para armazenamento de conteúdos assinados digitalmente, em formato *Abstract Syntax Notation One*[12] (ASN1). Aplica-se principalmente a documentos binários.

[12] Notação de Sintaxe Abstrata: Padrão de linguagem para estruturas de dados que representam, codificam, decodificam e transmitem dados. Eles encapsulam um conjunto de regras formais que descrevem a estrutura dos objetos, independentemente de um mecanismo de codificação específico da máquina. Também remove ambiguidades. *ETSI. ASN.1 Format for Signature Policies. Number TR* 102 272. v.1.1.1, dez. 2003.

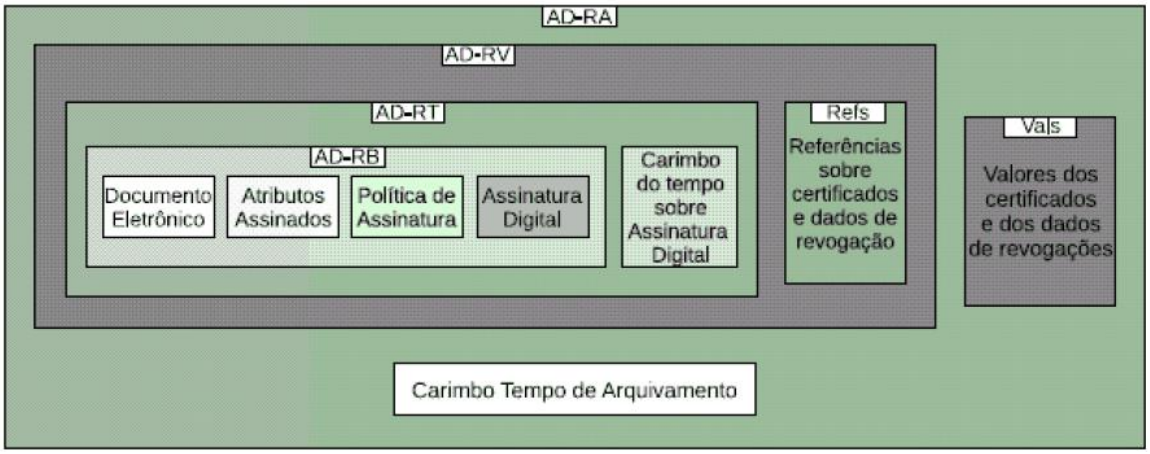
- XML *Advanced Electronic Signatures* (XAdES): É usado para descrever estrutura para armazenamento de conteúdos assinados digitalmente, em formato XML. Permite assinatura parcial do documento digital.
- PDF *Advanced Electronic Signatures* (PAdES): O PAdES é um padrão internacional de assinatura digital aceito pela ICP-Brasil que permite a representação visual das assinaturas nos próprios documentos em formato PDF.

A partir dos três padrões supracitados, as assinaturas digitais são criadas de acordo com a sua finalidade e longevidade esperada. Devido à adição de atributos específicos e para maximizar a interoperabilidade entre uma comunidade, foram estabelecidos os seguintes perfis ou formatos de assinatura digital, conforme explica BRY (2022):

- Assinatura Digital - Referência Básica (AD-RB): Assinatura simples e de curto prazo. Verifica os dados da assinatura e a sequência de código.
- Assinatura Digital – Referência de Tempo (AD-RT): Possui as características da AD-RB e um Carimbo do Tempo, que garante uma referência temporal segura e a longo prazo.
- Assinatura Digital – Referência para Validação (AD-RV) (* exceto para *PAdES):* Verifica todas as informações para validar uma assinatura e possui referência de tempo, da cadeia de certificação, assim como referências de revogação (Listas de Certificados Revogados – LCR ou respostas de Online Certificate Status Protocol – OCSP).
- Assinatura Digital – Referências Completas – (AD-RC): Os artefatos necessários para a validação da assinatura são incluídos no pacote de assinatura, viabilizando a sua verificação mesmo que alguns artefatos não estejam mais disponíveis online.
- Assinatura Digital – Referências para Arquivamento – (AD-RA): Conserva uma assinatura por anos ou décadas. Permite adicionar carimbos de tempo periodicamente para proteger a assinatura contra o enfraquecimento dos algoritmos utilizados.

A figura abaixo demonstra a disposição dos formatos das assinaturas digitais:

Figura 1 - AD com referência para arquivamento AD-RA



Fonte: Extraído de Hirata (2015, p. 11).

Para fins de auditoria e rastreabilidade, os processos de geração e verificação de assinatura digital devem possibilitar a realização, visualização e armazenamento de registros eletrônicos ou *logs* de suas atividades. Ressalta-se que a assinatura digital possui um ciclo de vida que compreende o processo de criação, a verificação ou validação, o armazenamento e a sua revalidação, conforme a ICP-Brasil (ITI, 2021b).

