WWW.CONTEUDOJURIDICO.COM.BR

UNIVERSIDADE FEDERAL DA BAHIA
INSTITUTO DE CIÊNCIA DA INFORMAÇÃO
CURSO DE ARQUIVOLOGIA

FERNANDO SEIXAS PEREIRA

CERTIFICAÇÃO DIGITAL: aplicação tecnológica para a autenticidade de documentos arquivísticos digitais.

Salvador
2014

WWW.CONTEUDOJURIDICO.COM.BR

FERNANDO SEIXAS PEREIRA

CERTIFICAÇÃO DIGITAL: aplicação tecnológica para a autenticidade de documentos arquivísticos digitais.

Monografia apresentada no Instituto de Ciência da Informação da Universidade Federal da Bahia, como requisito parcial para obtenção do grau de Bacharel em Arquivologia.

Orientadora: Professora Doutora Ana Paula de Oliveira Villalobos.

Salvador
2014

WWW.CONTEUDOJURIDICO.COM.BR

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DA BAHIA
INSTITUTO DE CIÊNCIA DA INFORMAÇÃO
COLEGIADO DO CURSO DE ARQUIVOLOGIA

TERMO DE APROVAÇÃO

Fernando Seixas Pereira

Certificação Digital: ferramenta tecnológica para a autenticidade de documentos arquivísticos digitais.

Trabalho de Conclusão de Curso (TCC) submetido à aprovação da Comissão Examinadora como requisito parcial para a obtenção do grau de Bacharel em Arquivologia, pelo Instituto de Ciência da Informação da Universidade Federal da Bahia, em 16 de dezembro de 2014.

EXAMINADORES:

Ana Paula de Oliveira Villalobos
Doutora em Educação(FACED-UFBA)
Professora do ICI/UFBA

Albano Souza Oliveira
Doutor em difusão do conhecimento (FACED-UFBA)
Professor ICI-UFBA

Hildenise Ferreira Novo
Doutora em Difusão do conhecimento(UFBA)
Professora do ICI/UFBA

WWW.CONTEUDOJURIDICO.COM.BR

P436 Pereira, Fernando Seixas

Certificação Digital: ferramenta tecnológica para autenci-
dade de documentos arquivísticos digitais./ Fernando Seixas
Pereira. – Salvador, 2014.
53 f. ;il.

Orientadora: Profa.Dra. Ana Paula de O. Villalobos

Monografia (Graduação) Arquivologia – Universidade
Federal da Bahia, Instituto de Ciência da Informação, 2014.

1.Certificação Digital. 2. Diplomática Arquivística.
3. Documentos Digitais. I.Villalobos, Ana Paula de. II Universidade Federal
da Bahia, Instituto de Ciência da Informação. III.Titulo

CDU 004.056

AGRADECIMENTOS

Agradeço a Deus pela minha vida, paciência, perseverança e entendimento.

A orientadora Doutora Ana Paula Villalobos, pela colaboração significativa, dedicação e orientação.

A meus pais por todos os esforços, ensinamentos e encorajamento.

A todos os professores do Instituto de Ciência da Informação, que colaboraram para a aquisição dos conhecimentos necessários à minha formação.

Aos meus colegas, que trabalhamos juntos durante o percurso do curso.

RESUMO

A certificação digital apresenta-se como um meio eficiente para garantir a aplicação dos princípios da autenticidade, integridade e a confidencialidade dos documentos digitais, elementos esses necessários para atividades seguras em meio eletrônico digital. Esta pesquisa identifica e descrevem os conceitos desses elementos e das tecnologias aplicadas para garantir esses princípios aos documentos arquivísticos em suportes digitais, como o certificado, identidade e assinatura digitais. Para tanto foi realizado uma revisão de literatura em livros, teses, legislações e trabalhos de especialista sobre o tema. O Arquivista profissional que tem como uma de suas atribuições o planejamento de novos documentos, pode encontrar na utilização da certificação digital uma maneira de segurança na produção de documentos para garantir a autenticidade e integridade dos dados e informações documentados em suportes eletrônicos digitais. A sociedade contemporânea utiliza cada vez mais as tecnologias informatizadas para realizar atividades e transações eletrônicas, produzir, transmitir e disseminar informações registradas em suportes eletrônicos digitais para satisfazer os interesses, cumprir direitos e deveres, que se exigem comprovação de dados e informações por meio eletrônico, e por essas tecnologias desenvolverem um papel muito importante da gestão e gerenciamento de documentos por meio de sistemas eletrônicos. Entretanto as problemáticas advindas pelo seu uso e a vulnerabilidade em que se encontravam as informações e documentos digitais produzidos e transmitidos na web; pela necessidade de comprovação exata da autoria dos envolvidos e os riscos de adulteração e

confidencialidade desses documentos levaram vários países a buscar soluções desses problemas. A certificação digital surgiu como uma ferramenta tecnológica capaz de solucionar esses empecilhos que para muitos países da Europa, o Reino Unido, Portugal, Espanha e Brasil essas preocupações poderiam atrapalhar o desenvolvimento do comercio eletrônico e consequentemente o desenvolvimento econômico dos países. Para trazer solução desses riscos no ambiente eletrônico os países criaram leis, normas e ferramentas tecnológicas para regulamentar e implementar as assinaturas digitais. Com a Diretiva de 1999, depois outros países também mostraram interesses em regular essa tecnologia de maneira que pudessem garantir os princípios da autenticidade, integridade e confidencialidade dos documentos digitais. No Brasil foi instituída em 2001 a Infraestrutura de Chaves Públicas para regulamentar a certificação digital no país.

Palavras-Chave: Certificação Digital. Autenticidade. Documento Digital. Assinatura Digital.

ABSTRACT

Digital certification is presented as an efficient way to ensure the application of the principles of authenticity, integrity and confidentiality of digital documents, these elements required for safe activities in digital electronic means. This research identifies and describes the concepts of these elements and applied technologies to ensure these principles to archival documents in digital media, with the certificate, identity and digital signature. The participants had to review the literature in books, theses, laws and expert studies on the subject. Professional Archivist that has as one of its tasks the planning of new documents, you can find in the use of digital certification a way to safety in the production of documents to ensure the authenticity and integrity of the data and information documented in digital electronic media. Contemporary society uses more and more computer technology to carry out activities and electronic transactions, produce, transmit and disseminate information recorded in digital electronic media to serve the interests, rights and duties to fulfill, which require verification of data and information by electronic means, and these technologies develop an important role of management and document management through electronic systems. However the problems arising from its use and the vulnerability they were in the information and digital documents produced and broadcast on the web; by the need to accurately prove the authorship of those involved and the risk of tampering and confidentiality of these documents have led many countries to seek solutions to these problems. Digital certification emerged as a technological tool to solve these obstacles that for many countries in Europe, the United Kingdom, Portugal, Spain and Brazil these concerns could hinder the

development of e-commerce and consequently the economic development of countries. To bring solution of these risks in the electronic environment countries have established laws, rules and technological tools to regulate and implement digital signatures. With the 1999 Directive, after other countries have also shown interest in this regular way technology that could ensure the principles of authenticity, integrity and confidentiality of digital documents. In Brazil was established in 2001 to Public Key Infrastructure to regulate the digital certification in the country.

Keywords: Digital Certification. Authenticity. Digital document. Digital signature.

LISTA DE QUADROS

Quadro 1- Respostas aos questionamentos..... 28

Quadro 2- Cursos de Arquivologia com disciplinas de diplomática, informática e autenticidade digital..... 35

Quadro 3- Elementos dos documentos digitais..... 43

LISTA DE FIGURAS

Figura 1- inserção de assinatura digital..... 19

Figura 2- linha de assinatura..... 19

Figura 3- configuração de assinatura..... 20

Figura 4 configuração para inserir a linha de assinatura..... 20

Figura 5- verificação de assinaturas válidas..... 21

Figura 6- verificação de assinaturas..... 21

Figura 7- configuração do estado do conteúdo..... 21

Figura 8- certificado digital..... 22

Figura 9- certificado da Certising..... 26

Figura 10- Acs no brasil..... 28

LISTAS DE ABREVEATURAS E SIGLAS

A1 Á A4	Certificados da Série A
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz
ACs	Autoridades Certificadoras
AR	Autoridade de Registro
ARs	Autoridades de Registros
BGBI.I.S	Do Federal
CIA	Conselho Internacional de Arquivos
CONARQ	Conselho Nacional de Arquivos
FURG	Universidade Federal do Rio Grande
GED	Gerenciamento Eletrônico de Documentos
ICP-BRASIL	Infraestrutura de Chaves pública brasileira

INTERPARES	Pesquisa Internacional em Registros Autênticos Permanentes em Sistemas Eletrônicos
ITU-T	União Internacional das Telecomunicações
LAN	Local Área Network
S1Á S4	Certificados da série S
SIGAD	Sistema Informatizado de Gestão Arquivística de Documentos
UEL	Universidade Estadual de Londrina
UEPB	Universidade Estadual da Paraíba
UFAM	Universidade Federal do Amazonas
UFBA	Universidade Federal da Bahia
UFMG	Universidade Federal de Minas Gerais
UFRGS	Universidade Federal do Rio Grande do Sul
UNESP	Universidade Estadual Paulista
X.509	Padrão para Certificados Digitais

SUMÁRIO

1. INTRODUÇÃO..... 09

2.CERTIFICAÇÃO DIGITAL..... 15

2.1CRIPTOGRAFIA..... 18

2.2 ASSINATURA DIGITAL..... 19

2.3 INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA..... 23

3.OS ARQUIVOS DIGITAIS COMO OBJETO DE ESTUDO NA ARQUIVOLOGIA CONTEMPORÂNEA..... 29

3.1 COMPETÊNCIA DO ARQUIVISTA RELATIVA AOS DOCUMETOS ARQUIVÍSTICOS DIGITAIS..... 33

4.UTILIZAÇÃO DAS TECNOLOGIAS NA PRODUÇÃO DE DOCUMENTOS DIGITAIS..... 36

4.1 TRANSAÇÕES EM MEIO ELETRÔNICO QUE GERAM DOCUMENTOS DIGITAIS..... 37

5. PRINCÍPIOS DA AUTENTICIDADE E INTEGRIDADE EM CERTIFICAÇÃO DIGITAL..... 39

6. CONSIDERAÇÕES FINAIS..... 47

REFERÊNCIAS..... 50

1. INTRODUÇÃO

Este trabalho aborda a certificação digital como meio de gestão da segurança das informações e documentos arquivísticos digitais, a qual busca manter os princípios da autenticidade, integridade e fidedignidade das informações e documentos produzidos, armazenados, transmitidos e divulgados em sistema computacional. Princípios esses que já vinham sendo estudados ha tempo pela diplomática, aplicados na análise dos documentos tradicionais.

Devido o surgimento dos documentos digitais, novos estudos foram realizados com a finalidade de aplicação desses princípios aos documentos digitais. Essa pesquisa observa esses estudos e aplicação desses princípios por meio da diplomática arquivística, conceito contemporâneo da tipologia documental e por meio da certificação digital. E verifica a regulamentação da certificação digital no Brasil pela instituição das Autoridades Certificadoras (ACs) da Infraestrutura de Chaves Públicas do Brasil (ICP-Brasil).

A diplomática arquivística é uma definição dada pelos estudos da tipologia documental, que segundo Bellotto (2006, p. 53) “ao incorporar todo corpo teórico e metodológico da antiga diplomática, pode ser chamada de diplomática arquivística [...]”.

