CERTIFICAÇÃO DIGITAL E ARQUIVOLOGIA: benefícios e aplicações

Tatiane Rodrigues do Nascimento
Kátia Viana Cavalcante
Felipe Vlaxio

RESUMO: A sociedade da informação abriu novos campos e oportunidades, e a informação nas redes digitais ganhou dimensões sem fronteiras, surgindo a necessidade de políticas de segurança para garantir a autenticação, privacidade, autorização e integridade dos dados. A solução encontrada para solucionar esses problemas foi a utilização de um sistema de criptografia. O governo brasileiro criou padrões técnicos para suportar um sistema criptográfico, chamado de Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), com o objetivo de regulamentar o uso de certificados digitais. Com o surgimento e crescimento intenso desse novo formato de documento, a Arquivologia sentiu necessidade de incorporar essa ferramenta. Se por um lado a assinatura digital confere autenticidade e integridade à informação, por outro os avanços não garantem a sua preservação no longo prazo. O valor legal da autenticidade desse documento está relacionado às assinaturas digitais. Sob a ótica da arquivística e da diplomática, a autenticidade dos documentos não depende apenas da assinatura, mas de um conjunto de elementos. O presente trabalho tem por objetivo analisar o mercado de certificado digital na cidade de Manaus, sob a ótica da Arquivologia, ou seja, da autenticidade e sigilo nos documentos digitais. Metodologicamente, refere-se a uma pesquisa de natureza qualitativa, com caráter exploratório-descritivo, realizada por meio de um estudo de caso e por possuir um objetivo definido. Buscou-se avaliar se as autoridades certificadoras possuem estruturas para garantir a segurança e transação dos documentos digitais na cidade de Manaus-AM. Como resultado, observou-se que o setor financeiro foi o primeiro a utilizar o certificado digital, seguido pelo setor fiscal, que ganhou destaque com a nota fiscal eletrônica, e mais tarde pelo judiciário, com o processo eletrônico, que ao mesmo tempo foi responsável por aumentar o número de advogados utilizando a assinatura digital. Foi constatado que a aplicação da certificação digital sobre informações registradas em suportes digitais garante a autenticidade, confidencialidade e integridade. No entanto, para que isto aconteça, é necessário que sejam observadas as normas e padrões estabelecidos pela ICP-Brasil. O uso do certificado digital para a Arquivologia

Tatiane Rodrigues do Nascimento
tatinas7@gmail.com
http://lattes.cnpq.br/0829261260888181
Bacharel em Arquivologia

Kátia Viana Cavalcante
kcavalcante@ufam.edu.br
http://lattes.cnpq.br/2715253110435470
Professora da Universidade Federal do Amazonas (UFAM) do Departamento de Arquivologia e Biblioteconomia. Doutora em Desenvolvimento Sustentável pela Universidade de Brasília. Mestre em Comunicação e Semiótica pela Pontifícia Universidade Católica de São Paulo.

Felipe Vlaxio
felipevlaxio@gmail.com
http://lattes.cnpq.br/8548694647391969
Graduando em Biblioteconomia

Submetido em: 30/03/2015
Publicado em: 14/06/2015

agrega valor tanto para a gestão documental como para a preservação dos documentos permanentes.

PALAVRAS-CHAVE: Arquivologia. Certificação digital. Documento digital. Assinatura digital.

1 INTRODUÇÃO

O advento da internet, intensificado no início dos anos 90, bem como o aumento do uso de computadores na vida das pessoas e nos processos institucionais contribuíram e contribuem para o crescimento de transações de bens, serviços e informações realizadas no ambiente digital. As relações nessa nova sociedade da informação abriram novos campos e oportunidades, a informação nas redes digitais ganhou dimensões, surgindo a necessidade de políticas de segurança para garantir a autenticação, privacidade, autorização, integridade dos dados. A solução encontrada para solucionar esses problemas foi a utilização de um sistema de criptografia.

A criptografia passou a ser estudada e usada por vários países que possuem leis, normas e padrões diferentes. O governo brasileiro criou em 2001 padrões técnicos para suportar um sistema criptográfico, chamado de Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), com o objetivo de regulamentar o uso de certificados digitais.

