GESTÃO DE DOCUMENTOS DIGITAIS EM APLICAÇÕES DE CERTIFICAÇÃO DIGITAL

Sânderson Lopes Dorneles*

Renato Fernandes Corrêa**

RESUMO

Analisa aplicações de certificação digital a fim de compreender essa tecnologia da informação e seu uso na gestão de documentos digitais. A utilização da certificação digital atribui credibilidade e valor legal ao registro de informações em suportes digitais, contribuindo para o crescente número dessas informações em ambiente digital. Com base em pesquisa bibliográfica este trabalho aborda os conceitos, tecnologias, as políticas públicas a respeito da certificação digital e a Infraestrutura Brasileira de Chaves Pública (ICP-Brasil). Pautado em estudos de caso com coleta de dados por meio de entrevistas e pesquisa bibliográfica, as aplicações de certificação digital Nota Fiscal Eletrônica (NF-e) e Programa Minha Certidão são analisadas quanto conformidade com a ICP-Brasil, programas e formatos de computadores utilizados no processo de certificação digital, procedimentos adotados para emissão de certificados e verificação da assinatura digital, armazenamento do documento certificado digitalmente, legislação concernente, segurança da informação, preservação digital e resultados dos projetos. Como resultado da pesquisa, verificou-se a existência de leis federais e estaduais que asseguram a utilização da certificação digital com valor legal, diferenças na aplicação da certificação digital pelos projetos, conformidades no que tangem a utilização de certificados digitais pertencentes à Infraestrutura Brasileira de Chaves Públicas, bem como diferenças nas políticas de segurança e de preservação da informação concebidas sob os preceitos das Instituições mantenedoras de cada projeto em análise. E como conclusão, sugere-se que os projetos que gerem documentos certificados digitalmente desenvolvam e apliquem normas e políticas mais criteriosas de gestão dos documentos.

Palavras-chave: Certificação digital. Documento digital. Gestão de documentos. Preservação digital.

* Arquivista do IFPB, Graduado em Arquivologia pela UFSM, Mestre em Ciência da Informação pela UFPE. *E-mail*: sanderson.dorneles@gmail.com

** Doutor em Ciência da Computação pela UFPE. Professor do Programa de Pós-Graduação em Ciência da Informação da UFPE. *E-mail:* fc_renato@yahoo.com.br

1 INTRODUÇÃO

As tecnologias da informação e as novas formas de produzir, disseminar e recuperar o conhecimento revolucionou os processos de criação de documentos. A Internet por sua vez encurtou as noções de tempo e espaço agilizando a forma de transmitir 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.

A aplicação da certificação digital sobre informações registradas em suportes digitais visam garantir a autenticidade, confidencialidade e integridade das mesmas diante de sua reconhecida instabilidade. Para tanto, é necessário o estabelecimento de políticas públicas, diretrizes, programas e projetos específicos, legislação, metodologias, normas, padrões e protocolos que minimizem os efeitos da fragilidade e da obsolescência de *hardware*, *software* e formatos e que assegurem, ao longo do tempo, a autenticidade, a confidencialidade, a integridade, o acesso contínuo e o uso pleno da informação certificada digitalmente a todos os segmentos da sociedade.

No Brasil, a certificação digital ganhou força através da criação de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais dotados de valor legal. Sob essa percepção o Governo Federal regulamentou via Medida Provisória nº 2.200-2 de 2001 as atividades de certificação digital no País, para garantir maior segurança nas transações eletrônicas e incentivar a utilização da Internet como meio para a realização de negócios.

Com a adoção da certificação digital na esfera governamental e comercial, o uso da certificação possibilitará a diminuição dos documentos tradicionais, uma vez que a maioria deles nasce em ambiente digital e, por falta da certificação, acaba ganhando o papel como suporte. Nesse sentido, serão necessárias aplicações de estratégias de preservação digital a fim de manutenção desses documentos por longos períodos nos arquivos das organizações, em virtude dos seus prazos de guarda.

Neste contexto, o presente trabalho analisa aplicações de certificação digital a fim de compreender essa tecnologia da informação no que tange

ao seu uso na gestão de documentos digitais, com foco nas estratégias de preservação digital e na preservação da memória registrada nesses documentos. Para tanto, traçou-se como objetivos específicos: descrever o processo de certificação digital; descrever políticas públicas de certificação digital; descrever o funcionamento dos projetos de aplicação da certificação digital; verificar a conformidade dos projetos com a legislação federal; descrever e avaliar as políticas de segurança da informação e de preservação digital adotadas pelos projetos.

A perspectiva em Arquivologia deste trabalho se concentra no modo como os projetos analisados lidam com a produção, tramitação e preservação dos documentos assinados digitalmente, que constituem objetos de estudo da Arquivologia.

O trabalho se encontra estruturado da seguinte forma: a base teórica do trabalho é apresentada nas seções 2 e 3 que versam respectivamente sobre Certificação Digital e Políticas Públicas de Certificação Digital no Brasil; a seção 4 apresenta os procedimentos metodológicos utilizados para a elaboração do trabalho; a seção 5 descreve as aplicações de certificação digital escolhidas como estudo de caso; a seção 6 traz os resultados dos estudos de caso; e a conclusão do trabalho é descrita na seção 7.

2 CERTIFICAÇÃO DIGITAL

Os computadores e a Internet são largamente utilizados para o processamento de informações e para a troca de mensagens e documentos entre indivíduos, governos e instituições privadas. Para tanto, estas transações digitais necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade, integridade e não-repúdio às informações eletrônicas.

Segundo MacNeil,

> [...] autenticidade é "a capacidade de se provar que um documento arquivístico é o que diz ser". A autenticidade de um documento está diretamente ligada ao modo, à forma e ao *status* de transmissão desse documento, bem como às condições de sua preservação e custódia. Isso quer dizer que o conceito de autenticidade refere-se à adoção de métodos que garantam que o documento não foi adulterado após a sua criação e que, portanto, continua sendo tão fidedigno quanto era no momento em que foi criado. Assim, em relação à autenticidade, considera-se que um documento eletrônico arquivístico autêntico é aquele que é transmitido de maneira segura, cujo *status* de transmissão pode ser determinado, que é preservado de maneira segura e cuja proveniência pode ser verificada. (MACNEIL

> 2000, apud RONDINELLI, 2002, p. 66).