A tipologia documental estuda a configuração da espécie do documento, que é produzido segundo uma atividade que tem como resultado a produção de tipos de documentos. Enquanto a tipologia analisa o documento pela atividade que o produz, a diplomática observa a natureza das informações do documento. Esses conhecimentos são necessários para observar a validade dos documentos, se o foi produzido de acordo com as normas que os regulamentas, perceber a origem do documento, quem o produziu, para quem, quando e para que finalidade. Essas informações são fundamentais para a autenticidade dos documentos. Pois cada documento autêntico tem uma identidade única, o que lhe garanti a autoria do documento. O documento digital também para ser autêntico deve apresentar uma identificação única, apresentar a origem, a data do documento, as pessoas

interessadas ou a quem se refere o documento, o assunto, o formato imposto pela normalização e por fim para que seja completo a (s) assinatura (s) do (s) signatário (s).

A certificação digital é constituída por um conjunto de normas, técnicas e elementos aplicados, os quais são descritos nesta pesquisa a criptografia, assinatura digital e o certificado validado e emitido por uma autoridade certificadora, que atestam ou asseguram uma identidade digital, que pode ser utilizada em sistemas eletrônicos digitais para realização de transações seguras, as quais tem por fins a produção de informações e documentos digitais.

Realizou-se uma pesquisa para compreender as definições e os elementos da certificação digital. Verificar a legislação que regulamenta essa atividade, os aspectos jurídicos, os princípios da autenticidade, integridade e fidedignidade com base na diplomática arquivística e os que são aplicados na certificação digital para garantir segurança das informações e dos documentos arquivísticos digitais por meio da certificação, identificar as autoridades certificadoras no país que emitem certificados digitais.

A utilização das tecnologias informatizadas pelas organizações contemporâneas trouxe mudanças nos suportes e formatos utilizados na produção documental na atual sociedade. A certificação da Infraestrutura de chaves públicas do Brasil apresenta-se como uma alternativa viável para manter a segurança dos princípios da autenticidade e integridade, a fim de que os documentos produzidos digitalmente sejam confiáveis e válidos judicialmente.

A certificação digital emitida por uma das ACs da hierarquia da ICP-Brasil tem essa finalidade, pois a ICP-Brasil foi instituída com a finalidade de garantir a autenticidade e integridade das informações e documentos digitais por meio de tecnologias e normas que garantam a aplicação dos princípios da autenticidade e integridade das informações e documentos digitais.

As organizações contemporâneas da sociedade da informação e do conhecimento encontram nas tecnologias informatizadas muitas vantagens para

produzir e gerir informações e documentos, pelo fato dessas disponibilizarem ferramentas na gestão das informações e dos documentos.

Com um simples computador é possível realizar diversas atividades, pode-se com o mesmo instrumento registrar e armazenar informações e documentos, assim como enviá-los por sistemas de transporte eletrônico para qualquer parte do mundo onde se tenha um computador com acesso a rede mundial de computadores conhecida de internet.

Com o uso da informática a sociedade produz, armazena, transmite informações e documentos em meios digitais, realiza acordos e contratos, acessa bancos de dados e consulta processos por meio eletrônico. A manipulação das informações e documentos digitais ao mesmo tempo em que traz vantagens pode trazer desvantagens.

Se essas informações e documentos digitais forem adulterados ou manipulados por usuários não autorizados, isso coloca em risco a autenticidade e integridade da preservação de documentos autênticos e a confidencialidades das informações, daí surgem ferramentas de segurança, que procuram resolver tais problemas.

Sistemas de intranet são utilizados para evitar usuários não autorizados em sistemas eletrônicos internos nas organizações, sistemas de autenticação de usuários e a certificação digital são mais uma ferramenta de segurança, utilizada para evitar os riscos de insegurança que as informações e documentos eletrônicos podem estar e de evitar falsa identidade digital.

A ICP-Brasil pretende resolver esses problemas ao inserir uma pessoa, organização ou sistema à sua base de certificação por intermédio de uma AC de sua hierarquia.

Com base em pesquisas de autores da Arquivologia e da Ciência da informação como Sânderson Lopes Dorneles, graduado em Arquivologia pela Universidade Federal de Santa Maria, Rosely Curi Rondinelli, doutora em Ciência da Informação, existe hoje a necessidade do arquivista contemporâneo da sociedade

da informação e do conhecimento atentar para o conhecimento relacionado aos documentos digitais.

Como profissional que lida com documentos arquivísticos, entende-se que documentos arquivísticos englobam os documentos digitais criados na decorrência de atividades. Razão essa pela qual possa precisar o arquivista diante dessas tecnologias de informações digitais, atentar para a legalidade; integridade e autenticidade das informações e dos documentos criados nesse ambiente. Ao participar como profissional em planejamento para produção e gestão de informações e documentos arquivísticos digitais nas empresas e organizações. De acordo com a lei 6.546, que regulamenta a profissão de Arquivista, no artigo 2º dentre suas atribuições estão o “planejamento, orientação, direção das atividades de identificação das espécies documentais e planejamento de novos documentos [...]”.

Portanto para atentar para esses princípios que dão validade jurídica aos documentos digitais e sua aplicação aos novos documentos produzidos em meios digitais é fundamental conhecer seu conceito e como são aplicados em ambientes digitais, através das tecnologias de certificação digital.

Este trabalho teve como objetivo geral reconhecer a aplicação dos elementos da certificação digital e analisar a aplicação dessa ferramenta para garantir os princípios da autenticidade, integridade e fidedignidade de documentos digitais pelas Autoridades Certificadoras da ICP-Brasil. Especificamente, verificar os elementos que compõem a certificação digital e a legislação para a gestão da segurança da autenticidade e integridade das informações e dos documentos em ambientes digitais.

No desenvolvimento essa pesquisa responde aos seguintes questionamentos: o que se entende por certificação digital; quais as razões para uma implantação de sistemas de certificação digital; como os princípios que caracterizam os documentos de arquivos a autenticidade, integridade e confiabilidade são garantidos com a certificação digital, quais elementos ou técnicas da certificação digital e os que devem ser observados para garantir autenticidade aos documentos digitais pela Arquivologia?

Também é importante saber que legislação no Brasil regula a certificação digital e judicialmente o que são observados para fins de autenticidade de uma certificação digital? A certificação digital da ICP-Brasil pode ser uma alternativa de segurança aplicada nas instituições arquivísticas e nos sistemas informatizados de gestão arquivística de documentos?

Ao fim dessa pesquisa foi possível identificar e descrever as definições de certificação digital e dos seus elementos, perceber quais técnicas e tecnologias implantadas para uma certificação digital, definir os elementos que compõem o certificado digital, verificar as entidades certificadoras de documentos digitais no país e evidenciar os impactos da certificação digital em termos qualitativos para seus usuários.

Certamente existem entidades certificadoras de documentos digitais no país e para entender os procedimentos realizados para a certificação digital é necessário conhecê-las e saber quais critérios e elementos são observados durante o processo de verificação dos requisitos para uma certificação digital e como funciona esse sistema de segurança da autenticidade dos documentos digitais.

Esses conhecimentos são imprescindíveis para o profissional Arquivista contemporâneo na atual sociedade da informação e conhecimento, onde as atividades profissionais das organizações estão utilizando cada vez mais as tecnologias informatizadas, visando à eficiência e serem eficaz em suas atividades e serviços.

O Arquivista tem hoje como desafio indicar e implementar sistemas de confiança e de segurança para as organizações, que utilizam sistemas computacionais para realizar transações ou atividades, os quais tem como resultado final a produção de informações registradas em suportes digitais. Vale ressaltar que o Arquivista contemporâneo é designado neste trabalho como o profissional de nível superior formado em Arquivologia.

Sendo assim este estudo se justifica tanto para a Arquivologia quanto para o profissional Arquivista, visto que a Arquivologia estuda os arquivos de modo geral, sendo tradicional ou contemporâneo e os profissionais Arquivistas tem como desafio

de objeto de trabalho a gestão autentica das informações e dos documentos arquivísticos digitais.

Nessa pesquisa, informação digital é sinônima de documento digital, uma vez que documento digital é a informação registrada em meio eletrônico digital. Particularmente os documentos arquivísticos digitais, que são originados durante a atuação profissional, pelas pessoas, por meio da tecnologia informatizada, para efeito de comprovação, atestado, declaração, tratado e qualquer outro fato que necessite ser registrado como prova de ato.

Para o desenvolvimento desta pesquisa realizou-se revisão de literatura, consulta à legislação que regulamenta a certificação digital no Brasil e descrição dos critérios e elementos necessários à certificação digital. Devido a isso, os métodos são bibliográficos e documentais.

Foram consultadas teses de dissertações e bibliografias que abordam o tema, documentos eletrônicos e legislativos que regulam a atividade de certificação digital pela Infraestrutura de chaves públicas no Brasil.

Os dados foram obtidos através dos meios de comunicação com informações sobre o assunto disponíveis nos sites das entidades certificadoras, livros atuais que abordam essa temática, e a legislação inerente a certificação digital, trabalhos de teses e dissertações disponibilizadas em revistas científicas eletrônicas. Caracterizando-se como bibliográfica e documental por utilizar documentos oficiais, bibliografias e documentos eletrônicos.

De acordo com Lakatos (2010, p. 166) entende-se que “a pesquisa bibliográfica, ou de fontes secundárias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses [...]”

Realizou-se uma identificação e análise dos elementos específicos que envolvem a certificação digital como a autenticidade, integridade, confidencialidade para se chegar à definição de certificação digital e da sua importância na perspectiva da Arquivologia. Foram encontradas poucas publicações na Arquivologia que se tratasse sobre a certificação digital, mas foram encontrados ricos materiais que

aborda sobre os princípios da autenticidade e integridade e documentos digitais. Esses materiais facilitaram no aproximamento, reconhecimento, identificação e descrição dos elementos da autenticidade documental.

2. CERTIFICAÇÃO DIGITAL

A resposta da primeira pergunta da pesquisa, o que se entende por certificação digital pode ser encontrada na definição de certificação digital. O dicionário brasileiro de terminologia arquivística do Arquivo nacional (2005) define certificação como “Afirmação ou atestação de um fato em razão de ofício”

No glossário do Instituto Nacional de Tecnologia da Informação certificação digital é definido como:

> Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um certificado digital por uma autoridade certificadora. (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2010).
>
> As Autoridades Certificadoras - ACs são entidades de Confiança, que emitem certificados digitais para outras entidades, empresas, indivíduos, que precisam se identificar e garantir as suas operações no mundo digital. (MONTEIRO; MIGNONI, 2007, p. 34).

A certificação digital é definida como uma atividade de reconhecimento em meio eletrônico, a qual estabelece uma relação única, exclusiva e intransferível entre uma chave de criptografia com uma pessoa física, jurídica, máquina ou aplicação. O estabelecimento dessa relação única, exclusiva e intransferível é fundamental e necessário para garantir a identidade digital, pois assim como a identidade que todos os cidadãos tem tradicionalmente, através dos elementos de identificação, que os identificam individualmente perante a sociedade são fundamentais para os reconhecerem a si próprios e seus atos praticados com sua identidade, também são necessários estabelecer os elementos a

identificação individual de cada pessoal que deseja praticar atos com efeitos jurídicos.

A certificação digital originou-se devido o uso das tecnologias computacionais para a realização de atividades diversas, que exigem segurança e autenticidade nas transações, principalmente nos negócios comerciais e de serviços firmados em meio eletrônico.