5 CERTIFICADO DIGITAL

Certificado digital é um registro eletrônico assinado, gerado por meio de um procedimento de certificação digital, que se destina a comprovar a relação existente entre um elemento criptográfico e uma pessoa física ou jurídica. O certificado digital contém diversas informações do proprietário – nome, CPF/CNPJ, e-mail e dados biométricos, e serve para confirmar, de forma inequívoca, a identidade de seu portador (BRY,2022).

Essas informações são atreladas a um par de chaves criptográficas individuais, geradas aleatoriamente por funções matemáticas (função *hash*). Uma delas é denominada chave privada e fica sob posse do proprietário, a outra é uma chave pública, que serve para verificação em bases de dados. Tanto a assinatura digital quanto o documento digital são protegidos por criptografia pelo certificado digital.

Os certificados digitais podem ser de vários tipos, sendo os mais comuns: A – certificado de assinatura digital (A1, A3 e A4); S – certificado de sigilo/confidencialidade (S1, S3 e S4); e T – certificado de tempo (*timestamp*[13]) (T3), que além de confirmar a identidade

[13] Carimbo de tempo.

do emissor, atesta a hora e a data em que um documento foi assinado digitalmente. A variação numérica após a letra (de 1 a 4) corresponde ao tipo de geração da chave[14] do certificado.

Segundo BRY (2022), a assinatura e o certificado digital possuem funções diferentes, mas se complementam para garantir a confiabilidade dos processos no meio digital.

6 AUTORIDADE CERTIFICADORA RAIZ, AUTORIDADE CERTIFICADORA E AUTORIDADE DE REGISTRO

Conforme o Glossário ICP-Brasil (ITI, 2007), uma Autoridade Certificadora Raiz (AC-Raiz), é a entidade que credencia, audita e fiscaliza as demais entidades da ICP-Brasil, além de ser a Entidade de Auditoria de Tempo (EAT). Assina seu próprio certificado e os certificados das Autoridades Certificadoras (AC). Por sua vez, a AC é uma entidade que emite, renova ou revoga certificados digitais de outras autoridades certificadoras ou de titulares finais, enquanto que a Autoridade de Registro (AR) é a entidade responsável pela interface entre o usuário e a AC. Tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais.

7 ASSINATURA DIGITAL NOS REPRESENTANTE DIGITAIS

A assinatura digital é um método de autenticação e identificação de produtor, enquanto que o certificado digital é um arquivo de autenticação, associado a um par de chaves (chave privada e chave pública) para realizar a verificação da assinatura digital. A assinatura digital funciona com a geração de um *hash* após a aplicação da chave privada do produtor sobre o documento previamente criptografado. Com a chave pública, é realizado o procedimento inverso para descriptografar o documento, verificando a sua integridade.

O certificado digital, por sua vez, possui um período de validade, que é um dos critérios avaliados na hora da checagem da assinatura digital. Nesse aspecto, o carimbo de tempo garante a tempestividade da assinatura digital por meio da aplicação no documento da data e hora exatas da assinatura com base em uma terceira fonte confiável, comprovando que um evento realmente aconteceu em uma determinada data e horário.

---

[14] 1 - Geração das chaves feita por software; chaves de tamanho mínimo de 1024 bits; armazenamento em dispositivo como HDs e pen drive; validade máxima de um ano. 2 - Geração das chaves feita por software; chaves de tamanho mínimo de 1024 bits; armazenamento em cartão inteligente (com chip) ou token USB (dispositivo semelhante a um pen drive); validade máxima de dois anos. 3 - Geração das chaves feita por hardware; chaves de tamanho mínimo de 1024 bits; armazenamento em cartão inteligente ou token USB; validade máxima de cinco anos. E, 4 - Geração das chaves feita por hardware; chaves de tamanho mínimo de 2048 bits; armazenamento em cartão inteligente ou token USB; validade máxima de seis anos (CONTABILIZEI, 2022).

Uma assinatura digital de arquivamento (AD-RA) permite aplicar o carimbo de tempo nos documentos digitais, por meio de um sistema específico, garantindo que a assinatura do documento foi realizada no tempo certo e validando o novo carimbo de tempo sobre o antigo, mesmo com o passar dos anos e o surgimento de novas tecnologias (BRY,2022).

8 A PRESUNÇÃO DE AUTENTICIDADE E VALIDADE JURÍDICA

Segundo a Resolução nº 37 do CONARQ (2012), a presunção de autenticidade do documento arquivístico digital é realizada por meio da análise da sua forma e conteúdo, do ambiente de produção, manutenção/uso e preservação de documentos e não apenas em características físicas ou em soluções tecnológicas. Assim, a presunção de autenticidade se baseia na confirmação da existência de uma cadeia de custódia ininterrupta.