O Instituto Nacional de Tecnologia da Informação (ITI) é o responsável por manter a ICP-Brasil e executar as políticas de certificados e normas. Possui um Comitê Gestor que estabelece a política, os critérios e as normas para licenciamento de Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviços de suporte em todos os níveis da cadeia de certificação, credenciando as respectivas empresas na emissão de certificados no meio digital.

Com a adoção do sistema de emissão de nota fiscal eletrônica NF-*e* pelas empresas, o volume de emissões e procura por certificados digitais foram mais intensos entre companhias de pequeno e médio porte. Desta feita, a tendência é que esse crescimento se torne mais acelerado com a utilização de certificados digitais em outras aplicações de empresas e setor público. Atualmente, vários setores da sociedade estão utilizando a certificação digital e pode-se citar como exemplo: os Governos Federal, Estadual e Municipal; Sistema Judiciário; Cartório Eletrônico; Sistema de Saúde, entre outros.

O Instituto Tecnologia da Informação (2014) revela que a emissão de certificados digitais no Brasil nos últimos dez anos

foi de seis milhões de certificados digitais, e que somente no ano 2013 foram emitidos mais de dois milhões deles.

Com o surgimento e crescimento intenso do uso do documento digital, a Arquivologia sentiu necessidade de incorporar essa ferramenta. Se por um lado a assinatura digital confere autenticidade e integridade à informação, por outro os avanços tecnológicos – incluindo avanços criptográficos, revogação e expiração da assinatura digital – não garantem sua preservação a longo prazo. O valor legal da autenticidade desse documento está relacionado às assinaturas digitais. Sob a ótica da arquivística e da diplomática, a autenticidade dos documentos não depende apenas da assinatura, mas de um conjunto de elementos. Entretanto, do ponto de vista jurídico, a assinatura ocupa um papel chave.

As assinaturas digitais e seu uso em documentos digitais, em justaposição a todos os pré-requisitos de segurança, são equiparados às assinaturas convencionais. Todavia, no caso da assinatura digital, essa ligação entre o documento e o autor é feita por um algoritmo de autenticação. Tanto as assinaturas manuscritas quanto as assinaturas digitais estabelecem os mesmos objetivos e finalidades, ou seja, a de possibilitar ao criador que o documento criado não seja alterado ou violado.

Nesse sentido, o trabalho buscou responder a seguinte pergunta: Os mecanismos usados são capazes de confirmar a autenticidade e o sigilo das informações? Para tanto, traçou-se como objetivo analisar o mercado de certificado digital na cidade de Manaus, sob a ótica da Arquivologia, ou seja, da autenticidade e sigilo nos documentos digitais.

2 FUNDAMENTOS TEÓRICOS E CONCEITUAIS

A intensidade do desenvolvimento nas últimas décadas do século XX consolidou a chamada sociedade da informação, onde as tecnologias de informação e das comunicações (TIC's) invadiram praticamente todas as áreas de atividades humanas, muitas vezes sem que os cidadãos se apercebessem da extensão da sua penetração nos aspectos mais comuns da vida em sociedade (BRITO et al., 1999).

As TIC's foram responsáveis por desenvolver novas atividades econômicas na prestação de serviços, nos meios de comunicação, no entretenimento, no comércio eletrônico, no desenvolvimento de *software* e em outros ramos que envolvem a economia digital. Esta nova economia se baseia na infraestrutura de comunicação, e, nesse novo contexto, as pessoas e organizações têm alterado seus hábitos de consumo. Desta feita, as empresas viram uma oportunidade de aumentar

seus negócios e passaram a atuar no mercado de transações online que ficou conhecido como *e-business*.

Surgem então termos como: *e-business*, que descreve o uso de meios e plataformas eletrônicos para conduzir os negócios de uma empresa; o *e-commerce,* expressão que deriva do termo comércio eletrônico, onde as negociações são realizadas exclusivamente pelo formato eletrônico. O *e-commerce* possui vários tipos de transações que ocorrem entre pessoas, empresas e até mesmo governos, onde todos buscam relacionar-se para realizar negócios (TURBAN, 2005). O crescimento deste ramo comercial incentivou o surgimento de novas ferramentas, principalmente no mercado de serviços fiscais e bancários. É o caso, por exemplo, da **NF-e**/Nota Fiscal Eletrônica e do ***e-Boleto***/Boleto Eletrônico.