Realizada por uma autoridade certificadora com objetivo de certificar as atividades realizadas nos sistemas informatizados, para validar endereços na web, documentos digitais de pessoas físicas e jurídicas que utilizam essas tecnologias como meio de efetuar transações. A certificação digital é uma aplicação que busca segurança nas relações que geram informações por meio de equipamentos eletrônicos. As autoridades certificadoras são responsáveis em emitir os certificados digitais. Com a certificação digital é possível obter segurança para atividades que geram documentos e informações tanto em rede LAN de nível local nos sistemas restritos a usuários do ambiente interno das instituições, pelos sistemas de intranet e extranet, como de rede WAN que se pode ter acesso à rede mundial de computadores (internet). Um sistema de certificação digital pode identificar um usuário em sistemas de intranet e internet.

Através da certificação digital pode-se garantir a identificação do usuário que utiliza sua identidade digital. Portanto qualquer atividade realizada com o uso da identidade digital, tais como informações e documentos produzidos nas transações e acordos são de responsabilidades do usuário à qual pertence sua identidade digital. A assinatura digital produzida por uma chave privada deve tão somente lhe pertencer, razão pela qual deve manter em secreto o código que criou para sua chave privada, que corresponde à chave pública.

Os documentos digitais assinados digitalmente tornam-se autênticos pelo fato da assinatura ser de reconhecimento único e exclusivo por meio de um certificado digital emitido por uma autoridade de confiança que garanti a identificação única e exclusiva de pessoa física, jurídica, máquina ou aplicação. Através dos quais é possível produzir várias espécies de documentos e assiná-los em meios digitais. A

identidade exclusiva garante a identificação das partes envolvidas, que se identificam por meio da identidade digital.

Vejamos as definições da lei 11.419 de (2006), que dispõe sobre a informatização de processos judiciais, sobre meio eletrônico e transmissão eletrônica.

> § 2o Para o disposto nesta Lei, considera-se:
>
> I - meio eletrônico qualquer forma de armazenamento ou tráfego de documentos e arquivos digitais;
>
> II - transmissão eletrônica toda forma de comunicação a distância com a utilização de redes de comunicação, preferencialmente a rede mundial de computadores;

O meio eletrônico é utilizado para armazenar e transmitir os documentos eletrônicos, embora a literatura internacional muitas vezes se refira tanto aos documentos digitais como os eletrônicos da mesma maneira, no Brasil existe diferenciação na definição dos termos utilizados, observamos essa diferença no conceito seguinte do dicionário de terminologia arquivística do Arquivo Nacional que considera documento eletrônico como “Gênero documental integrado por documentos em meio eletrônicos ou somente acessíveis por equipamentos eletrônicos, como cartões perfurados, disquetes e documentos digitais”. (ARQUIVO NACIONAL, 2005, p.75).

Documento arquivístico digital é o documento produzido na decorrência de atividades por meio das tecnologias informatizadas pelas pessoas e organizações.

A diferença entre documento arquivístico convencional e o digital consistem no uso do suporte para registrar a informação e produzir o documento. Enquanto suportes de documentos arquivísticos convencionais pode ser o pergaminho, papiro, papel, fitas VHS, o documento arquivístico digital é criado em sistemas computacionais, através dos hardwares e softwares como nos mostra a definição seguinte de documento digital. “Documento codificado em dígitos binários, acessível por meio de sistema computacional”. (ARQUIVO NACIONAL, 2005, p.75).

2.1 CRIPTOGRAFIA

A criptografia é utilizada para criar os pares de chaves pública e privada. É uma técnica de segurança utilizada para codificar e decodificar uma mensagem, a fim de torná-la confidencial, devendo ser decodificada pelo destinatário autorizado por uma chave secreta. Para manter a segurança da confidencialidade da mensagem codificada o responsável pela chave que permite decodificar a mensagem não deve revelar a lógica matemática, caso contrário outros poderão decodificar e ler a mensagem.

Existe a criptografia simétrica e assimétrica. A criptografia simétrica utiliza uma só chave à pública que permite ao mesmo tempo codificar e decodificar a mensagem. Enquanto que a criptografia assimétrica utiliza duas chaves, uma pública que é conhecida por todos e a outra privada que somente o destinatário deve saber para decodificar a mensagem confidencial como nos mostra (BODÊ, 2006, p. 59):

> Quando alguém precisar enviar uma mensagem criptografada para algum indivíduo, utilizará o algoritmo RSA (atualmente existem outros algoritmos disponíveis, com o mesmo princípio e alteração nas fórmulas matemáticas) e a chave pública do destinatário. Esta mensagem quando criptografada não necessitará da chave pública para reverter o processo (como em algoritmos simétricos), mas sim sua chave privada, a qual pode ser utilizada pelo destinatário da mensagem (e somente através desta chave) para desfazer o processo criptográfico.

A criptografia utiliza técnicas matemáticas e de computação, com objetivos diplomáticos arquivísticos e jurídicos, que é tornar as informações dos usuários, que podem ser pessoas físicas ou jurídicas, confidencial, a fim de evitar adulterações no conteúdo das informações e manter a originalidade para efeitos de valor legal. A criptografia assimétrica também é utilizada na criação da assinatura digital.

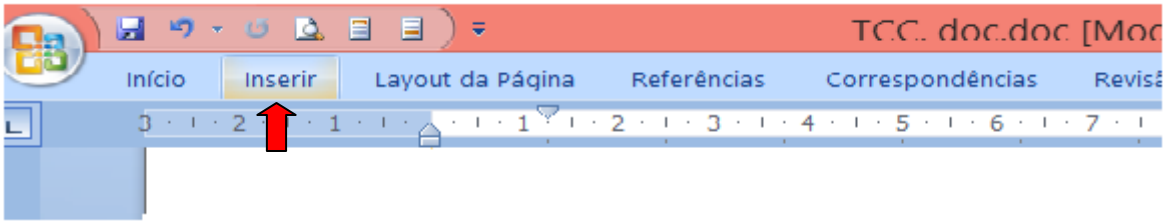
2.2 ASSINATURA DIGITAL

A assinatura digita é hoje utilizada por pessoas físicas, jurídicas, organizações e redes de computadores para ter uma identidade eletrônica que possa ser validada e autenticada. Depois de produzido um documento, ele pode receber a assinatura digital, que atestará que esta assinatura pertence ao autor do documento.

Assinatura em meio eletrônico, que permite aferir a origem e a integridade do documento. (ARQUIVO NACIONAL, 2005, p.). É possível utilizar assinaturas digitais certificadas pelas autoridades emissoras em documentos criados no office Word 2007. Para assinar digitalmente documentos depois de criado o conteúdo do documento. Entretanto o nível de segurança dessa assinatura depende das políticas de certificação utilizadas para emissão do certificado digital. Existem tipos de assinaturas digitais que podem não ter valor judicial. Pode-se utilizar qualquer assinatura de um certificado digital baixado no computador ou smart card.

Na opção inserir é possível colocar uma linha de assinatura digital no documento.

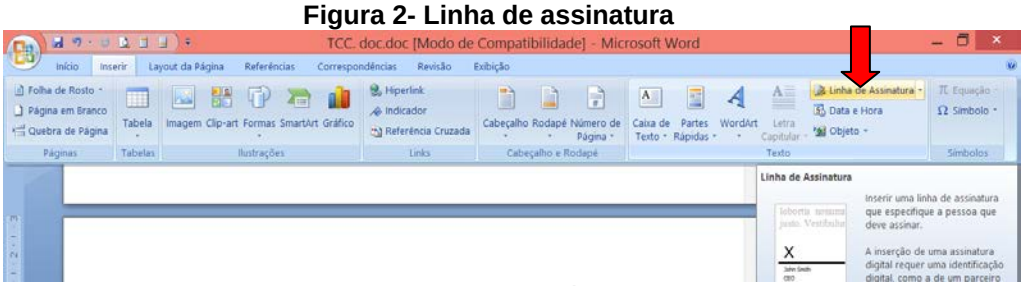
Figura 1- Inserir assinatura digital



Fonte: tela capturada em documento do word computador próprio.

Após clicar em inserir abri a linha de assinatura no canto superior direito.

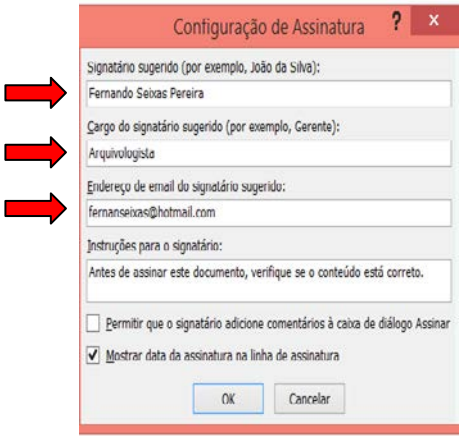
Figura 2- Linha de assinatura



Fonte: documento próprio.

Depois de clicar em linha de assinatura, abrirá a caixa de configuração de assinatura, preencha o nome do signatário, o cargo e endereço de e-mail e clique em ok.

Figura 3- Configuração de assinatura

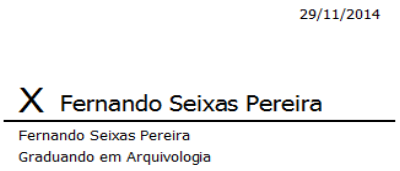


Fonte: configuração de assinatura em documento próprio

.

Aparecerá à linha para assinatura. Após clicar sobre a linha abrisse uma página para preenchimento de dados e assinar o documento. No final será mostrada uma linha com a assinatura.

Figura 4: assinatura digital

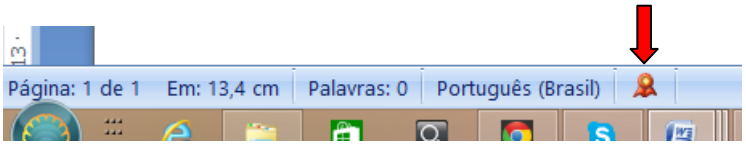


Fonte: elaboração própria

Também é possível verificar assinaturas válidas no próprio Word 2007, por meio dos procedimentos:

No ícone na parte inferior da tela do documento do Word como mostra a seta na figura 6:

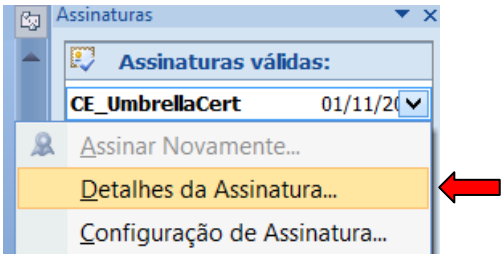
Figura 5: verificação de assinaturas válidas



Fonte: imagem capturada em documento word computador próprio.

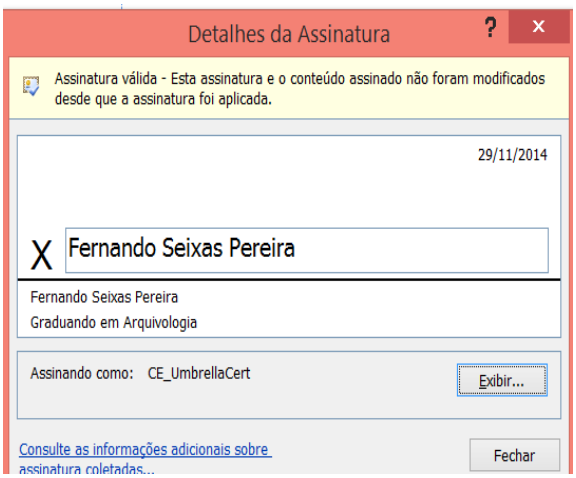
Logo depois aparece o campo detalhes da assinatura, ao clicar nesse campo abri uma tela informado o estado das informações do conteúdo do documento.