No que se referem aos demais mecanismos de segurança Silva *et al* (2008) trazem os seguintes conceitos:

- Confidencialidade – é a garantia de que a informação é acessível somente por pessoas autorizadas;
- Integridade – consiste em proteger a exatidão e completeza da informação e dos métodos de processamento;
- Não – repúdio – o serviço de não-repúdio impede que uma parte envolvida na comunicação venha a negar falsamente a sua participação em qualquer momento da comunicação. Uma das partes pode tentar repudiar seu envolvimento para enganar a outra, alegando, por exemplo, que não teve participação em uma transação bancária. O serviço de não-repúdio deve garantir evidências, durante uma comunicação, que poderão ser usadas em momentos de desacordos entre as partes envolvidas.

Para o Instituto Nacional de Tecnologia da Informação - ITI (2005) a certificação digital é a tecnologia que provê estes mecanismos. No cerne da certificação digital está o certificado digital, um documento eletrônico emitido por uma terceira parte confiável (Autoridade Certificadora), que associa o nome (e atributos) de uma pessoa ou instituição a uma chave criptográfica pública. A chave pública é uma cadeia aleatória de *bits* utilizada em conjunto com um algoritmo que serve para validar uma assinatura realizada em documentos eletrônicos. Segundo Maia e Pagliusi (2011) o número de chaves possíveis depende do tamanho (número de *bits*) da chave. Por exemplo, uma chave de oito *bits* permite uma combinação de no máximo 256 chaves (2^8). Quanto maior o tamanho da chave, mais difícil quebrá-la, pois estamos aumentando o número de combinações.

Segundo Silva *et al* (2008, p. 26) um certificado digital (também chamado de certificado de chave pública) é uma ligação entre a chave pública de uma entidade e um ou mais atributos relacionados a esta entidade, armazenados em um arquivo digital. O usuário neste caso pode ser uma pessoa, dispositivo de *hardware* ou um processo de *software*. O certificado digital produz a garantia que a chave pública pertence à entidade. Além disso, garante também que a entidade (e somente esta entidade) possui de fato a correspondente chave privada.

O certificado apresenta-se sob o formato X.509 que é um padrão de formato de certificado criado pela *International Telecommunication Union – Telecommunication Standartization Sector* (ITU-T) e *ISO/International Electrotechnical Commission* (IEC). Segundo Adams e Just (2004) o padrão teve seu início em 1988 e só começou a ser divulgado, reconhecido, e implementado em pequena escala no final de 1993 e início de 1994, quando se deu efetivamente o início da Infraestrutura de Chave Pública (ICP), do inglês *Public Key Infrastructure* (PKI), apesar de o termo ter surgido posteriormente. Atualmente o padrão se encontra na terceira versão (v3), lançada em 1996, com a possibilidade de usar campos de extensão.

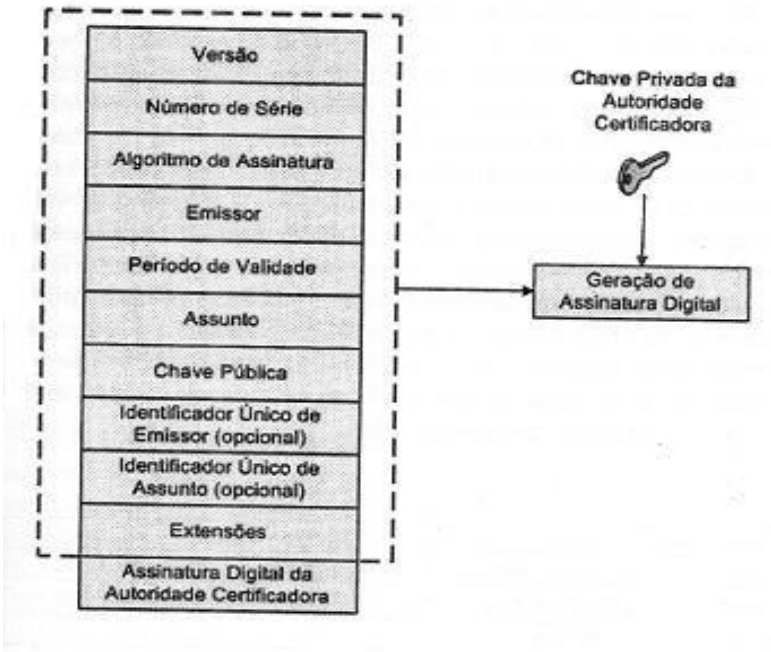
A Figura 1 ilustra o formato de certificado X.509 v3 e o Quadro 1 que descreve os campos do certificado.

Para melhor compreender a certificação digital é necessário discutir conceitos relevantes que fazem parte desta temática, tais como, criptografia[1] na forma simétrica e assimétrica, assinatura digital, função *hashing*, e certificado digital. Pois todos esses conceitos estão interligados e se complementam a fim de atribuir as características indispensáveis à segurança da informação.

Segundo conceituações publicadas em cartilha do ITI (2005) a criptografia simétrica realiza a cifragem e a decifragem de uma informação através de algoritmos que utilizam a mesma chave, garantindo sigilo na transmissão e armazenamento de dados. Como a mesma chave deve ser utilizada na cifragem (Fig. 2) e na decifragem (Fig. 3), a chave deve ser compartilhada entre quem cifra e quem decifra os dados. O processo de compartilhar uma chave é conhecido como troca de chaves. A troca de chaves deve ser feita de forma segura, uma vez que todos que conhecem a chave podem decifrar a informação cifrada ou mesmo reproduzir uma informação codificada.

[1] Criptografia: é um processo matemático usado para embaralhar os dados de uma mensagem que deve ser sigilosa. (CARVALHO, 2006, p. 477)

Figura 1: Certificado Digital no Padrão X.509 v3



Fonte: SILVA *et al* (2008).

Quadro 1: Descrição dos campos de um certificado no formato X.509 v3

NOME DO CAMPO	DESCRIÇÃO
Versão	Número de versão X.509 do certificado, tendo como valor válido apenas 1,2 ou 3.
Número de Série	Identificador único do certificado e representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma autoridade certificadora.
Algoritmo de Assinatura	Identificador do algoritmo usado para assinatura do certificado pela autoridade certificadora
Emissor	Nome da autoridade certificadora que produziu e assinou o certificado
Período de Validade	Intervalo de tempo de duração que determina quando um certificado deve ser considerado válido pelas aplicações.
Assunto	Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade.
Chave Pública	Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada.
Identificador Único de Emissor (opcional)	Campo opcional para permitir o reusa de um emissor com o tempo.
Identificador Único de Assunto (opcional)	Campo opcional para permitir o reusa de um assunto com o tempo.
Extensões (opcional)	Campos complementares com informações adicionais personalizadas.