No entanto, o uso dessas novas ferramentas impõe limitações que surgem o tempo inteiro, como: barreiras tecnológicas, manutenção de *hardware e software* apropriados para o gerenciamento, e, principalmente, a necessidade da segurança nas transações e dos novos formatos de documentos que são gerados no ambiente digital (STALLINGS, 2008).

Os serviços de segurança implementam diretrizes, que são classificadas em cinco categorias: autenticação, privacidade, autorização, integridade e irretabilidade, que ditarão as regras que baseiam toda a confiança dos sistema (MACHADO, 2010).

Todavia, os mecanismos utilizados para a segurança da informação são bem específicos, a certificação e assinatura digital. A certificação digital assegura a autenticidade da assinatura digital combinando aspectos tecnológicos e jurídicos (PEREIRA, 2009).

O certificado digital é um arquivo de computador, que como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade possuem também uma Chave Pública do Assinante. Estes documentos eletrônicos são chancelados digitalmente pela entidade emissora, conhecida como Autoridade Certificadora, com o objetivo de interligar a Chave Pública a uma pessoa ou entidade, possuindo o mesmo valor de um documento físico (MONTEIRO; MIGNONI, 2007).

A assinatura digital é um sistema de identificação numérico, que faz uso da criptografia, capaz de prover os requisitos de validade do documento. Na criptografia são usados dois tipos de chaves para cifrar e decifrar as informações. Seu uso como forma de garantir a confidencialidade de uma informação é composto por três elementos básicos: o método de cifragem; o de decifração e o da chave (MACHADO, 2010).

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que a verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública pode decifrá-la. Os métodos criptográficos impedem que a assinatura digital seja falsificada e garantem que os dados do certificado sejam verdadeiros.

3 DOCUMENTO DIGITAL E A ARQUIVOLOGIA

No ambiente digital, o documento não possui os padrões mais conhecidos como a linguagem alfabética, o suporte de papel e a leitura direta. Ocorre que, no ambiente digital, tudo é codificado em linguagem binária, que, para ser traduzida, necessita da intermediação de programas computacionais codificados em bits.

Nos últimos anos, várias pesquisas estão sendo feitas por profissionais da Arquivologia, na área da diplomática e da tecnologia da informação, para definir o conceito de documento na era digital. No Brasil, a questão do documento digital é alvo de estudos e discussões que são desenvolvidos com base na literatura arquivística e projetos como o InterPARES (2014) e InterPARESTrust. As discussões permeiam uma hierarquia conceitual, partindo das definições de documento, documento digital, documento arquivístico e documento arquivístico digital (CÂMARA..., 2010; CONSELHO..., 2011; RONDINELLI, 2011).

Ao abordar o assunto na diplomática, Rondinelli (2011, p. 236) afirma que os documentos arquivístico digitais se constituem de determinadas partes, como forma documental, anotações, contexto, suporte, atributos e componentes digitais. O autor descreve cada parte como:

a) Forma Documental que divide-se em: **Elementos intrínsecos**, são as cincos pessoas (autor, redator, destinatário, originador e produtor), data cronológica, data tópica, indicação e descrição da ação ou assunto e atestação. E os **elementos extrínsecos**, que são as características de apresentação geral, características de apresentação específica; assinatura digital, marcas d'água, logomarca;
b) Anotações: indicação de prioridades, data e hora de envio e do recebimento, indicação de anexo;
c) Contexto: jurídico administrativo, de proveniência, de procedimentos, documental e tecnológico;
d) Atributos: nome do autor, destinatário, formato;
e) Componentes Digitais: dados de forma, de conteúdo e de composição.

O documento digital tem suas especificidades e complexidades. Tem, pois, a necessidade de manutenção da autenticidade em toda a cadeia de custódia, acesso em longo prazo e consequente

preservação. O documento apresenta especificidades que podem comprometer sua autenticidade, devido à rápida obsolescência das tecnologias e de intervenções não autorizadas que podem ocasionar adulteração e destruição.