Figura 6: Verificação de assinatura



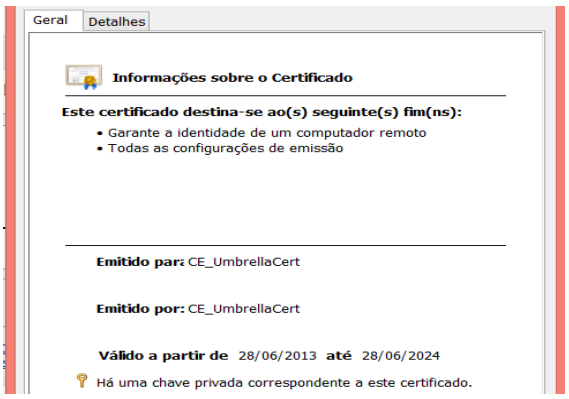
Fonte: imagem capturada em documento de elaboração própria.

Figura 7: Confirmação do estado do conteúdo



Fonte: captura de detalhes no editor Word.

Figura 8- Certificado digital



Fonte: captura de imagem certificado digital do computador próprio.

No detalhe mostrado a assinatura e o conteúdo não foram modificados. Essa ferramenta de verificação pode garantir a aplicação do princípio da integridade da diplomática, se aplicado com nível de segurança elevando, onde é possível saber de fato quem é o signatário, devido à verificação e comprovação da documentação de identificação antes da emissão do certificado.

Ao clicar em exibir em detalhes da assinatura é aberta uma janela que informa as garantias do certificado, a autoridade emissora e data de validade.

Esse tipo de assinatura confirma a integridade do documento. Entretanto não pode garantir que os dados de identificação do assinante são realmente do signatário que assinou o documento.

Embora a verificação da integridade do conteúdo e da assinatura seja possível não prova que a autoria seja verdadeira. Nesse tipo de assinatura existe risco quanto à veracidade do documento, já que não pode provar que foi de fato o indivíduo que o assinou.

Entretanto é possível criar mecanismos que reforce a segurança desse tipo de assinatura. Por exemplo, o signatário pode fazer um acordo de modelo tradicional com seu destinatário se responsabilizando por todos os documentos que este enviar pelo seu computador ao destinatário.

É importante ressaltar que assinatura digitalizada não é assinatura digital. A assinatura digital é garantida por meio de um certificado digital e identidade digital. A

assinatura digitalizada é realizada por meio de digitalização da assinatura. A assinatura digitalizada pode ser usada como uma imagem por meio da assinatura digital.

No Brasil em 2001, com a instituição da ICP-Brasil, as organizações ligadas a sua infraestrutura podem encontrar amparo legal para documentos certificados pelas ACs da ICP-Brasil, dando a mesma validade jurídica que os documentos convencionais. Isso nos responde com relação ao terceiro e quarto questionamento sobre que legislação regulamenta as atividades de certificação digital e o que são observados judicialmente para fins de autenticidade.

2.3 INFRAESTRUTA DE CHAVES PÚBLICAS BRASILEIRA

A medida provisória nº 2.200-2, 2001 regulamenta e propicia validade jurídica às transações realizadas eletronicamente pelas pessoas físicas, jurídicas e servidores web, que estejam ligados a infraestrutura de chaves públicas no Brasil.

> Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

A medida provisória deixa claro no artigo 1º que a infraestrutura de chaves pública foi instituída com a finalidade de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica.

> Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras compostas pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

AC RAIZ	Executar as políticas e fiscaliza as ACs e ARs:
ACs	Emitir certificados para usuários finais.
ARs	Atender as solicitações dos usuários finais encaminhar as ACs.

O comitê gestor aprova as políticas de certificação da ICP-Brasil.
Composição do Comitê Gestor
Instituto Nacional de Tecnologia da Informação

Ministério da Fazenda

Federação Brasileira de bancos;

Câmera brasileira de Comercio Eletrônico;

Ministério do Desenvolvimento, Indústria e Comércio exterior;

Associação dos Juízes Federais do Brasil;

Ministério do Planejamento Orçamento e Gestão;

Confederação Nacional do Comércio de Bens, Serviços e Turismo;

Ministério da Ciência e Tecnologia;

Gabinete de Segurança Institucional.

A AC raiz primeira autoridade da cadeia de certificação informada no artigo quinto é o Instituto Nacional de Tecnologia da Informação (ITI), órgão responsável em executar as políticas de certificados aprovadas pelo comitê gestor da ICP-Brasil. O ITI emite, expede, distribui e revoga certificados digitais para as autoridades certificadoras. É de sua competência também fiscalizar as Autoridades Certificadoras e as Autoridades de Registro.

> Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar

> e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Diretamente subordinadas a AC Raiz encontram-se as ACs, responsáveis em emitir, renovar e revogar os certificados digitais emitidos aos usuários finais. As autoridades certificadoras da ICP-Brasil emitem certificados que garantem a identidade digital das pessoas ou organizações, o endereço de computadores, à confirmação de autoria de correios eletrônicos.

> Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

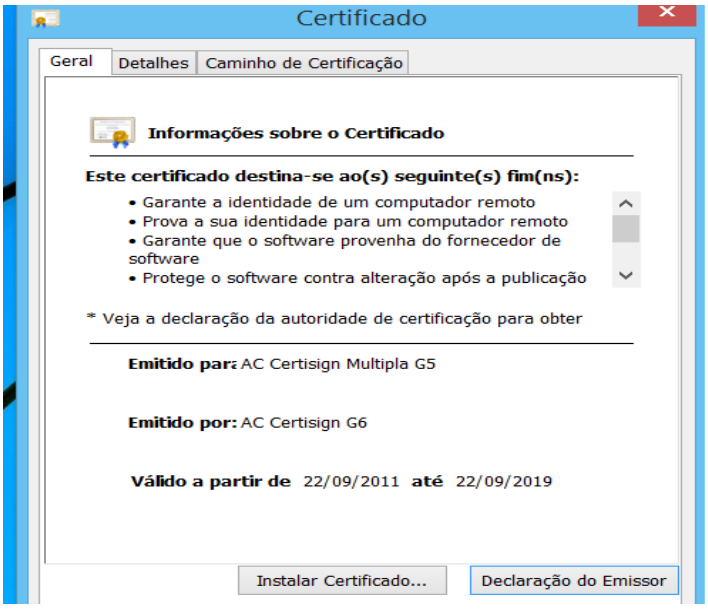
As ARs são responsáveis em intermediar entre os usuários finais e as ACs para os procedimentos da solicitação dos certificados digitais e verificação da documentação para confirmação dos dados do solicitante.

“Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.”

Todas as áreas de trabalho da sociedade que utilizam sistemas informatizados para realizar atividades, que resultam em produção, armazenamento e transmissão de dados, informações e documentos podem incrementar por meio da solicitação a uma AR a certificação de uma AC da ICP-Brasil ou a qualquer outro emissor desde que aceito pelas partes como válidos. Vale ressaltar que MP acrescentou esse parágrafo após receber críticas de infringir alguns princípios da constituição brasileira e por segundo alguns pesquisadores não seguir padrões da UNCITRAL.

> § 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. (MEDIDA PROVISÓRIA, nº 2.200-2,2001).

Figura 9: certificado da Certisign



Fonte: captura de certificado digital Certising computador próprio.

Este certificado da versão 3 da Certising garante a identidade de um computador, a identidade de um signatário para um computador. Permite que os dados sejam assinados com a hora atual. Entretanto ele é emitido para AC Certising. Existem padrões de certificados para pessoas físicas, jurídicas e aplicações. Os padrões dos certificados podem ser mudados devidos mudanças na regulamentação da política de certificação da ICP-Brasil. Os certificados da ICP-Brasil tem ganhado espaços em várias organizações no Brasil.

> É um conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2010).
> São os certificados usados para confirmação da identidade na web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações. (INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, 2010).

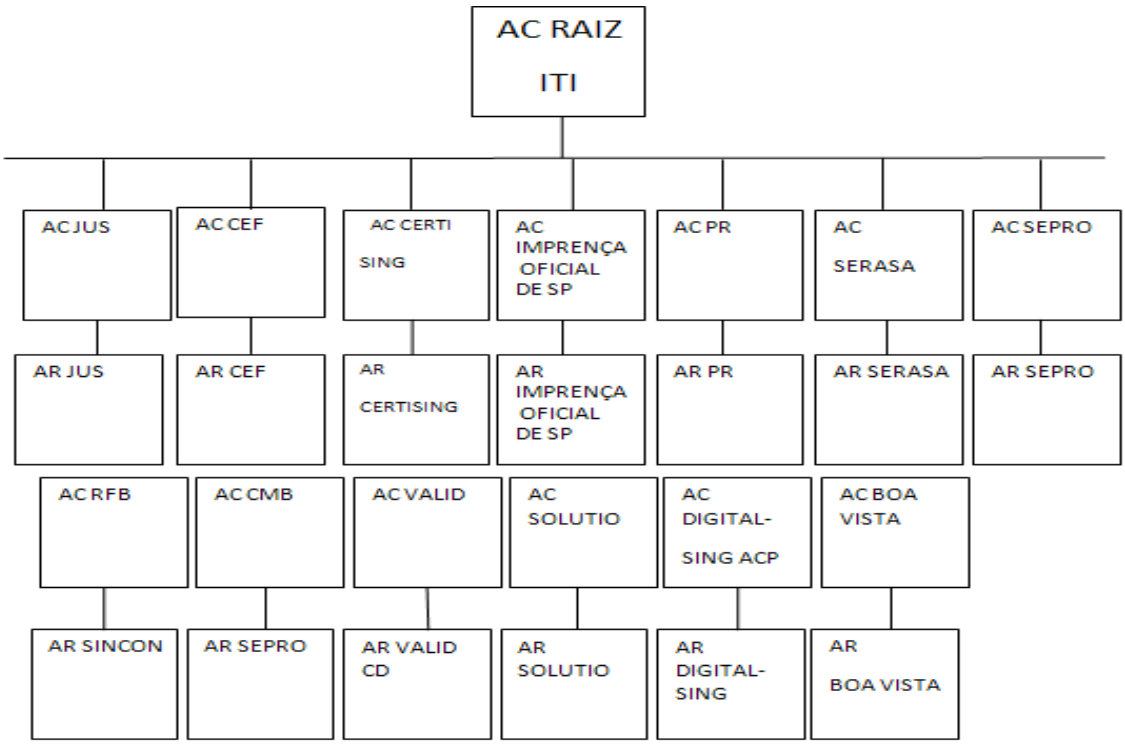
O Serviço de Processamento de Dados (SEPRO) tornou-se uma AC e AR da ICP- Brasil, embora antes da instituição da Medida Provisória 2:200-2 já tinha criado em 1999 um Centro de Certificação Digital.