Para assegurar que os documentos arquivísticos digitais sejam confiáveis e autênticos, é fundamental a implantação de um SIGAD, visando o controle do ciclo de vida dos documentos, mantendo a relação orgânica, garantindo a confiabilidade, a autenticidade e o acesso, ao longo do tempo, aos documentos arquivísticos e, consequentemente, o seu valor como fonte de prova das atividades do seu produtor. É obrigatório que um SIGAD verifique a validade da assinatura digital no momento da captura de um documento, que realize a verificação da assinatura e que registre como metadado[15] além destas informações, a data e da hora da verificação. É altamente recomendável que um SIGAD verifique também a origem e a integridade destes documentos (CONARQ,2022).

Por fim, um SIGAD pode e deve interoperar com um RDC-Arq para armazenar documentos de longa temporalidade ou destinados à guarda permanente. Segundo a Resolução nº 43 (CONARQ, 2015), o RDC-Arq é um repositório digital com capacidade de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário, que armazena e gerencia esses documentos, seja nas fases corrente e intermediária, seja na fase permanente.

[15] Por sua vez, metadados são dados estruturados que permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo, e viabilizam a gestão de documentos nos suportes não-digitais, digitais e híbridos (CONARQ, 2022). Possibilitam a interoperabilidade de sistemas, de padrões internacionais e modelos nacionais de metadados, como o modelo em desenvolvimento pelo Grupo de Trabalho de Padrão de Metadados do Governo Eletrônico (e-PMG), integrante dos Padrões de Interoperabilidade de Governo Eletrônico (e-PING).

9 CONSIDERAÇÕES FINAIS

As assinaturas digitais possuem especificidades que contribuem para a preservação do documento digital e essas características precisam ser avaliadas com mais profundidade, como é o caso da assinatura digital para arquivamento, AD-RA. Esses atributos, em conjunto com a utilização de SIGADs e RDC-Arqs contribuem para garantir a validade jurídica e são cruciais para a presunção de autenticidade dos documentos digitais. Para os representantes digitais, essas questões são essenciais, em virtude da substituição do suporte documental.

REFERÊNCIAS

ADOBE. **Assinaturas eletrônicas têm validade legal? Com certeza.** 2022. Disponível em: https://www.adobe.com/br/sign/compliance/electronic-signature-legality.html. Acesso em: 10 ago. 2022.

BRY. BRySigner. **Tipos de assinatura digital: saiba quais são as modalidades, padrões e artefatos.** [S.l.]. BRyTecnologia, 2022. Elaborado por Cristian Thiago Moecke. Disponível em: https://www.bry.com.br/blog/tipos-de-assinatura-digital/. Acesso em: 29 mai. 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 37, de 19 de dezembro de 2012.** Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais. Disponível em: http://antigo.conarq.gov.br/images/publicacoes_textos/ conarq_ presuncao_autenticidade_completa.pdf Acesso em: 27 maio 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 43, de 04 de setembro de 2015.** Altera a redação da Resolução do CONARQ nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_diretrizes_rdc_arq_resolucao_43.pdf Acesso em: 27 maio 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 50, de 06 de maio de 2022.** Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, versão 2. Disponível em: https://www.gov.br/conarq/pt-br/ legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-50-de-06-de-maio-de-2022. Acesso em: 27 maio 2022.

CONSULTOR JURÍDICO. Conjur. **Assinatura digital em título extrajudicial é válida mesmo sem certificado da ICP-Brasil**. 2021. Disponível em: https://www.conjur.com.br/2021-nov-24/assinatura-digital-valida-mesmo-certificado-icp-brasil. Acesso em: 10 ago. 2022.

CONTABILIZEI. Contabilizei.blog. **Certificados digitais: conheça os tipos e as vantagens de ter na sua empresa.** [S.l.]. Contabilizei.blog, 2022. Disponível em: https://www.contabilizei.com.br/contabilidade-online/tipos-de-certificado-digital/. Acesso em: 29 maio 2022.

HIRATA, Wilson. **PAdES – Novo Padrão Brasileiro de Assinatura Digital.** Belo Horizonte. 2015. Apresentação de Power Point. 18 slides. color. Disponível em: https://certforum.iti.gov.br/2015/brasilia/wpcontent/uploads/2014/10/apresentação_hirata.pdf. Acesso em: 29 maio 2022.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). **Glossário ICP-Brasil.** Versão 1.2. 2007. Disponível em: https://www.gov.br/iti/pt-br/central-de-conteudo/glossario-icp-brasil-versao-1-2-novo-2-pdf/view. Acesso em: 10 ago. 2022.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Requisitos das Políticas de Assinatura Digital na ICP-Brasil.** 2021. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/instrucoes-normativas/IN032021_DOC_15.03_assinada.pdf. Acesso em: 10 ago. 2022.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Visão geral sobre Assinaturas Digitais na ICP-Brasil.** 2021b. Disponível em: https://www.gov.br/iti/pt-br/assuntos/legislacao/resolucoes/resolucoes-old/Resoluo_CGICPBrasil_182Dec10139Etapa3DOC15_assinada.pdf. Acesso em: 10 ago. 2022.