O uso de tecnologia digital para produzir documentos reconfigurou os elementos formais tradicionais por meio dos quais eles eram reconhecidos autênticos. Durante séculos, a autenticidade dos documentos baseou-se em elementos como selos, assinaturas, carimbos e em vários procedimentos para gerar e transmitir, usar e manter os documentos.

A perspectiva da Arquivologia e o uso da ferramenta do certificado digital na pesquisa se concentram no modo como esses documentos digitais estão garantindo autenticidade e segurança às informações prestadas.

O Sistema Informatizado de Gestão Arquivística de Documentos recomenda serviços de segurança apoiados em criptografia. Estes requisitos de segurança só são aplicáveis a organizações em que há elevada necessidade de garantia de sigilo. Os requisitos de assinatura digital e certificação digital são necessários para aquelas organizações em que documentos são assinados digitalmente ou para as verificações eletrônicas de autenticidade. Entretanto, adverte que os requisitos só são aplicáveis quando há necessidade de utilizar assinaturas digitais para assegurar autenticação, imputabilidade e irretratabilidade.

Assim, em relação à autenticidade, considera-se que o documento eletrônico arquivístico autêntico é aquele que é transmitido de maneira segura, cujo status de transmissão pode ser determinado, que é preservado de maneira segura e cuja proveniência pode ser verificada (MACNEIL apud RONDINELLI, 2005).

O uso de documentos digitais é um dos fenômenos da sociedade da informação e seus impactos no cotidiano já é sentido de maneira muito prática. O Governo e os órgãos públicos são os grandes geradores de demanda da certificação digital, e as empresas usufruem desta tecnologia para assinar, enviar documentos e para se identificar em diversos sistemas destas instituições.

4 PROCEDIMENTO E METODOLOGIA

Enquadra-se na tipologia de pesquisa exploratório-descritiva, realizado por meio de um estudo de caso e por possuir um objetivo definido. Buscou-se analisar se as autoridades certificadoras possuem estruturas para garantir a segurança e transação dos documentos digitais na cidade de Manaus. Do ponto de vista da forma de abordagem do problema, a pesquisa

tem característica qualitativa, uma vez que tal perspectiva é essencial na discussão sobre dados e informações, e parece-nos não ser prudente analisar a gestão documental sem considerar o contexto no qual é realizada.

Os procedimentos adotados para se alcançar os objetivos traçados foram os seguintes:

a) Levantamento de Dados: A pesquisa bibliográfica e documental teve como objetivo a identificação de documentos e artigos, julgados essenciais para fornecer subsídios à pesquisa; Para a pesquisa de campo, praticou-se o desprendimento dos métodos pré-estabelecidos, dos manuais, para conhecer e interpretar o outro em seu universo social, conforme Bourdieu (1999). Para tanto, aplicou-se roteiro de entrevista semiestruturado, com objetivo de coletar informações para construção de um diagnóstico das instituições que certificam e utilizam a certificação digital localizadas na cidade de Manaus. A amostragem de entrevistados ocorreu por meio de visitas às instituições-objeto deste estudo, selecionadas por julgamento e indicadas pelo responsável, conforme explicitados a seguir: para a amostra, escolheu-se membros com legitimidade e representatividade para opinar sobre o assunto da investigação. Hair Jr *et al* (2005) comentam que a amostragem, por julgamento, envolve a seleção de elementos para um fim específico, no qual o julgamento do pesquisador é utilizado para selecionar os elementos da amostra entre aqueles que ele considera como população-alvo.
b) Análise de dados: As entrevistas foram analisadas utilizando-se do método da análise de conteúdo (BARDIN, 1977), capaz de proporcionar uma interpretação aproximada da realidade, a partir da contextualização das respostas dos entrevistados. Para a consecução e a apreciação do estudo, em seus aspectos, utilizou-se a compreensão dos elementos por sua descrição e interpretação, e a partir da observação direta ao uso e aplicabilidade da certificação digital nos documentos digitais e segurança, autenticidade e sigilo das informações.