Fonte: SILVA *et al* (2008)

Figura 2: Criptografia simétrica: cifragem

Fonte: CARVALHO (2008), adaptado

Figura 3: Criptografia simétrica: decifragem

Fonte: CARVALHO (2008), adaptado

Dessa forma, o uso de uma única chave requer cuidados dobrados para não cair em mãos erradas, o que torna o processo de trocas de chaves muito frágil. Assim sendo, mesmo que vulnerável, a criptografia simétrica garante **confidencialidade** a um documento digital.

A criptografia assimétrica consiste da cifragem e a decifragem de uma informação através de algoritmos que utilizam respectivamente uma chave pública e uma chave privada, garantindo sigilo na transmissão e armazenamento de dados. Para auferir maior segurança na utilização de chaves, a criptografia assimétrica é realizada com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simul-taneamente e está relacionado entre si, o que possibilita que a operação executada por uma seja revertida pela outra. A chave privada deve ser mantida em sigilo e protegida por quem gerou as chaves. A chave pública é disponibilizada e tornada acessível a qualquer indivíduo que deseje se comunicar com o proprietário da chave privada correspondente (ITI, 2005).

As figuras 4 e 5 ilustram respectivamente o esquema da cifragem e decifragem com chaves assimétricas.

Figura 4: Criptografia assimétrica: No remetente, cifragem com a chave pública do destinatário.

Fonte: CARVALHO (2008), adaptado

Figura 5: Criptografia assimétrica: No destinatário, decifragem com a chave privada.

Fonte: CARVALHO (2008), adaptado

Segundo Maia e Pagliusi (2011), a grande vantagem deste sistema é permitir que qualquer um possa enviar uma mensagem secreta, apenas utilizando a chave pú-

blica de quem irá recebê-la. Como a chave pública está amplamente disponível, não há necessidade do envio de chaves como é feito no modelo simétrico. A **confidencialidade** da mensagem é garantida, enquanto a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens.

No contexto da criptografia assimétrica e do uso da chave pública e privada, surge a assinatura digital. Conforme Carvalho (2006, p. 498) a assinatura digital se baseia em criptografia simétrica e assimétrica, e difere das mesmas na forma como as chaves serão utilizadas. No processo criptográfico, o remetente usa a chave pública do destinatário para cifrar a mensagem, esperando que o destinatário utilize a sua chave privada para decifrar a mensagem, enquanto no processo de assinatura digital, com o qual se deseja a **autenticidade**, o remetente utilizará a sua chave privada para "assinar" a mensagem. Por outro lado, o destinatário usará a chave pública do remetente para confirmar que ela foi enviada por aquela pessoa.

Neste sentido, a assinatura digital é dotada de **autenticidade**, por garantir a identificação de quem enviou a mensagem, bem como caracteriza o **não-repúdio**, uma vez que o remetente da mensagem não poderá dizer que não foi ele quem escreveu aquela mensagem. E para garantir a **confidencialidade** com assinatura digital, basta combinar a criptografia assimétrica com assinatura digital. Sendo assim, o remetente primeiro assina a mensagem, utilizando sua chave privada. Em seguida, ele criptografa a mensagem novamente, junto com sua assinatura, utilizando a chave pública do destinatário. Este, ao receber a mensagem, deve, primeiramente, decifrá-la com sua chave privada, o que garante sua **confidencialidade**. Em seguida, "decifrá-la" novamente, ou seja, verificar a assinatura digital utilizando a chave pública do remetente, garantindo assim sua **autenticidade**.

A **integridade** é conquistada por meio da assinatura digital e pela função *hashing* (conhecida também por função resumo), pois sua utilização é componente das assinaturas digitais, desempenhando a função de catalisador dos algoritmos assimétricos, em virtude dos mesmos serem mais lentos que os simétricos, no que tangem ao processo de cifragem de grandes mensagens. Para tanto, a função *hashing*, que gera um valor pequeno, de tamanho fixo, derivado da mensagem que se pretende assinar, de qualquer tamanho. Oferecendo, agilidade nas assinaturas digitais, além de integridade confiável.

Segundo Maia e Pagliusi (2011), esse valor serve para garantir a **integridade** do conteúdo da mensagem que representa. Assim, após o valor *hash* de uma mensagem ter sido calculado através do

emprego de uma função *hashing*, qualquer modificação em seu conteúdo, mesmo em apenas um *bit* da mensagem será detectada, pois um novo cálculo do valor *hash* sobre o conteúdo modificado resultará em um valor *hash* bastante distinto.

De posse das tecnologias que auferem a autenticidade, confidencialidade, integridade e não-repúdio das informações eletrônicas, cujos mecanismos e características da segurança da informação estão sintetizados no Quadro 2, resta aquela que atesta o valor legal, atribuindo **confiabilidade**. Assim surgem os certificados digitais, os documentos eletrônicos que guardam informações sobre pessoas e instituições e é atestado por uma Autoridade Certificadora, que funcionam como verdadeiros cartórios digitais.

Quadro 2: Característica de Segurança *versus* Mecanismo de Segurança

CARACTERÍSTICA DE SEGURANÇA	MECANISMO DE SEGURANÇA
Autenticidade e Não-repúdio	Assinatura digital
Confidencialidade	Criptografia assimétrica
Integridade	Função *hashing* da assinatura digital
Confiabilidade	Certificado digital

Fonte: Elaboração própria

Para implementar as funcionalidades da certificação digital, é necessário planejar cuidadosamente uma infraestrutura para gerenciar os certificados digitais. Uma Infraestrutura de Chave Pública (ICP), do inglês *Public Key Infrastructure* (PKI), consiste em um componente essencial de uma estratégia global de segurança que deve trabalhar em conjunto com outros mecanismos de segurança, práticas de negócios, e os esforços de gestão de riscos (WEISE, 2001).

Sobre a Infraestrutura de Chave Pública (ICP) Kuhn *et al* (2001) fazem as seguintes considerações:

> Infraestrutura de Chave Pública é a combinação de *software*, tecnologias de criptografia e serviços que permite às empresas protegerem a segurança das suas comunicações, negócios e transações em redes. A ICP integra certificados digitais, criptografia de chave pública, e autoridades de certificação em uma completa arquitetura de segurança em rede. (KUHN *et al*, 2001, p. 15-16)

Para o funcionamento desses cartórios digitais são necessários os seguintes elementos funcionais: uma Autoridade Certificadora (AC) e uma Autoridade de Registro (AR), que fazem parte de uma ICP. Segundo Weise (2001), a geração, distribuição e gestão de chaves públicas e certificados associados normalmente ocorrem através de Autoridades Certificadoras, Autoridades de Registro e serviços de diretório. Um dos grandes benefícios de uma ICP é o estabelecimento de uma hierarquia de confiança, onde o certificado digital é assinado pela AC, garantindo a identidade dos indivíduos, e os indivíduos podem utilizar seus certificados para estabelecer confiança entre si.