O SEPRO é classificado como empresa pública, foi criado em 1964 pela lei 4516 de 1º de dezembro. Vinculado ao Ministério da Fazenda, seu objetivo é o tratamento das informações e processamento de dados, por meio da computação eletrônica e eletromecânica. A empresa pública SEPRO emite certificados para pessoas físicas, jurídicas, equipamentos e aplicações. Para garantir identidade na Web, transações eletrônicas e assinatura de documentos digitais e verificação da integridade do documento são utilizados certificados A1 á A4. Os certificados A1 tem validade de 1ano e o de A3 de três anos. Para manter a confidencialidade de mensagens e informações sigilosas são utilizados os tipos S1 á S4. Certificado digital de acordo as normas do comitê gestor. Essa reação dos usuários na aquisição de certificados emitidos pelas ACs da ICP-Brassil, isso significa que as pessoas e organizações confiam nos sistemas de certificação da ICP-Brasil, pois muitos profissionais e organizações tem utilizados para fins de autenticidade e integridade das informações por meio de sistemas computacionais.

Com o uso da certificação digital e a validade jurídica dos documentos digitais a produção de alguns documentos em papel, que outrora eram exigidos para serem entregues tende reduzir ou erradicar devido aos documentos que se tornaram digitais. Com isso o uso de papel tende a diminuir.

Em 15 de outubro de 2002 o Diário oficial da união publicou o despacho do ITI na página 14 seção 1 o credenciamento da empresa privada CERTISING como AC vinculada a AR da ICP-Brasil. Foram encontrados na Hierarquia da ICP- Brasil outras autoridades certificadoras como AC Caixa Econômica Federal, Ac Casa da Moeda do Brasil, Valid Cert Digital, Soluti, Digital Sign, Ac Boa Vista, Ac Serasa, AC Presidência da República e Imprensa Oficial de São Paulo.

Figura 10: ACs NO BRASIL



Fonte: Elaboração própria com base na referência da estrutura da ICP-Brasil.

Quadro 1 : respostas aos questionamentos

Razões para Implantação da Certificação Digital ICP-Brasil	Como os Princípios são Garantidos	Elementos e Técnicas da Certificação Digital	Observar Elementos para Garantir os Princípios da Autenticidade e Integridade dos Documentos Digitais	Legislação no Brasil que Regulamenta a Certificação Digital
Garantir autenticidade, integridade e validade jurídica dos documentos e aplicações em forma eletrônica	Através de técnicas e ferramentas tecnológicas: Certificado digital, criptografia, assinatura digital, ACS	Certificado digital, criptografia, assinatura digital,	Data do documento, hora e lugar onde foi criado, transmitido e recebido, identificação dos nomes dos autores, destinatário nome do criador, título ou assunto, código de classificação e os que forem determinados por normas e regulamentos.	Medida Provisória 2:200.2

Fonte: elaboração própria.

3. OS ARQUIVOS DIGITAIS COMO OBJETO DE ESTUDO NA ARQUIVOLOGIA CONTEMPORÂNEA

Para se entender a relação da Arquivologia com as técnicas de gestão de documentos digitais com relação à certificação digital é necessário compreender seu objeto de trabalho, os termos e os instrumentos arquivísticos utilizados no ambiente de trabalho do profissional arquivista na atual sociedade.

Arquivologia é a área do conhecimento que estuda a composição e originalidade dos documentos de arquivos, a autenticidade e a organicidade dos documentos segundo sua espécie documental e tipo documental, a estrutura, o formato e os elementos que compõem cada documento que lhes dão validade jurídica, a função e finalidade dos arquivos como lugar de guarda de documentos com valor probatório, científico, histórico, administrativo e jurídico. Razões pelas quais nos mostra a importância do papel da Arquivologia nos estudos em relação à análise diplomáticas e tipológica dos documentos, que tem como fim os arquivos. Os documentos de arquivos devem ser autênticos para cumprirem seus propósitos e terem valor probatório. Uns dos objetivos do arquivo custodiar documentos autênticos. Se um documento não é autênticos não cumpri legalmente seu propósito. Pode-se ser por isso nulo e considerado falso e não cumprir seu objetivo.

Vê-se hoje a necessidade dos cursos de Arquivologia em ensinar sobre os novos formatos de documentos e como manter os princípios diplomáticos arquivísticos nesses documentos digitais.

A Arquivologia é responsável pela formação do profissional arquivista. Encontramos a definição de Arquivologia no Dicionário brasileiro de terminologia arquivística como: “disciplina que estuda as funções do arquivo e os princípios e técnicas a serem observados na produção, organização, guarda, preservação e utilização dos arquivos. Também chamada arquivística.”. (ARQUIVO NACIONAL, 2005, p.37).

Os arquivos existem desde muito tempo, sua existência está relacionada aos conjuntos de documentos, ou seja, as informações registradas nos suportes, para guarda e disponibilização, a fim de servirem como prova de atividades desenvolvidas, de fato histórico, científico, de direitos e obrigações. Entretanto já havia os cuidados com a autenticidade dos documentos como mostra Silvia (1999 p. 46-47).

> (...) os primeiros arquivos reúnem já ingredientes que vieram a tornar-se clássicos e hoje são ainda defendidos pela disciplina (Arquivística). A mais importante das revelações tem a ver com o respeito pelos aspectos orgânicos da estrutura arquivística, como se comprovou em Ebla (Síria). Mas havia também grandes cuidados com a identidade e autenticidade dos próprios documentos. As placas sumérias evidenciam também, desde cedo, uma estrutura diplomática coerente e eficaz, a qual, em grande medida, servirá de modelo às chancelarias europeias das épocas medieval e moderna. A correspondência e os contratos administrativos incluem, conforme os casos, a identificação das partes, o nome das testemunhas ou do escriba, a menção da data e, até, a estampagem de selos de validação. A tipologia documental era muito variada, estando já então definidas as principais categorias que integram os arquivos de época mais recente: cartas régias, tratados internacionais, atas, missivas, contratos, assentos contábeis, censos etc. Nem mesmo estão ausentes os documentos cartográficos como, por exemplo, a placa legendada em caracteres cuneiformes, do século XIII a C; com a representação da cidade de Ninive ou papiro egípicio com a planta topográfica das minas de ouro de Gebel.

Os meios utilizados para registrar as informações são modificados quando surgem novos suportes para registrar e armazenar as informações. Percebe-se que nos primeiros arquivos as informações eram registradas em suportes como pergaminho, material feito da pele de animais. Depois o homem aprendeu a produzir o papiro, material fabricado com o uso de planta.

O desenvolvimento dos instrumentos utilizados para registrar e guardar as informações em meio eletrônico digital permitiu a produção de documentos e arquivos digitais.

Para se entender o que são arquivos digitais é necessário à compreensão de arquivo em sentido geral, o conceito de arquivo antes do seu conceito na forma digital nos ajuda a perceber a função e finalidade dos arquivos, as quais permanecem as mesmas quanto os arquivos digitais.

A diferença assim como no documento convencional e documento digital está nos aspectos físicos ou materiais utilizados para acumular, conservar e acessar os documentos. De acordo com o dicionário de terminologia arquivística do Arquivo Nacional (2005, p. 27) arquivo é formado por um “conjunto de documentos produzidos e acumulados por uma entidade coletiva, pública ou privada, pessoa ou família, no desempenho de suas atividades, independentemente da natureza do suporte”.

Com essa definição percebe-se que o arquivo é constituído por conjuntos de documentos produzidos pelas organizações e pessoas no decorrer das suas atividades, que registram informações em qualquer suporte, com a finalidade de produzir documentos probatórios. Observa-se que independentemente do suporte utilizado para registra às informações, o arquivo é constituído por conjunto de documentos.

Independe a natureza do suporte utilizado para produzir os documentos, qualquer que seja a sua natureza pode ser considerado documento de arquivo, nesse caso a pesquisa concentra-se nos suportes eletrônicos digitais, pois estes permitem a produção de documentos digitais, que por sua vez são os objetos os quais devem ser garantidos os princípios da autenticidade e integridade por meio da certificação digital.

A literatura arquivística denomina todos os documentos que são de arquivo de documentos arquivísticos. Entende-se por documentos arquivísticos aqueles que são produzidos pelas organizações e indivíduos na decorrência de suas atividades.

O arquivo digital é produzido, armazenado e transferido por sistemas informatizados de gerenciamento de arquivos eletrônicos e definido como “documento codificado em dígitos binários, acessível por meio de sistema computacional”. (ARQUIVO NACIONAL, 2005, p.75)

Os arquivos tem a finalidade de ser o local de guarda de informações arquivísticas. A guarda desses documentos está relacionada a outros objetivos, como preservar memória de uma organização e sociedade. Ser locais de prova de

informações diversas contidas nos documentos. Disponibilizar o acesso e disseminação da informação.

A informação em sentido geral pode ser um dado ou conteúdo registrado em algum suporte e capaz de passar uma mensagem compreendida. De acordo o dicionário brasileiro de termos arquivístico do Arquivo Nacional (2005, p. 107) informação é “elemento referencial, noção, ideia ou mensagem contida num documento”. A informação digital também tem a mesma finalidade de passar uma mensagem compreensível, podendo ser um conteúdo, entretanto ela está contida em suportes eletrônicos digitais, criada pela sociedade por sistemas computacionais.

Podemos afirmar que todas as organizações públicas ou privadas produzem documentos de arquivos. Seja documentos com valor administrativo, financeiro, fiscal, jurídico, de identificação, pessoal, acadêmico e histórico de saúde.

Os documentos quando produzidos e armazenados em sistemas eletrônicos digitais são definidos como documentos arquivísticos digitais e recebem geralmente um complemento em sua nomenclatura em relação ao convencional, por exemplo, o prontuário do paciente e o processo, que na forma digital é prontuário eletrônico e processo eletrônico. O arquivo digital é produzido, armazenado e transferido por sistemas informatizados de arquivos eletrônicos.

Alguns especialistas mostram a necessidade dos arquivistas em abordar mais sobre as ferramentas de produção, tramitação e disseminação da informação e de documentos, que possibilitam a gestão dos documentos digitais, já que as organizações a utilizam em seu ambiente de trabalho.

Arquivista é o “profissional de nível superior, com formação em Arquivologia ou experiência reconhecida pelo Estado.” (ARQUIVO NACIONAL, 2005, p. 26).

3.1 COMPETÊNCIA DO ARQUIVISTA RELATIVA AOS DOCUMETOS ARQUIVÍSTICOS DIGITAIS

São necessárias ao arquivista novas competências além das tradicionais, ao atuar na gestão de arquivos eletrônicos nas organizações, que utilizam sistemas de arquivos eletrônicos. São demandadas habilidades em trabalhar com essas tecnologias para administrar os documentos digitais em observar os elementos que dão autenticidade e garantem sua integridade, também deve considerar a interdisciplinaridade com profissionais de outras áreas que trabalham diretamente com essas ferramentas.

> Para serem bem sucedidos, devem retificar-se a si próprios e às suas relações com as organizações produtoras. Este desafio não é opcional: perderão influência e relevância a menos que desenvolvam soluções para responder às necessidades dos seus clientes em matéria de arquivos electrónicos. Mas se responderem estrategicamente, reposicionando-se institucional e profissionalmente, as perspectivas são otimistas. Para isso têm de adquirir novas competências e aprender a trabalhar com terceiros que detêm as competências necessárias à gestão dos documentos de arquivos eletrônicos. (CIA, 2005, p. 27).

Em todas as áreas profissionais o auxílio de campos diferentes é fundamental para o desenvolvimento de certas atividades. É importante e necessário para o arquivista o trabalho em equipe com profissionais de outras áreas de conhecimento, que tem como objeto profissional as tecnologias da computação, a certificação digital e a relação jurídica dos documentos.