5 RESULTADOS E ANÁLISES

O uso de Certificado Digital tem aumentado nos últimos anos e acompanhado o desenvolvimento tecnológico e econômico das cidades brasileiras. A cidade de Manaus consta entre as principais capitais do país, possuindo o 6º maior Produto Interno Bruto (PIB), além de ser o 7º município mais populoso do Brasil, segundo estimativas do Censo 2010/IBGE.

O seu desenvolvimento nas últimas décadas foi impulsionado em grande parte pelo Polo Industrial de Manaus (PIM), que é um fator importante para a economia local e o crescimento do mercado do certificado digital na cidade devido aos fiscos. Em

razão da legislação atual e da necessidade de se ter um ambiente digital seguro e dinâmico, a certificação digital passou a ser integrada nos setores públicos e privados na cidade de Manaus.

O crescimento das instituições atuando no mercado e utilizando a certificação digital em Manaus cresceu nos últimos cinco anos, o que de certa forma contribui para a existência na cidade das principais Autoridades Certificadoras (Serasa Experian, Certisign, Fenacon e Valid), que são entidades que emitem certificados digitais para empresas e indivíduos.

A seguir será apresentado um panorama das autoridades certificadoras e usuárias localizadas na cidade e posteriormente a análise das informações advindas das entrevistas com os gestores:

a) **Serasa Experian – Serviços e Assessoria S/A:** tornou-se Autoridade Certificadora e Registradora em 2002, fornecendo todos os tipos de certificados digitais em operação no Brasil. A Serasa Experian provê todos os tipos de certificados digitais, bem como soluções customizadas para a utilização da tecnologia de certificação digital e de Notas Fiscais Eletrônicas. Esta fornece segurança dos certificados digitais para quase todos os grupos financeiros participantes do sistema de pagamentos brasileiro (SPB). A Autoridade Certificadora Serasa Experian – Manaus emite mensalmente a média de 600 certificados digitais, além de possuir representantes autorizados na cidade, como a Caixa Econômica, Correios, CDL e outros, que são responsáveis por maximizar as vendas no segmento;
b) **Câmara Dos Dirigentes Lojistas – CDL Manaus:** é uma entidade sem fins lucrativos, voltada para o desenvolvimento da atividade mercantil, mediante prestação de serviços nas áreas de Proteção ao Crédito (SPC), Telemarketing, Cobrança e Protesto de Títulos, Capacitação e Publicação de Informações Institucionais e Comerciais, Certificação Digital e CDL Celular. A CDL Manaus é uma Autoridade de Registro para emissão da certificação digital modelo ICP-Brasil. Os produtos oferecidos são principalmente para as empresas que são obrigadas a emitir nota fiscal eletrônica (NF-e). Pessoas físicas que precisam validar suas transações eletrônicas, como advogados, contadores ou empresários (e-CPF). Pessoas jurídicas que precisam validar transações eletrônicas (e-CNPJ). A entidade possui grande importância para a implantação da NF-e mediante realização das atividades em parceria com a SEFAZ/AM. A cidade de Manaus foi a primeira capital a emitir a NF-e. O fato ocorreu no dia 1 de março de 2013, sendo possível mediante Protocolo de Cooperação entre Secretaria de Fazenda do Estado do Amazonas (SEFAZ) e a Secretaria Municipal de Finanças, Tecnologia da Informação e Controle Interno (SEMEF). A Câmara de Dirigentes Lojistas disponibiliza programas gratuitos à disposição dos

lojistas: são pacotes de emissores com as funções básicas para a empresa emitir a NF-e em um caixa.

c) **Processo Judicial eletrônico da Justiça do Trabalho – PJe-JT no TRT 11:** o PJe é um processo sem papel no qual petições, despachos, sentenças, entre outros, são praticados, comunicados, armazenadas e disponibilizados no meio eletrônico. É um documento gerado e mantido em sua forma eletrônica, sem a necessidade de ser impresso ou assinado manualmente para ter valor.

Para utilizar o sistema, os advogados precisam da certificação digital. Além de identificar com precisão pessoas físicas e jurídicas, o certificado garante, ainda, confiabilidade, privacidade, integridade e inviolabilidade nas transações realizadas na internet. A exigência da certificação digital é uma tendência mundial em segurança da informação. O sistema do PJe-JT possui uma política de segurança que atende a esta premissa de forma a garantir a identificar com precisão pessoas físicas e jurídicas.