Resumidamente, o usuário faz seu credenciamento junto a uma Autoridade Certificadora (AC) a fim de registrar o seu certificado digital e pode gerar o par de chaves (pública e privada). Segundo Silva *et al* (2008, p. 30) os passos de geração da chave pública e privada, a transferência da chave pública para uma AC e a transferência da chave privada para o dono são essenciais durante o registro de certificados. O dono pode gerar o par de chaves em algum tipo de sistema local, armazenar a chave privada e mandar a chave pública para a AC. O armazenamento da chave privada geralmente envolve criptografia, fazendo com que uma senha seja requisitada toda vez que precisar ser usada.

Para proteção das chaves, são utilizados dispositivos como, os cartões inteligentes (*smartcards*). Eles se assemelham – em formato e tamanho – a um cartão de crédito convencional. Os *smartcards* são um tipo de *hardware* criptográfico dotado de um microprocessador com memória capaz de armazenar e processar diversos tipos de informações. Com eles é possível gerar as chaves e mantê-las dentro de um ambiente seguro, uma vez que as operações criptográficas podem ser realizadas dentro do próprio dispositivo.

Por outro lado, alguns usuários preferem manter suas chaves privadas no próprio computador. Neste caso, deverão ser tomadas medidas de segurança: como proteção por senha do *software* que gera o par de chaves, não compartilhar com ninguém a senha de acesso à chave privada e não instalar o certificado com a chave privada em computador de uso público, tudo isso para não comprometer a segurança da chave privada.

O certificado digital, diferentemente dos documentos utilizados usualmente para identificação pessoal como CPF e RG, possui um período de validade que pode variar de um até quatro anos, assim como apresenta custos. Os valores estão atrelados ao período de validade, quanto maior o prazo de validade maior será o valor, e aos tipos de aplicações, tais como, certificado para uso pessoal, pessoa jurídica, *sites* e ou servidores. A tabela de preços é estipulada por cada AC que faz parte de uma ICP, oportunizando a livre concorrência. Cabe ressaltar, também, que só é possível assinar um documento, enquanto o certificado é válido. Entretanto, é possível conferir as assinaturas realizadas mesmo após o certificado expirar.

Sobre este aspecto da validade do certificado, Silva *et al* (2008, p.29) comentam que em algumas situações, é preciso que um certificado seja revogado antes do seu período de validade terminar. Estas situações podem ocorrer, por exemplo, com o vazamento da chave privada ou mudança de dados do dono do certificado. Nestes casos, as entidades que

emitiram o certificado devem possuir mecanismos que permitam mudar o estado de revogação de certificados.

Para tanto, surgem as Listas de Certificados Revogados (LCR) que são mecanismos que uma autoridade certificadora usa para publicar e disseminar informação sobre certificados revogados. Conforme Silva *et al* (2008, p.29) uma LCR é uma estrutura de dados, digitalmente assinada pela autoridade certificadora, que contém: dia e hora da publicação da LCR, nome da autoridade certificadora e os números de série de todos os certificados revogados que ainda não foram expirados. Ao trabalhar com certificados, uma aplicação deve obter a lista de certificados revogados mais recentes e verificar se o número de série do certificado, que está se tentando usar na aplicação, não está na lista de certificados revogados.

Já a renovação do certificado pode ser necessária para a substituição da chave privada por outra tecnologicamente mais avançada ou devido a possíveis mudanças ocorridas nos dados do usuário. Essas alterações têm como objetivo tornar mais robusta a segurança.

Diante do exposto sobre os conceitos relacionados à certificação digital, é oportuno esclarecer o contexto da Arquivologia na aplicação dessa tecnologia.

Segundo Bodê (2006) o uso de assinaturas digitais baseadas em chaves públicas e ICPs confiáveis com respaldo legal podem agregar ainda mais valor e aplicabilidade aos documentos digitais, cujas consequências para a Arquivologia são importantes, tanto no que cabe à Gestão Documental dos documentos não permanentes, como a administração dos acervos Permanentes. Além da preservação de documentos digitais, a presença nas organizações de documentos digitais autênticos e com valor legal, aumenta ainda mais a carga de responsabilidade para sua correta administração.

Além disso, o número de documentos digitais com valor arquivístico tende a crescer devido aos fatores técnicos e tecnológicos que possibilitam nivelar os documentos digitais ao mesmo *status* de documentos em suportes tradicionais, como o papel, no que tange a seu valor legal, bem como devido ao fato destes documentos receberem uma aceitação social e legal (BODÊ, 2006, p. 66). No contexto brasileiro essa aceitação já pode ser percebida em virtude do respaldo legal implementado pela Medida Provisória nº 2.200-2, de 2001, melhor explorada na seção Políticas Públicas de Certificação Digital, e a aceitação social pode ser vista por intermédio dos projetos Nota Fiscal Eletrônica e Programa Minha Certidão, analisados neste trabalho, que se utilizam da certificação digital.

Dessa forma, a compreensão da forma como os certificados digitais são aplicados propicia os subsídios necessários para um bom gerenciamento dos documentos assinados digitalmente.

3 POLÍTICAS PÚBLICAS DE CERTIFICAÇÃO DIGITAL

No Brasil, a Medida Provisória (MP) Nº 2.200-2 com força de lei, de 24 de agosto de 2001 instituíram a Infraestrutura de Chaves Pública Brasileira (ICP-Brasil) para garantir a autenticidade, a confidencialidade, a integridade e a validade jurídica de documentos em forma digital, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. Nela ficou estabelecido que a ICP-Brasil será composto: por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras, formada pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

De acordo com o texto da Medida Provisória 2.200-2, a função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por doze membros, sendo cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares: Ministério da Justiça; Ministério da Fazenda; Ministério do Desenvolvimento, Indústria e Comércio Exterior; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência e Tecnologia; Gabinete de Segurança Institucional da Presidência da República; e Casa Civil da Presidência da República que o coordenará. (BRASIL, MP Nº 2.200-2, 2001).

O Comitê Gestor da ICP-Brasil (CG ICP-Brasil), instituído pela referida Medida Provisória, foi regulamentado pelo Decreto nº. 6.605, de 14 de Outubro de 2008, e terá por finalidade atuar na formulação e controle da execução das políticas públicas relacionadas à ICP-Brasil, inclusive nos aspectos de normatização e nos procedimentos administrativos, técnicos, jurídicos e de segurança, que formam a cadeia de confiança da ICP-Brasil (BRASIL, DECRETO Nº 6.605, 2008).