O relacionamento entre as áreas pode ajudar a compreender os significados e funcionamentos das ferramentas que são utilizadas em no seu ambiente de trabalho na gestão da segurança dos documentos digitais e a desenvolver suas atividades na gestão e preservação das informações e documentos arquivísticos digitais autênticos e confiáveis.

O conhecimento da computação pode ajudar a entender melhor o funcionamento e estrutura dos sistemas de arquivos eletrônicos digitais, esses conhecimentos são básicos para compreensão de um sistema de certificação digital, que objetiva a autenticidade dos documentos digitais.

Embora o aperfeiçoamento que se deve ter diante dos problemas profissionais cabe ao interesse de cada profissional. A preservação digital de documentos arquivísticos autênticos é uma função arquivística, para sua concretização há necessidade da interdisciplinaridade com outros profissionais. É fundamental o conhecimento dos princípios da autenticidade, integridade, confiabilidade, informática, softwares, hardwares, sistemas de arquivos digitais, sistemas de gestão de documentos eletrônicos e preservação digital.

A consciência da realidade, que mostra o envolvimento da Arquivologia com conhecimentos de campos como a diplomática, tecnologias da informação e com disciplinas voltadas para a verificação da autenticidade dos documentos digitais pode ser observada na grade curricular dos cursos de Arquivologia de algumas universidades Federais e Estaduais do país, que oferecem atualmente disciplinas voltadas para a diplomática e para o uso das tecnologias informatizadas de gestão de documentos digitais. Entretanto a pesquisa não aprofunda o estudo nas disciplinas, mas nos objetos que elas estudam os documentos digitais, a autenticidade digital, os princípios diplomáticos aplicados aos documentos digitais por meio das técnicas de segurança especificamente a aplicação da certificação digital. Não há como aprofundar o conhecimento sobre certificação digital sem antes ter noção básica das tecnologias digitais como a computação e informática.

Esses conhecimentos podem ajudar a ter compreensão de como são produzidos documentos arquivísticos digitais e identificar a autenticidade desses documentos. A certificação digital originou-se posteriormente a criação da informática, que no início preocupava-se em transmitir dados e informações. A implantação e utilização da certificação digital são realizadas com a própria tecnologia, por isso é fundamental conhecimentos básicos de computação, hardware e software.

Quadro 2: cursos de Arquivologia com disciplinas de diplomática, informática e autenticidade

Arquivologia Universidades			
UFAM	UFMG	UEPB	UNESP
Diplomática; Gerenciamento Eletrônico de Documentos Arquivístico.	Diplomática; Introdução à Informática; Gestão Arquivística de Documentos Digitais.	Diplomática; Documento Digital.	Diplomática; Gerenciamento Eletrônico de Documentos; Introdução à Ciência da Computação; Autenticidade Digital; Arquitetura da Informação Digital; Preservação Digital; Repositório
UFRGS	**FURG**	**UEL**	**UFBA**
Diplomática; Documento Digital; Gerenciamento Eletrônico de Documentos Arquivístico.	Diplomática; Produção de Documentos Eletrônicos; Gerenciamento Arquivístico de Documentos Eletrônicos.	Diplomática Contemporânea; Preservação de Documentos Digitais.	Diplomática; Preservação Digital Gerenciamento Eletrônico de Documentos.

Fonte: elaboração própria.

Para compreender a certificação digital é importante também conhecer a razão do seu uso, finalidade e funcionamento. Embora não foi encontrada nenhuma disciplina específica “Certificação Digital”, essas disciplinas nos cursos de Arquivologia referentes à diplomática contemporânea e voltadas para o ambiente digital podem ajudar a entender os fundamentos dos princípios da diplomática, da ciência da computação, da produção e gerenciamento de documentos eletrônicos e da autenticidade digital.

A autenticidade pode ser garantida com o certificado digital e assinatura digital. A integridade pode ser observada com sistemas de verificação de assinatura digital para saber se um documento sofreu ou não adulteração desde sua existência.

Para aplicar essas técnicas são utilizadas programação de procedimentos automatizados, que utilizam ferramentas de criação de sistemas informatizados de gerenciamento de dados e informações, através do uso de linguagens de programação e lógica de programação. A certificação emitido pelas Acs da ICP-Brasil pode ser uma alternativa aliada nos SIGADs como mais um instrumento de segurança na gestão de documentos digitais.

4. UTILIZAÇÃO DAS TECNOLOGIAS NA PRODUÇÃO DE DOCUMETOS ARQUIVÍSTICOS DIGITAIS

Para serem produzidos informação e documentos arquivísticos digitais e realizar o seu armazenamento, a sua recuperação e acesso são necessário o computador, que são formados por hardwares e softwares. As partes físicas como do monitor, placa mãe e de vídeo são considerados hardware. Já os sistemas e programas lógicos são conhecidos como softwares, que através das funcionalidades do hardware e de programação são utilizados para processar informações. As informações podem ser armazenadas em suportes de armazenamento de dados como o Disco Rígido, HD, CD e DVD. Com os softwares ou sistemas de gestão de documentos é possível produzir, acessar, reproduzir e transmitir dados e documentos.

Essas ferramentas são tão eficientes e eficazes, que as organizações tem se tornados dependentes desses recursos objetivando obter eficiência, rapidez e segurança na gestão e gerenciamento das informações e documentos. Essas tecnologias também são usadas para a implantação de sistemas de certificação digital.

Dorneles e Corrêia (2013, p. 4) afirmam a revolução das tecnologias da informação nos processos de criação de documentos e a importância dos profissionais da Arquivologia em compreender esse fenômeno de produção dos documentos digitais, da legalidade e autenticidade, devido à preservação da memória social por meio do meio eletrônico. Seja por deveres para comprovação de

informações digitais geradas na decorrência das atividades, que precisam ser preservadas para prestação de dados e informações, seja por colaboração dos conteúdos para pesquisa e disseminação do conhecimento.

> As tecnologias da informação e as novas formas de produzir, disseminar e recuperar o conhecimento revolucionou os processos de criação de documentos [...] Um problema, contudo permanece em aberto, a questão da legalidade e autenticidade das informações contidas nos registros gerados na forma digital bem como a discussão das novas formas de preservação desses documentos certificados digitalmente.
>
> Para os profissionais da Arquivologia é relevante compreender esses processos de produção, tramitação, utilização e armazenamento de documentos digitais. Uma vez que, permitirá a preservação da memória da sociedade, devidamente registrada nesse tipo de suporte.

A verificação dos aspectos relacionados à produção de documentos para identificar os elementos que caracterizam a autenticidade pode ser realizada quando o profissional compreende seu contexto de origem e identifica os elementos na estrutura documental. “Os estudos de diplomática e tipologia levam a entender o documento desde o seu nascedouro, a compreender o porquê e como ele é estruturado no momento de sua produção.” (BELLOTO, 2004, p. 45). Essa compreensão é fundamental para a análise diplomática do documento. Através da qual é possível perceber os elementos que proporcionam a autenticidade do documento.

4.1 TRANSAÇÕES EM MEIO ELETRÔNICO QUE GERAM DOCUMENTOS DIGITAIS

As transações em ambientes digitais são realizadas por pessoas físicas, jurídicas, organizações, sistemas de intranet, servidor web ou qualquer responsável que produza um documento ou informação digital ao realizar atividades na função de cargos, ou como cidadão em busca de serviços, produtos e informações através dos sistemas computadorizados. Daí surge à importância de segurança e autenticidade nessas transações, a certificação digital foi criada com a finalidade de garantir essas possibilidades.

Os sistemas eletrônicos permitem a possibilidade de adulteração das informações arquivísticas registradas em suportes eletrônicos digitais. A certificação digital da infraestrutura de chaves públicas do Brasil pode ajudar a evitar que documentos digitais não autênticos sejam preservados, através da conferência da autenticidade do documento. Foi justamente para garantir a segurança em transações econômicas realizadas em meio eletrônico, o que levou alguns países a criar leis para regulamentar a segurança dessas transações.

Com relação aos aspectos jurídicos desses novos tipos de documentos observa-se que vários países tem buscado uma maior garantia no nível de segurança com relação à autenticidade para garantir a validade jurídica dos documentos digitais, pois sabemos que a fácil manipulação e adulteração dessas informações e documentos tem sido a razão de se buscar mecanismos de segurança, que possam garantir a autenticidade dessas informações e documentos digitais e garantir sua validade jurídica. Importante frisar que cada país tem a sua própria regulamentação.

Na Europa em 1999 o Parlamento Europeu e o Conselho da união Europeia fixaram por meio da directiva 1999/93 à regulamentação da assinatura digital. Em 2001 Alemanha e Argentina criam leis relativas à assinatura digital e assinaturas eletrônicas. A Alemanha por meio da lei Federal *BGBl. I, S. 876* institui à assinatura eletrônica. A Argentina pela lei 25.506 de 14 de novembro reconhece a firma eletrônica e digital e sua eficácia jurídica.

A comissão das nações unidas com a finalidade de assegurar o direito internacional na segurança dos dados automatizados produzidos por meio do comercio eletrônico cria a lei modelo das assinaturas eletrônicas, onde defini termos utilizados na assinatura eletrônica.

Em 2003 a Espanha aprovou e estabeleceu por meio da lei 59/2003 o regulamento da assinatura eletrônica e dos serviços de certificação. O MERCOSUL reconhece a eficácia jurídica da assinatura eletrônica para o aproveitamento sócio econômico e garantir segurança e confiança nos documentos eletrônicos, de acordo a resolução 36/06 a assinatura eletrônica avanças baseadas em certificados reconhecidos permitem alcançar um maior nível de segurança. Esse nível de

segurança é importante para garantir a realização de transações seguras, a autenticidade, integridade e confidencialidade em meio digital.

5. PRINCÍPIOS DA AUTENTICIDADE E INTEGRIDADE EM CERTIFICAÇÃO DIGITAL

A verificação da autenticidade e integridade do documento digital pode ser realizada com ferramentas da certificação digital, que é o ato de certifica-se através da análise dos elementos necessários se o documento analisado preenche os requisitos necessários para serem autênticos e se esses elementos analisados comprovam de fato a autoria do documento.

A definição da disciplina diplomática e esclarecimento do seu objeto de estudo são fundamentais para compreender os princípios originados pelos seus estudos e que hoje são objetos que a certificação digital procura garantir, por meio de aplicação tecnológica. Tecnológica porque não é somente o uso de ferramentas, mas de estudos arquivísticos diplomáticos contemporâneos e jurídicos. No dicionário de terminologia arquivística diplomática é “disciplina que tem como objeto o estudo da estrutura formal e da autenticidade dos documentos”. (ARQUIVO NACIONAL, 2005, p. 70).

Os estudos dos princípios da autenticidade da diplomática contemporânea podem servir de subsídios aos estudos da Arquivologia, razão pela qual essa disciplina consta na grade cursos de Arquivologia de Universidades Federais e Estaduais no país.

> A apropriação da arquivística pela diplomática e o uso da crítica diplomática para compreensão dos documentos gerados no tempo de hoje dará origem a chamada diplomática contemporânea, que encontra na América do Norte, mas precisamente nos estudos de Luciana Duranti, um lócus investigativo privilegiado. (TOGNOLI; GUIMARÃES, 2009 p. 33).