Todas as turmas do TRT-11 e todas as varas do trabalho de Manaus já operam com o PJe-JT. A ferramenta vem sendo implantada gradualmente na região de modo a proporcionar maior agilidade e modernidade na resolução dos processos. O TRT-11 possui aproximadamente 30 mil processos eletrônicos, e desde a implantação do PJe o trabalho foi otimizado, reduzindo custos e espaço físico para arquivamento.

Verificou-se que a difusão do certificado digital em Manaus acompanhou o surgimento e obrigatoriedade das leis nos setores público e privado. O setor financeiro foi o primeiro a utilizar o certificado digital, seguido pelo setor fiscal, que ganhou destaque com a nota fiscal eletrônica, e mais tarde pelo judiciário, com o processo eletrônico, que ao mesmo tempo foi responsável por aumentar o número de advogados utilizando a assinatura digital.

Com a utilização do certificado digital, percebeu-se que os processos internos das instituições tornaram-se mais ágeis, confiáveis e sigilosos, assim como tornaram a comunicação mais eficiente e segura. A contribuição do uso está atrelada principalmente à segurança. Os gestores entrevistados reconheceram que o uso do certificado digital torna as aplicações mais seguras, além de atribuir autenticidade e legalidade jurídica.

As certificadoras capacitam regularmente seus usuários sobre as medidas de segurança que devem ser adotadas ao utilizar o certificado digital e sobre o status da legislação vigente. O Instituto Tecnologia da Informação (2014) realiza anualmente auditoria que verifica se todas as normas e exigências impostas pela legislação estão sendo cumpridas pelas certificadoras.

Ainda segundo os entrevistados, a falta de segurança no uso do certificado digital acontece quando seu uso é feito por terceiros, ou seja, o dono do certificado autoriza que outra pessoa utilize sua identidade digital, configurando um crime de falsificação de identidade.

Com relação ao custo, a aplicação da certificação digital foi responsável por diminuir vários custos para as instituições. Os gestores afirmaram que o uso de certificado digital além de diminuir a burocracia, foi responsável por reduzir a utilização de papel, amortizando custos com tramitação de documentos. Outro ganho citado foi redução de custos com espaço físico para arquivamento.

Em relação à infraestrutura tecnológica, as instituições investiram em Tecnologia da Informação (TI) devido às novas exigências do mercado e à rápida obsolescência de *hardware* e *software*. Ressalta-se que os gastos com os novos equipamentos de TI já eram esperados por parte das instituições, uma vez que eram necessários para o funcionamento das mesmas. Identificou-se também que as certificadoras possuem profissionais capacitados para a instalação do certificado digital, além de disponibilizarem canal de suporte técnico para solução de possíveis dúvidas/problemas.

A certificação digital foi incorporada rapidamente às atividades do trabalho e foi classificada como de fácil compreensão e uso.

6 CONCLUSÃO

Diante da popularização da internet, das TIC's e do novo formato de transações no ambiente digital, surgiu a necessidade de tecnologias para garantir autenticidade e segurança nas informações e documentos que circulam no ambiente digital. Atualmente, existe a necessidade de equiparar os documentos digitais com os documentos convencionais (papel), usufruindo dos mesmos benefícios, mas com as diferenças que existem em cada suporte.

Nesse sentido, a pergunta que norteou este trabalho é respondida com a utilização do Certificado Digital ICP-Brasil. Uma vez que a aplicação da certificação digital sobre informações registradas em suportes digitais garante a autenticidade, confidencialidade e integridade. No entanto, para que isto aconteça, faz-se necessário o uso das normas e padrões estabelecidos pela ICP-Brasil.

O uso do certificado digital para a Arquivologia agrega valor tanto para a gestão documental como para a preservação dos documentos permanentes. E, nesse contexto, ressalta-se o

importante papel que o certificado digital tem para os documentos digitais e para a Arquivologia. No entanto, são escassos os estudos da área voltados para o documento digital. Nesse sentido, recomenda-se para futuros trabalhos de pesquisa os desafios que o uso de assinatura digital de longa duração apresenta.