Dos atos normativos da MP 2.220-2, ressaltam-se as seguintes competências:

> - A execução das Políticas de Certificados e de Normas Técnicas e Operacionais aprovadas pelo Comitê Gestor da ICP-Brasil é realizada pela Autoridade Certificadora Raiz da ICP-Brasil, que é a primeira autoridade da cadeia de certificação.
> - O Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada ao Ministério da Ciência e Tecnologia, é a AC-Raiz da ICP-Brasil
> - Compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certi-

> ficados das autoridades certificadoras de nível imediatamente subsequente ao seu. A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras (ACs) estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor.
> - Já as Autoridades Certificadoras (AC), que são 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 manter registro de suas operações.
> - Com relação às Autoridades de Registro (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. Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicas e as pessoas jurídicas de direito privado. (BRASIL, MP 2.200-2, 2001)

Sob essa estrutura é regida a política de geração e controle de certificados digitais brasileiros. Quanto aos benefícios da aplicação da certificação digital na implantação de políticas públicas no contexto do governo eletrônico, Alonso, Ferneda e Braga (2011) esclarecem que:

> O uso dessa tecnologia, nos casos de aplicação aos processos relativos à implantação de políticas públicas, é apontado como capaz de prover segurança às bases de dados de programas governamentais; facilitar a arrecadação de impostos; proporcionar segurança na tramitação de processos; assegurar um melhor controle dos programas de governo e garantir a segurança das transações eletrônicas. Além disso, são conferidas qualidades à certificação digital, como proporcionar celeridade à tramitação de processos e aumentar a transparência das ações governamentais. (ALONSO et al, 2011, p. 21)

Nesse sentido, buscou-se nessa seção ilustrar como se estrutura a ICP-Brasil, apresentando a legislação pertinente, os conceitos e as regras normativas. Com isso, demonstra-se a instrumentação jurídica necessária para o uso da certificação digital no país.

4 METODOLOGIA

O presente trabalho vale-se da pesquisa exploratória conforme define Gil (2009, p. 41), fazendo uso da pesquisa bibliográfica sobre os principais conceitos da certificação digital e estudo de caso de dois projetos de aplicação da certificação digital.

A pesquisa bibliográfica foi conduzida para identificar e abordar os conceitos, tecnologias, políticas públicas e projetos que aplicam a certificação digital. Segundo Gil (2009, p. 45) a principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Sendo assim, livros e artigos científicos serviram de fontes bibliográficas para exploração do tema da certificação digital.

Os estudos de caso consistem dos projetos Nota Fiscal Eletrônica (NF-e) da Secretaria da Fazenda do Estado de Per-

nambuco (SEFAZ-PE) desenvolvido em parceria com a Receita Federal do Brasil, e o Programa Minha Certidão cujo suporte tecnológico foi desenvolvido pela Agência Estadual de Tecnologia da Informação (ATI) do Estado de Pernambuco. Estes projetos foram escolhidos por serem projetos pioneiros de aplicação da certificação digital no Brasil, por promoverem a aceitação social da tecnologia ao gerarem documentos certificados digitalmente que chegam ao cidadão comum, bem como o acesso facilitado aos gestores destes projetos.

Os estudos de caso foram delimitados pela coleta de dados sobre cada projeto através de pesquisa bibliográfica, entrevistas semi-estruturadas e posterior análise. Nessa perspectiva buscou-se estudar como essas aplicações de certificação digital produzem documentos certificados digitalmente e promovem a gestão e preservação destes documentos.

As primeiras informações sobre os projetos que aplicam a certificação digital foram encontradas na Internet, em *site*s de notícias, revistas digitais e nos próprios *sites* das Instituições idealizadoras dos projetos. Foi também possível obter informações nas apresentações dos projetos no 8º e 9° CERTFÓRUM etapa Recife, fórum de certificação digital realizado pelo Instituto Nacional de Tecnologia da Informação (ITI) nos anos de 2010 e 2011 respectivamente.

As entrevistas semi-estruturadas foram realizadas no ano de 2011 junto aos responsáveis pelas referidas aplicações de certificação digital com questionamentos sobre: conformidade dos certificados com a ICP-Brasil - relaciona-se ao respaldo legal; programas e formatos de computadores utilizados no processo de certificação digital - relaciona-se às estratégias de preservação da tecnologia para emitir/assinar/visualizar documentos; armazenamento do documento certificado digitalmente – relaciona-se com preservação do documento digital; legislação concernente - relaciona-se aos dispositivos legais que respaldam a utilização do documento assinado digitalmente; segurança da informação - relaciona-se aos mecanismos de proteção contra sinistros físicos, lógicos e humanos; preservação digital - relacionam-se as estratégias adotadas para a preservação do formato, *software* e *hardware*; e resultados dos projetos - relaciona-se ao benefício social que a utilização da tecnologia proporcionará aos indivíduos. Em um segundo momento foi necessária a aplicação de outro roteiro com questionamentos a respeito da preservação digital com perguntas que versaram sobre tabela de temporalidade de documentos, destinação do documento digital e estratégias utilizadas para a preservação do documento digital.

Sendo assim, os roteiros das entrevistas foram enviados via *e-mail* para cada

entrevistado, o que proporcionou maior tranquilidade aos entrevistados para formular as respostas. Logo após a coleta dos dados foi feita a análise, e tecidas as devidas considerações.

5 APLICAÇÕES DE CERTIFICAÇÃO DIGITAL

No Brasil, o número de certificados digitais emitidos no país aumentou 50% em apenas sete meses, em agosto de 2009 foram emitidos 45.085 certificados e já em março de 2010 o número atingiu 105.659. Os dados são do Instituto Nacional de Tecnologia da Informação (ITI), responsável pela manutenção da Infraestrutura de Chaves Pública Brasileira (ICP-Brasil). O crescimento desse mercado deve-se, principalmente, à Instrução Normativa 969 da Receita Federal, de outubro de 2009, que obriga as empresas de todo o País a prestarem contas ao Fisco usando assinatura digital, como também, aos avanços e a obrigatoriedade do documento eletrônico no Poder Judiciário Brasileiro. (ITI, 2010)

Neste contexto nacional e das diversas aplicações da certificação digital, cabe explanar sobre o projeto Nota Fiscal Eletrônica e o programa Minha Certidão, nas subseções a seguir.

5.1 Projeto Nota Fiscal Eletrônica (NF-e)

A Nota Fiscal Eletrônica (NF-e) é desenvolvida de forma integrada pelas Secretarias de Fazenda dos Estados e Secretaria da Receita Federal do Brasil, a partir da assinatura do Protocolo de Cooperação do Encontro Nacional dos Administradores Tributários (ENAT) 03/2005, de 27 de agosto de 2005, que atribui ao Encontro Nacional de Coordenadores e Administradores Tributários Estaduais (ENCAT) a coordenação e a responsabilidade pelo desenvolvimento e implantação do Projeto NF-e. Dentre as Secretarias de Fazenda Estaduais, a Secretaria de Fazenda do Estado de Pernambuco (SEFAZ-PE) foi pioneira.