Os estudos com relação à autenticidade, integridade, fidedignidade e confidencialidade dos documentos eletrônicos têm sido discutidos em várias partes

do mundo, dando origem às teorias conceituais capazes de identificar se um documento eletrônico é realmente autêntico. Ação necessária para que os documentos digitais sejam aceitos legalmente diante do direito. Os estudos desses princípios, as técnicas, e normalização da certificação digital são realizados com a pretensão de garantir segurança nas transações eletrônicas, que são realizadas por meio dos sistemas computacionais, essas transações acabam por produzir informações e documentos digitais para realizar acordos, comercio eletrônico, contratos, obtenção de certidão e quaisquer outras atividades, através de sistemas informatizados.

O projeto INTERPARES tem desenvolvido vários estudos voltados para a análise de como os documentos digitais podem ser autênticos e garantir a integridade do seu conteúdo. No próprio site do INTERPARES é possível verificar os conceitos dado pelos pesquisadores de autenticidade, integridade, confiabilidade e completude do documento eletrônico. O projeto Interpares I iniciado em 1998 disponibilizou no seu site o trabalho “A preservação em longo prazo de registros eletrônicos autênticos” onde traz a definição de autenticidade como a qualidade de ser autênticos e dignos de aceitação com base em fatos.

A diplomática contemporânea ou diplomática arquivística vem colaborando significativamente para o desenvolvimento dos estudos quanto a esses princípios a fim de permitir a identificação da autenticidade de documentos. A certificação digital utiliza ferramentas para garantir a autenticidade e que são capazes de identificar a integridade e autenticidade de documentos digitas, e se não sofreu adulterações em seu conteúdo.

O Conselho Nacional de Arquivos por meio da resolução 37 estabelece diretrizes para presunção de autenticidade de documentos arquivísticos digitais, esse documento afirma que a presunção da autenticidade dos documentos arquivísticos digitais não se limita as características físicas nem em soluções das tecnologias, mas também com instrumentos usados na análise diplomática à forma, o conteúdo e o ambiente de produção dos documentos digitais como nos mostra a citação CONARQ abaixo:

> Os documentos arquivísticos digitais apresentam dificuldades adicionais para presunção de autenticidade em razão de serem facilmente duplicados, distribuídos, renomeados, reformatados ou convertidos, além de poderem ser alterados e falsificados com facilidade, sem deixar rastros aparentes. Assim, a presunção de autenticidade do documento arquivístico digital é realizada por meio da análise da sua forma e do seu conteúdo, bem como do ambiente de produção, manutenção/uso e preservação desse documento, e não apenas com base em suas características físicas ou em soluções tecnológicas. (CONARQ, 2012, p. 1).

Ao falar sobre a fidedignidade do documento eletrônico Rondinelli (2005, p. 64) afirma que “esta relacionado ao momento de criação do documento e, portanto, refere-se ao grau de completude da sua forma intelectual e de controle dos seus procedimentos de criação”. De acordo com projeto sobre a preservação da integridade dos registros eletrônicos desenvolvido pelo Interpares por Luciana Duranti e com a participação dos colaboradores East Wood e Mac Nel um registro é completo quando “tem todos os elementos da forma exigida pelo sistema jurídico em que é criado” (INTERPARES, 1997).

Completude significa algo que é completo, com relação a completude da forma intelectual e de controle de criação do documento eletrônico, significa que ele obedece todos os requisitos necessários do sistema jurídico em que foi produzido.

Com relação aos elementos que compõe ao grau de completude, os quais podem garantir fidedignidade em um documento eletrônico, Rondinelli descreve novos elementos que deverão ser observados em uma análise diplomática, “à data faz-se necessário acrescentar a hora da transmissão aos destinatários, externos ou internos, e ao dossiê ao qual pertence”.

Duranti citada por Rondinelli, explica o que são documentos legalmente autênticos e diplomaticamente autênticos. Durante (1995, apud Rondinelli, 2005):

> Documentos legalmente autênticos são aqueles que dão testemunho sobre si mesmos devido à intervenção, durante ou após sua criação, 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 com (os) nome(s) da (s) pessoa(s) componente(s) para criá-los [“...]”.

O conjunto de elementos a serem observados para a autenticidade dos documentos digitais de acordo com Mac Neil (2000, apud Rondinelli, 2005) é:

> Data do documento, hora e lugar da criação, transmissão e recebimentos, identificação dos nomes do autor, destinatário e escritos (se cada um ou ambos forem diferentes do autor), nome (ou timbre), do criador, título ou assunto, código de classificação e qualquer outro elemento exigido pelos procedimentos do criador e/ou sistemas jurídicos.

Esses dados permitem verificar a autenticidade dos documentos digitais. Assim como para verificar a autenticidade nos documentos convencionais por meio da data, hora, lugar de produção, identificação dos autores, destinatários, identificação do produtor pessoa ou organização, o assunto e assinatura esses elementos são fundamentais para garantir a autenticidade dos documentos digitais. Acrescidos a esses dados existem outros elementos a serem obervados na verificação dos documentos digitais devido à necessidade de se comprovar a hora de transmissão e recebimento do documento via sistema informatizado.

Carimbo do tempo utilizado na certificação digital é uma tecnologia capaz de registrar o momento em que foi realizada uma assinatura por um signatário, garantido assim o atributo da tempestividade, que um documento deve conter. A tempestividade de um documento é a capacidade que um documento tem de provar o dia, hora e local de sua produção.

Os metadados do documento eletrônico servem para fazer a sua análise quanto à autenticidade e fidedignidade. A observação e identificação desses elementos no documento são necessários para identificar a sua origem, a data de criação, o local onde foi produzido, o criador, destinatário e assunto. Segundo Rondinelli (2002, p. 62) os “Metadados, portanto, se constituem em componentes do documento eletrônico arquivístico e em instrumentos para sua análise diplomática.”.

Quadro 3 : elementos dos documentos digitais

Mac Neil	Certificado Digital
Data do documento	Título
Hora e lugar da criação, transmissão e recebimento	GERAL: A finalidade, destinatário, data de validade,
Identificação dos nomes do autor, destinatários, escritor e do criador	DETALHES: Versão, número da série, algoritmo hash, emissor, requerente, chave pública, tipo de requerente, uso da chave
Título ou assunto	CAMINHO: Autoridade Raiz à certificado do usuário final.
Código de classificação	
Outros que possam ser exigidos pelo sistema jurídico	

Fonte: elaboração própria com referência dos elementos prepostos por Mac Nel.

Os elementos necessários à constituição do documento eletrônico envolvem vários aspectos, depende do tipo de documento, da finalidade do documento, das partes envolvidas, do produtor, dos sistemas jurídicos que regulamenta e padronizar a forma, estrutura e elementos do documento digital que será produzido. Uma espécie e tipo de documento podem conter elementos a mais ou diferente que outro, depende dos fatores envolvidos. O documento autêntico não significa que haja veracidade em seu conteúdo, ou seja, a sua autoria pode ser verdadeira, mas o conteúdo não.

É importante diferenciar autenticidade de autenticação. Um documento é autêntico quando prova que foi produzido de fato pela pessoa ou organização que evidência ter sido produzido, através da comprovação da autoria ou da identidade dos autores. A autenticação ocorre quando uma autoridade competente confirma a

originalidade de um documento, é uma atestação de que a cópia do documento original autenticada representa o original em sua integridade.

Um documento mantém sua integridade quando seu conteúdo não sofre adulteração, apresentando a mesma forma e originalidade de quando foi validado com a assinatura dos autores necessários para sua concretização.

Existem documentos que para terem valor jurídico e serem capazes de concretizar o seu objetivo deve seguir uma padronização imposta pelo direito por meio da normalização ou padronização. A padronização é uma forma de garantir a autenticidade do documento e a normalização para garantir que o documento criado e observância as normas tenham valor jurídico e possa ter efeito judicial.

A observância e aplicação das normas jurídicas e regulamentos do órgão produtor é um papel arquivístico e um elemento a estar no planejamento do arquivista ao participar da criação de novos documentos, pois essa observância evitará a produção de documentos não autênticos.

Os documentos digitais são produzidos pelas atividades realizadas pelas organizações e sociedade em sistemas computacional, como as transações comerciais eletrônicas, arquivos criados, armazenados e enviados com o uso das novas tecnologias da informação e comunicação.

Entretanto esses documentos passaram a ser regulamentados constitucionalmente e a ter validade jurídica no mundo e no Brasil há pouco tempo. Há pouco mais de uma década atrás quando se observa a regulamentação das assinaturas digitais na Europa em 1999 para garantir o desenvolvimento do comercio eletrônico e para isso a necessidade de transações seguras.

É importante notar que as transações comerciais eletrônicas acabam por produzir documentos arquivísticos digitais, que são provas de registro de relações de transações realizadas em suportes digitais, como acordos, contratos e compras.

Grandini et-al (2002, p. 1) declaravam no as problemáticas causadas pela produção dos documentos digitais quanto a sua validade diante do direito e da sociedade, o que para os autores apresentavam grandes empecilhos para o

desenvolvimento do comercio eletrônico, sugerindo uma reformulação das leis que legalizasse também o uso da documentação digital, pois no Brasil,

> Sabemos que muitos ordenamentos jurídicos não estavam preparados para lidar com esse fenômeno, pois a maioria dos Estados preceitua regras de validade dos negócios jurídicos baseados em documentos escritos e memorizados sobre o papel. Assim, com essa nova forma de negociar e "assinar" alguns questionam a natureza jurídica, os efeitos, a segurança e, principalmente, a validade dos documentos digitais, diante da inicial insegurança do Direito e da sociedade perante eles.
>
> A falta de regulamentação dos documentos digitais representa hoje um dos maiores empecilhos ao desenvolvimento do comércio eletrônico. Por essa razão, os países precisam reformular suas leis, adequando-as à nova realidade, em busca de dar amparo legal e igualitário ao uso tanto da documentação tradicional quanto da digital.
>
> O receio que existe ainda hoje de estabelecer pactos via documentos digitais, como é o caso da *Internet,* faz com que juristas e técnicos passem a se preocupar com a garantia da segurança e validade jurídica de tais negócios. De tal modo, ferramentas de apoio vão sendo criadas com a finalidade de impedir ataques às redes e também vão surgindo sistemas protetores contra operações ilegais.

Casa Grande (2011, p. 9) nos afirma a importância das novas tecnologias nas relações da sociedade, mas também fala dos ricos que estas podem trazer com relação à necessidade da confidencialidade:

> Os níveis de interação proporcionados pelas novas tecnologias vem abrindo novos campos de oportunidades. Revolucionando as relações pessoais, sociais, comerciais, etc. As opções parecem infindáveis. Algumas barreiras, no entanto, tem impedido ou dificultado esses avanços. Dentre elas, as crescentes relações que dependem da Internet. Um meio que oferece muitos riscos e carece de confidencialidade.

O autor continua sua análise e reafirma o próprio uso das novas tecnologias para resolver os problemas de confidencialidades dizendo que "na busca por soluções, novas tecnologias têm sido empregadas. A Certificação Digital se apresenta como uma das alternativas viáveis". Casa Grande (2011, p. 9).

Antes do surgimento do computador as organizações trabalhavam com instrumentos tradicionais para produzir os documentos, armazenar e transmitir ou enviar para outros setores e departamentos internos quanto o ambiente externo para outras organizações. As legislações que regulavam os aspectos jurídicos e

diplomáticos da forma e estrutura dos documentos não tinham ainda uma regulamentação aos documentos digitais, pois esses ainda não existiam.

Com o advento da computação e dessas novas tecnologias da informação e comunicação que são criadas, as organizações contemporâneas encontram diversas ferramentas que auxiliam na produção, armazenamento, recuperação, acesso, transmissão e disseminação de documentos digitais, a utilização dessas tecnologias permite originar novos formatos de documentos por meio dos equipamentos eletrônicos.