DIGITAL CERTIFICATION AND ARCHIVOLOGY: benefits and applications

ABSTRACT: Information Society has opened up new fields and opportunities, and the information in digital networks has gained dimensions without borders, emerging the need for security politics in order to guarantee data authentication, privacy, authorization and integrity. The solution found to solving those problems was the use of a cryptography system. Brazilian government has created technical standards to support a cryptographic system called Brazilian Infrastructure of Public Keys (ICP-Brasil), with the main goal to regulate the use of digital certificates. As the emerging of this new document format intensively grows, Archivology has felt the need to incorporate this tool. If for one side digital signatures give information authenticity and integrity, on the other side the advances do not guarantee its long-term preservation. The legal value of this document's authenticity relates to the digital signatures. Under the optics of archivistics and diplomatics, the authenticity of the documents does not depend only on the signature, but on a set of elements. This paper intends to analyze the digital certification market in the city of Manaus, under the optics of Archivology, that is, the authenticity and secrecy in digital documents. Methodologically, it refers to a qualitative-nature research, with descriptive-exploratory characteristics, made on a case study and because it has a defined objective. It sought evaluating if the certificating authorities own mainframes to assure the safety and the transaction of the digital documents in the city of Manaus-AM. As a result, it observed that the financial sector was the first one to utilize digital certificate, followed by the fiscal sector, which came to prominence with the electronic fiscal note, and later by the judiciary sector with the electronic process, which at the same time was responsible for enhancing the number of attorneys using digital signature. It has verified that the application of digital certification on information registered in digital supports guarantees authenticity, confidentiality and integrity. However, in order for this to happen, it is necessary to observe the norms and standards established by the ICP-Brasil. The use of

digital certificate to the Archivology aggregates value as much for documental management as for the preservation of permanent documents.

KEYWORDS: Archivology. Digital certification. Digital document. Digital signature.

REFERÊNCIAS

BARDIN, Laurence. **Análise de conteúdo**. Lisboa: Edições 70, 1977.

BOURDIEU, Pierre. Compreender. In: _____. (Orgs). **A miséria do mundo**. 3. ed. Petrópolis: Vozes, 1999.

BRITO, Pedro Quelhas et al. **O futuro da internet:** estado da arte e tendência de evolução. Portugal: Centro Atlântico, 1999.

CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS (CTDE). **Glossário:** versão 5.1, 2010. Disponível em: ‹http://www.documentoseletronicos.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm›. Acesso em: 13 nov. de 2014.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). Câmara Técnica de Documentos Eletrônicos (CTDE). E-Arq Brasil: **Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos.** Rido de Janeiro: Arquivo Nacional, 2011. Disponível em: <http://www.documentoseletronicos.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm>. Acesso em: 18 nov. 2014.

HAIR JR., Joseph F. et al. **Fundamentos de métodos e pesquisa em administração**. Porto Alegre: Bookman, 2005.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). Disponível em: <http://www.iti.gov.br>. Acesso em: 13 nov. 2014.

MACHADO, Robson. **Certificação digital ICP-Brasil**: os caminhos do documento eletrônico no Brasil módulo usuário. Rio de Janeiro: Impetus, 2010.

MONTEIRO, Emiliano S.; MIGNONI, Maria Eloisa. **Certificados digitais**: conceitos e práticas. Rio de Janeiro: Brasport, 2007.

PEREIRA, Samáris Ramiro. Certificação digital através do algoritmo RSA. **Periódico Eletrônico da FATEC/São**

Caetano do Sul, São Caetano do Sul, v. 1, n. 1, p. 74 a 86. ago./dez. 2009.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos:** uma abordagem teórica da diplomática arquivística contemporânea. 4. ed. Rio de Janeiro: FGV, 2005.

_____. **O conceito de documento arquivístico frente à realidade digital:** uma revisitação necessária. 2011. 270 f. Tese (Doutorado)- Curso de Ciência da Informação, Universidade Federal Fluminense, Rio de Janeiro, 2011.

STALLINGS, Willian. **Criptografia e segurança de redes**: princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

TURBAN, Efraim**. Administração de tecnologia da informação:** teoria & prática**.** Rio de Janeiro: Elsevier, 2005.