De acordo com o Ministério da Fazenda (2009, p.10), no Manual de Integração do Contribuinte, o Projeto NF-e tem por objetivo a implantação de um modelo nacional de documento fiscal eletrônico para substituir a sistemática atual de emissão do documento fiscal em papel, com validade jurídica garantida pela assinatura digital do remetente, simplificando assim as obrigações acessórias dos contribuintes e permitindo, ao mesmo tempo, o acompanhamento em tempo real das operações comerciais pelo Fisco.

Segundo informações veiculadas no *site* da SEFAZ-PE (http://www.sefaz.pe.gov.br/), a implantação da NF-e constitui grande avanço para facilitar a vida do contribuinte e as atividades de fiscalização so-

bre operações e prestações tributadas pelo Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e pelo Imposto sobre Produtos Industrializados (IPI).

Num momento inicial, a NF-e substituirá as notas modelo 1 e 1A (utilizadas, em regra, para documentar transações comerciais com mercadorias entre pessoas jurídicas) e está sendo emitida apenas por grandes contribuintes desde abril de 2008.

5.2 Programa Minha Certidão

A Corregedoria-Geral da Justiça de Pernambuco (CGJ) lançou, em 2008, o Programa Minha Certidão, em conjunto com o Governo do Estado de Pernambuco, a Agência Estadual de Tecnologia da Informação (ATI), a Associação dos Registradores Civis de Pessoas Naturais (ARPEN-PE), a Secretaria Estadual de Saúde e a Secretaria de Desenvolvimento Social e Direitos Humanos. O objetivo é erradicar o sub-registro[2], facilitando o recebimento da certidão de nascimento, que será emitida na maternidade, no dia do nascimento da criança.

Todo o procedimento de registro de nascimento será viabilizado através do Sistema Estadual de Registro Civil (SERC), que é informatizado e produz a certidão *online*. Dessa forma, os pais não precisam se deslocar até o cartório.

Segundo Miranda (2009), o Corregedor-Geral da Justiça de Pernambuco, desembargador José Fernandes de Lemos, esclareceu que o Estado de Pernambuco tem um percentual elevado de sub-registro, com 21,4% de crianças nascidas vivas sem certidão de registro civil de nascimento conforme dados fornecidos pelo Instituto Brasileiro de Geografia e Estatística (IBGE). O projeto Minha Certidão quer diminuir esse número e contribuir para efetivar a cidadania no País. O SERC será implantado nas maternidades de saúde públicas e privadas situadas em Pernambuco e nos Serviços de Registro Civil (cartórios) mediante convênio com a coordenação da CGJ.

Atualmente, oito unidades de saúde da capital já possuem o sistema, sendo eles: Hospital Barão de Lucena, Hospital das Clínicas, Centro Integrado de Saúde

[2] Segundo o IBGE, sub-registro é o conjunto de nascimentos não registrados no próprio ano de nascimento ou no 1º trimestre do ano subsequente. Contudo, tal definição não abrange todos os casos de pessoas ainda não registradas ou os que não têm em seu poder sua certidão. Os dados informados são estimativas estatísticas e não revelam todas as possibilidades de sub-registramento, já que deveriam ser consideradas as situações de partos domiciliares e a migração populacional. Na prática, porém, a população atingida pela falta de registro é composta, ainda, por aqueles que vivem em entidades de abrigo, pela população de rua, por pessoas com transtorno mental, além da população migratória que chega à região de destino sem documentação e não consegue registrar os filhos. (Referência: CORREGEDORIA GERAL DA JUSTIÇA DO ESTADO DO RIO DE JANEIRO. **Sub-Registro Civil**. Disponível em: < http://cgj.tjrj.jus.br/projetos-especiais/sub-registro-civil>. Acesso em 06 dez. 2013)

Amaury de Medeiros (CISAM), IMIP, Hospital Agamenon Magalhães, Maternidade Barros Lima, Policlínica e Maternidade Arnaldo Marques, e Maternidade Bandeira Filho. A meta do Governo do Estado é interligar todas as 217 maternidades pertencentes ao Sistema Único de Saúde aos 294 cartórios de registro civil existentes em Pernambuco até 2011. No total, o projeto recebeu um investimento de R$ 2,4 milhões, que estão sendo aplicados na aquisição de equipamentos e na capacitação de recursos humanos (GONÇALVES, 2011).

Os computadores instalados nas maternidades vão encaminhar os dados do declarante e a declaração de nascido vivo, que são escaneados e enviados pela Internet para os cartórios. O registrador recebe o material, confere e gera a certidão de nascimento, assinada digitalmente e reenviada para a maternidade. Resultado: a mãe já sai da maternidade com a criança e com a certidão de nascimento.

6 ANÁLISE DOS ESTUDOS DE CASO

Nesta seção são descritos e analisados os dados obtidos sobre os projetos Nota Fiscais Eletrônica e Programa Minha Certidão.

De acordo com os objetivos deste trabalho foram elaborados os questionamentos e submetidos às Instituições detentoras dos projetos em análise. Pela Secretaria de Fazenda do Estado de Pernambuco, o arquiteto de *software* Jonysberg Quintino Peixoto e pela Agência de Tecnologia da Informação de Pernambuco, os gerentes de projeto Enildo Ferreira das Chagas e Tereza Novais Silva, gentilmente responderam aos questionamentos. O Quadro 3 sintetiza as respostas obtidas para cada projeto nos aspectos analisados.

No que diz respeito à discussão das formas de preservação digital, foram obtidas em um primeiro momento poucas informações sobre os procedimentos para a guarda das Notas Fiscais Eletrônicas e Certidões de Nascimento como pode ser observado no Quadro 3. Principalmente se os referidos documentos estão sujeitos a tabelas de temporalidade, bem como se após o prazo de guarda estes ainda serão conservados ou não por terem sido avaliados como de caráter histórico. Neste sentido, foi necessária a submissão de outro roteiro de entrevista com perguntas mais pontuais sobre esses aspectos da gestão documental, sintetizados no Quadro 4.