A revolução do uso dos sistemas informatizados possibilitou a sociedade realizar diversas atividades que consequentemente acaba por produzir documentos digitais, os usuários pode interagir com o ambiente interno e externo das organizações, realizar acordos e compras, consulta de processos, solicitação de certidões, acesso a contas bancárias, firmar contratos, registrar informações em sistemas de gerenciamento de informações e documentos, digitalizar documentos, o que origina a produção de documentos arquivísticos digitalizados.

Com a utilização da certificação digital deixou de existir a exigências de entrega de muitos documentos outrora exigidos em suporte papel. Desse modo muitos profissionais e pessoas deixam de se deslocar até o local onde precisam comprovar dados e informações por utilizar meios eletrônicos na produção de arquivos digitais aceitos pela organização que exige a comprovação dos dados e informações.

Geralmente a própria entidade exigente disponibiliza sistema informatizado para o envio dos dados comprobatórios. Esses sistemas são estruturados e programados com ferramentas de comprovação de dados por meio de usuários e senhas. Outras exigências de comprovação de dados também são solicitadas dependendo das políticas de segurança e mecanismos capazes de garantir a autenticidade e integridade dos dados e informações documentadas.

No Brasil a lei 12.682 de (2012) regulamenta a elaboração, reprodução e arquivamento de documentos públicos e privados em meio eletromagnéticos.

> Art. 3º O processo de digitalização deverá ser realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP - Brasil.
>
> Parágrafo único: os meios de armazenamento de documentos digitais deverão protegê-lo de acesso, uso, alteração, reprodução e destruição não autorizadas.

O Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e tecnologias como o Gerenciamento Eletrônico de Documentos (GED) permitem a gestão de documentos, produção, gerenciamento e preservação de documentos digitais, trazendo soluções para as organizações também na gestão do acúmulo de documentos. Esses instrumentos trouxeram mudanças na maneira de produzir e utilizar os documentos, auxiliando as organizações, na criação, armazenamento e transmissão de documentos e informações digitais.

Por sua vez as relações realizadas com o uso desses instrumentos ao mesmo tempo em que trouxe benefícios tem levantado questões quanto a integridade desses documentos, e alguns países tem criado leis para regulamentar os processos relacionados aos documentos digitais por meio da assinatura digital.

A regulamentação é necessária para garantir a autenticidade dos documentos digitais, para que sejam confiáveis e para que não sejam repudiados juridicamente. As práticas aplicadas na utilização dos documentos por meio dos sistemas de certificação digital devem estar de acordo às normas regulamentadoras.

6. CONSIDERAÇÕES FINAIS

A certificação é vista como um meio que viabiliza garantir os princípios da autenticidade, integridade e confidencialidade dos documentos em meio eletrônico. Tanto é assim que vários países como Alemanha, Argentina, Espanha, Brasil e o MERCOSUL regulamentaram a certificação digital, a fim de garantir transações eletrônicas seguras por meio dos certificados e das assinaturas digitais.

A infraestrutura da certificação digital alinhada às normas, padronizações e regulamentos das Acs da ICP-Brasil garantem a autenticidade e integridade dos documentos digitais assinados digitalmente.

Os aspectos dos princípios da autenticidade das informações registradas são bem antigos, mas com o advento das tecnologias informatizadas, as organizações produzem registros e documentos digitais, devido a isso estudos têm sidos realizados para analisar esses elementos aplicados as informações e documentos em ambientes digitais.

A Arquivística contemporânea percebe hoje os documentos e arquivos digitais como objeto de estudo e trabalho. O Conselho Internacional de Arquivos e o projeto interpares tem desenvolvidos vários trabalhos voltados a análise da autenticidade dos documentos eletrônicos. Os documentos de arquivo, produzidos na decorrência das atividades pelas organizações e indivíduos são informações registradas em qualquer que seja o seu suporte, os documentos digitais, cujas informações são registradas em suportes digitais com a utilização sistemas informatizados.

O documento assinado por meio digital de uma autoridade certificadora da ICP-Brasil ou de outra que não seja da sua hierarquia desde que aceita pelas partes como válidas em acordo tem valor judicial, assim como os documentos válidos em suporte papel.

A regulamentação das assinaturas digitais teve interesse em assegurar o desenvolvimento do comercio eletrônico. Entretanto para isso ser garantido teve-se que garantir a autenticidade e integridade dos documentos digitais, pois esses são intermediários na comprovação e manifestação das ações registradas em suportes digitais.

No Brasil desde a Medida Provisória 2.200 os documentos digitais assinados por uma identidade digital da ICP-Brasil passaram a ser reconhecidos juridicamente. Com a instituição da certificação digital pela ICP-Brasil, as organizações podem encontrar maior segurança na gestão da autenticidade, integridade, confiabilidade e confidencialidade dos registros digitais.

Os sistemas informatizados das organizações certificados pelas ACs interligadas a ICP-Brasil, recebem uma identidade digital, que comprova o endereço de um comutador remoto, por meio do qual é possível realizar atividades de produção e gestão de documentos digitais, assinar os documentos, transmitir ou enviá-los e receber por serviço de protocolo.

Os documentos digitais produzidos pelas organizações certificadas por umas das ACs Brasil tem valor de prova e são autênticos para o direito constitucional.

As instituições arquivísticas podem encontrar na ICP-Brasil uma ferramenta eficiente para manter a segurança da autenticidade das informações e documentos arquivísticos digitais.

REFERÊNCIAS

ARQUIVO NACIONAL (Brasil). **Dicionário brasileiro de terminologia arquivística.** Rio de Janeiro: Arquivo Nacional, 2005. 232p.

ALEMANHA. "Ato de Assinatura de 16 de Maio de 2001 (BGBl. I, p 876), na redacção dada pelo artigo 4º da Lei de 26 de Fevereiro de 2007 (BGBl. I, p 179)". Disponível em: <https://www.certisign.com.br/documents/10163/690007a3-95f5-4bf8-a632-076bcb0e3e1a> Acesso em 30/11/2014.

BELLOTTO, Heloísa Liberalli. **Arquivos permanentes: tratamento documental.** Rio de Janeiro, FGV, 2004, 320p.

Brasil. Decreto nº 3996, de 31 de outubro de 2011, Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. **Diário Oficial [da] Republica Federativa do Brasil**, Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm>. Acesso em 23/08/2014.

BRASIL. Lei nº12682, de 9 de julho de 2012, dispõem sobre a elaboração e o arquivamento de documentos em meio eletromagnéticos**. Diário Oficial [da] Republica Federativa do Brasil,** Brasília, 9 de jul. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12682.htm> Acesso em 02/10/2014

CASA GRANDE, Airton Ruberval**. Avaliação da confiabilidade da Certificação Digital**. 2011. 31 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

CONARQ (Brasil). Resolução nº 37, de 19 de dezembro de 2012. **Diário Oficial [da] República Federativa do Brasil,** Brasília, 19 de dez de 2012. 245º ed. Seção 1.

DIRECTIVA 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 1999. Relativa a um quadro legal comunitário para as assinaturas eletrônicas. Disponível em: <https://www.certisign.com.br/documents/10163/7ddbaaab-52f0-4a14-849a-2caa12e776f2> Acesso em 30/11/2014.

DORNELES, Sânderson Lopes; CORRÊA, Renato Fernandes. **Gestão de Documentos Digitais em Aplicações de Certificação Digital.** v2, n.2, Rio de Janeiro: Informação Arquivística, p. 3 32. Disponível em:

<http://www.aaerj.org.br/ojs/index.php/informacaoarquivistica/article/view/28.> Acesso em 24/08/2014.

ESPANHA. Lei 59/2003 de 19 de dezembro, dispõe sobre assinatura eterônica. Disponível em: <https://www.certisign.com.br/documents/10163/a2921636-8387-4e9f-97b1-1c8e1c15effd> Acesso em: 30/11/2014

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. São Paulo. Atlas. 1999.

GRANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. A validade jurídica dos documentos digitais. In: **Âmbito Jurídico,** Rio Grande, III, n.9, maio 2002. Disponível em: WWW.ambitojuridico.com.br/site/index.php?artigo_id=4411&n_link=revista_artigos_leitura Acesso em 12/09/2014.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). Glossário ICPBrasil. Versão 1.2. 03.10.2007 Disponível em: http://www.iti.gov.br/images/twiki/URL/pub/Certificacao/Glossario/Glossario_ICP_Brasil_Versao_1.2_novo-2.pdf. Acesso em: 10/10/2014.

INSTITUTO NACIOAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). A certificação digital entre nós. Disponível em: <http://www.iti.gov.br/noticias/iti-na-midia/1056-a-certificacao-digital-entre-nos> Acesso em 09/10/2014.

INSTITUTO NACIOAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). Comitê Gestor. Disponível em: http://www.iti.gov.br/icp-brasil/comite-gestor.

INSTITUTO NACIOAL DE TECNOLOGIA DA INFORMAÇÃO (Brasil). Estrutura Completa ICP-Brasil. Disponível em: <http://www.iti.gov.br/images/icp-brasil/estrutura/2014/atualizacao18/Estrutura_completa.pdf> Acesso em: 01/11/2014.

INTERNATIONAL COUNCIL ON ARCHIVES. Documentos de arquivos eletrônicos: Manual para Arquivistas. Disponível em: <file:///C:/Users/user/Downloads/ICA_Study-16-Electronic-records_PT.pdf.> Acesso em: 10/10/2014.

LARKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. São Paulo. Atlas, 2010.

MERCOSUL Res.37/06 Reconhecimento Jurídico da Eficácia
do Documento Eletrônico, a assinatura electrónica e a Eletrônica Avançada

Assinatura no dóminio do MERCOSUL. Disponível em: <https://www.certisign.com.br/documents/10163/b5c3f561-069a-4943-9d27-7e15805c17f1> Acesso em: 30/11/2014.

MONTEIRO; MIGNONI. **Certificados digitais conceitos e práticas.** 2007, p.34. Disponível em: <http://www.pontodeensino.com/livros/livro_certificados_digitais.pdf> Acesso em: 07/09/2014.

PAULA, S. d. **CERTIFICAÇÃO DIGITAL E ASSINATURA DIGITAL: A experiência da USP.** P.19. Disponível em: <http://www.usp.br/arquivogeral/wp-content/uploads/anexo/palestras/silvio.pdf> Acesso em 07/09/2014.

Requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da icp-brasil. 18 de dezembro de 2010. Disponível em: http://www.iti.gov.br/images/legislacao/Docicp/DOC-ICP-04_-_Versao_5.3_-_REQ._MIN._PARA_AS_PCs_NA_ICP-BRASIL_29.04.2014.pdf. Acesso em: 25/06/2014.

RONDINELLI, R. C. **Gerenciamento Arquivístico de documentos eletrônicos: uma abordagem da diplomática arquivística contemporânea.** 4ed. Rio de janeiro. FGV, 2005. 160p.

SILVA, A. M., et al. **Arquivística: teoria e prática de uma ciência da informação.** Porto: Afrontamento, 1999.

TOGNOLI, N. B; GUIMARAES, J. A. C. **A diplomática contemporânea como base metodológica para organização do conhecimento arquivístico: perspectiva de renovação a partir das ideias de Luciana Duranti.** 2009, SP. Disponível em: <file:///C:/Users/user/Downloads/Dialnet-ADiplomaticaContemporaneaComoBaseMetodologicaParaA-2921994%20(6).pdf> Acesso em 01/10/2014