Quadro 3: Quadro comparativo das aplicações de Certificação Digital

ASPECTOS	PROJETO/INSTITUIÇÃO	
	NF-e/SEFAZ-PE	Minha Certidão/ATI-PE
Ano de implantação	2008	2008
Objetivo	Implantar um modelo nacional de documento fiscal eletrônico.	Erradicar o Sub-Registro de Nascimento.
Metodologia	Implantação de infraestrutura para emissão de nota fiscal eletrônica que facilita o controle pela SEFAZ-PE e Receita Federal do Brasil.	Implantação de Postos de Atendimento de Registro Civil de Nascimento nas Maternidades, nos quais será emitida a Certidão de Nascimento da criança antes da alta da mãe. Interligando Cartórios de Registro Civil e Maternidades.
Autoridades Certificadoras da ICP-Brasil	Todas credenciadas pela ICP-Brasil	SERASA para os certificados digitais pessoais A3 e CERTISIGN para os certificados digitais para servidor web SSL
Programas de computador utilizados para emitir/assinar/visualizar documentos	Os programas para emitir, assinar e visualizar são livres e podem ser obtidos no *site* do portal nacional da NF-e disponível em: < http://hom.nfe.fazenda.gov.br/portal/listaSubMenu.aspx?Id=/fwLvLUSmU8= >	O programa para emitir é o sistema web SERC, para assinar é o BRY Sgner e para visualizar é o proxy ViaCert.
Formato do arquivo	XML	BMP
Local de armazenamento	Em meio digital.	Em meio digital e uma via é impressa para ser entregue ao declarante.
Fundamentação legal	Protocolo ICMS 10 e Decreto Estadual nº 31.612.	Provimento nº 38/2008 da Corregedoria Geral de Justiça-PE, Decreto Estadual 32.876/2008, Provimento nº11/2010 da Corregedoria Geral de Justiça – PE e Provimento nº13/2010 do Conselho Nacional de Justiça (CNJ)
Segurança da informação	Processo de comunicação do contribuinte com o aplicativo autorizador de NF-e, que é feito sob o protocolo HTTPS, com autenticação mútua, ou seja, certificados de servidor e de cliente, para garantir todo o processo.	Possui um Comitê Gestor de Segurança da ATI, Normas Gerais de Utilização de Rede Email Internet, Política de Segurança da Informação – Diretrizes Gerais, Norma para Desenvolvimento Seguro de Aplicações Web, Norma de Segurança de Uso de Rede Sem Fio e Assinatura de Termo de Responsabilidade.
Preservação digital	Utiliza ferramentas para viabilização da guarda, indexação e preservação dos originais.	Rotinas de *backup* para os Servidores de Dados e de Arquivos.
Resultados	Melhor acompanhamento fiscal, aumento da arrecadação e autorização média de 150.000 Notas Eletrônicas para circulação, evitando assim a emissão de 750.000 folhas de nota fiscal modelo 1 e 1^A (em 5 vias).	O projeto está implantado em oito maternidades e 19 cartórios, bem como já foram emitidas mais de dez mil certidões de nascimento.

Fonte: Dados da pesquisa

Quadro 4: Detalhamento da destinação e preservação dos documentos digitais

ASPECTOS	PROJETO/INSTITUIÇÃO	
	NF-e/SEFAZ-PE	Minha Certidão/ATI-PE
Tabela de Temporalidade de Documentos	Não possui.	Não possui.
Destinação do documento digital	Guarda Permanente.	Guarda Permanente.
Estratégias utilizadas para a preservação do documento digital	Migração e cópia de segurança.	Cópia de segurança.

Fonte: Dados da pesquisa

Através dos Quadros 3 e 4 é possível observar o panorama geral da gestão documental adotada por cada projeto e comparar suas especificidades.

Diante das respostas obtidas nas entrevistas e das informações disponíveis nos endereços eletrônicos das Instituições detentoras dos projetos, bem como nas legislações pertinentes a cada projeto, verificou-se metodologias diferentes para emissão do documento certificado digitalmente, mas os projetos utilizam certificados digitais de AC credenciadas pela AC-Raiz da ICP-Brasil. No entanto, devem ser pontuadas suas diferenças.

Enquanto a NF-e permanece em meio digital, a Certidão de Nascimento assinada digitalmente migra para o suporte em papel, utilizando o processo de certificação digital para a elaboração do documento que será impresso. Aqui se observam as finalidades de cada aplicação que convergem para a agilização dos processos de emissão de notas ficais e certidões de nascimento, mas que devido às especificidades de cada tipologia documental apresentam concepções diversas sobre os estágios de preparação e de transmissão de documentos. Pois se colocam a NF-e como original e a Certidão de Nascimento impressa como a original em virtude da legislação notarial existente no Brasil e da necessidade do uso de documentos de identificação civil em suporte de papel. Portanto, apesar das divergências, a tecnologia contribui para a velocidade desses procedimentos altamente burocráticos. Para tanto, espera-se que as legislações sejam adequadas aos avanços tecnológicos atuais e vindouros.

No que se refere a formatos e *softwares*, também são distintos. Enquanto a SEFAZ-PE utiliza a NF-e em

XML e dispõe dos *softwares* livres do Ministério da Fazenda para assinar e visualizar o documento, a ATI utiliza as certidões de nascimento em BMP e *software* proprietário, o BRY Sgner, que tem o objetivo básico de realizar as operações de assinatura digital e que pode ser adquirido gratuitamente no *site* <http://signer.bry.com.br/instrucoes.html >. Enquanto o *Proxy* ViaCert é utilizado para a conferência de assinaturas digitais, realizada nos formulários web utilizados no SERC.

Sobre a perspectiva da preservação digital, Barbedo *et al* (2008) recomendam a não utilização de formatos e *softwares* proprietários para armazenamento e preservação digital a longo prazo, pelas seguintes razões:

- Um formato de arquivo é ultrapassado por outro formato ou por uma versão mais recente que comporta mais complexidade;
- Um dado formato não vinga ou as empresas não criam *software* compatível;
- Um dado formato falha estagna ou já não é compatível com os sistemas atuais;
- O *software* que suporta o formato falha comercialmente ou é adquirido por um concorrente que o retira do mercado.

Nesse sentido, é necessário identificar quais os formatos que por serem normalizados e/ou não proprietários e de fácil preservação em longo prazo poderão ser utilizados alternativamente. Sendo assim, a NF-e está adequada a tal recomendação enquanto a Certidão de Nascimento utiliza-se de formato e programas de computador proprietários em desalinho com tal orientação.

O embasamento legal da SEFAZ-PE está fundamentado no Protocolo ICMS 10 de 18 de abril de 2007, em nível nacional, que estabelece obrigatoriedade da utilização da Nota Fiscal Eletrônica (NF-e) para os setores de fabricação de cigarros e distribuição de combustíveis líquidos. E, em nível estadual, pelo Decreto nº 31.612, de 03 de abril de 2008 que introduz alterações na Consolidação da Legislação Tributária do Estado, relativamente à Nota Fiscal Eletrônica (NF-e) e ao Documento Auxiliar da Nota Fiscal Eletrônica (DANFE).

No que tange a fundamentação legal do Programa Minha Certidão, está amparado pelas seguintes legislações:

• Provimento nº 38/2008 da Corregedoria Geral de Justiça-PE: Determina a utilização do SERC para

realização do Registro de Nascimento e emissão da primeira Certidão no âmbito das Maternidades, bem como normatiza a assinatura da Certidão de Nascimento pelo Método da Certificação Digital.

• Decreto Estadual 32.876/2008: Institui o Comitê Gestor do Programa Minha Certidão, com membros nomeados pelo Ato 3.993/2008.

• Provimento nº11/2010 da Corregedoria Geral de Justiça – PE: Determina a utilização do SERC pelos Cartórios de Registro Civil das Pessoas Naturais do Estado de Pernambuco.

• Provimento nº13/2010 do Conselho Nacional de Justiça (CNJ): Dispõe sobre a emissão de certidão de nascimento nos estabelecimentos de saúde que realizam partos.

No que diz respeito às políticas de segurança e preservação da informação digital, as mesmas são convencionadas por cada Instituição mantenedora do projeto.

No tocante ao meio de comunicação físico, ambos utilizam a Internet com servidores certificados digitalmente. Em relação a normas e políticas de segurança, a SEFAZ-PE informou apenas o processo de comunicação do contribuinte com o aplicativo autorizador de NF-e, que é feito sob o protocolo HTTPS, com autenticação mútua, ou seja, certificados de servidor e de cliente, para garantir todo o processo. Enquanto a ATI mencionou a existência das suas políticas que podem ser acessadas no seu *site* (http://www2.ati.pe.gov.br/web/site-ati), merecendo destaque a Norma Técnica ATI-SGR-PR/001:10 (Política de Segurança da Informação – Diretrizes Gerais), que tem o objetivo de padronizar e estabelecer requisitos mínimos, a fim de proporcionar condições que assegurem à integridade, a confidencialidade, a disponibilidade, bem como a legalidade da informação no âmbito do ambiente computacional da ATI.

No que concerne à preservação da informação digital ressalta-se que nem sempre as instituições possuem condições de manter em longo prazo os seus documentos digitais, uma vez que não têm estrutura tecnológica e recurso suficiente para acompanhar a obsolescência tecnológica. Como também, segundo Innarelli (2007):

> a preservação digital é um assunto complexo e recente e não se restringe ao estudo de mídias, técnicas de backup, técnicas de migração, técnicas de autenticação etc. Este assunto deve ser estudado de forma interdisciplinar e institucionalmente, cabendo aos profissionais da informação a garantia da preservação e manutenção do documento digital

> de forma íntegra e autêntica. (INNARELLI, 2007, p. 71)

A esse respeito, a SEFAZ-PE informou que possui um plano de preservação digital de seus documentos, de caráter confidencial, porém utiliza ferramentas para viabilização da guarda, indexação, preservação dos originais, garantindo sua autenticidade, entre outras. Enquanto a ATI fez menção as suas políticas na palestra proferida por Freitas e Rocha (2011), onde são discriminadas duas formas de *backup*:

- *Backup* do Servidor de Dados: no Servidor de Dados dois tipos *backups* estão agendados, o primeiro é o *backup* que acontece a cada hora, minimizando assim possíveis perdas, e o segundo é o *backup* que acontece diariamente consolidando as informações geradas no dia ambos agendados no *cron* do Linux, um Robô ainda faz um *backup* diário em Fita LTO3 que permanece por até 90 dias.
- *Backup* do Servidor de Arquivos: no Servidor de Arquivos o *backup* é de responsabilidade de um robô que roda diariamente fazendo o *backup* dos arquivos em Fita LTO3 que permanece por até 90 dias.

Dessa forma, verifica-se que estratégias e políticas de preservação digital de ambos os projetos precisam ser repensadas e elaboradas, a fim de salvaguardar por longos períodos seus documentos digitais.

Sobre os resultados do projeto Nota Fiscal Eletrônica Jonysberg Quintino Peixoto informou que houve melhor acompanhamento fiscal; aumento da arrecadação; e autorização média de 150.000 Notas Eletrônicas para circulação, evitando assim a emissão de 750.000 folhas de nota fiscal modelo 1 e 1^{A} (em 5 vias). Com isso a NF-e contribui para a redução dos gastos com impressão de notas fiscais e a redução da sonegação de impostos.

Enquanto Enildo Ferreira das Chagas e Tereza Novais Silva apresentaram os seguintes resultados do Programa Minha Certidão: o projeto está implantado em oito maternidades e 19 cartórios; e foram emitidas mais de dez mil certidões de nascimento. O Programa Minha Certidão agiliza o processo de emissão da Certidão de Nascimento, deixando-a mais ao alcance dos novos cidadãos.

No que tange à legalidade e autenticidade das informações contidas nos registros gerados na forma digital, cabe frisar que tanto a NF-e e a Certidão de Nascimento assinada digitalmente são dotadas de autenticidade e integridade,

proporcionadas pela utilização de certificados digitais da ICP-Brasil cujo amparo legal está contido na já referendada Medida Provisória nº 2.200-2, de 24 de agosto de 2001 que institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

Assim como o amparo legal é reforçado por legislações federais e estaduais (já mencionadas acima) que convencionam a utilização de certificados digitais para a assinatura das Notas Fiscais Eletrônicas e Certidões de Nascimento.

Quanto a gestão documental relativa à preservação digital, descrita no Quadro 4, os dados revelam que, muito embora as instituições não apliquem uma tabela de temporalidade aos documentos digitais, demonstram a preocupação de armazenar os documentos permanentemente. No entanto, apenas a ATI mencionou uma estratégia de preservação digital, adotando a migração. Observa-se também, que ambas as instituições citaram equivocadamente rotinas de cópia de segurança como sendo estratégias de preservação.

Nesse sentido, ressalta-se o senso de guarda e segurança da informação de cada instituição pesquisada, mesmo que a responsabilidade legal para a custódia da NF-e seja dos contribuintes que utilizam a plataforma tecnológica da SEFAZ-PE e no caso das certidões de nascimento, a responsabilidade jurídica fica a cargo dos cartórios, órgãos dotados de fé pública para emitir as certidões de nascimento.

Dessa forma, os planos de preservação digital de documentos devem contemplar mais medidas para combater a obsolescência tecnológica. Assim como, devem atentar ao seguinte problema:

> Em razão da necessidade de conversões, a assinatura digital não garante a autenticidade do documento, no longo prazo, tornando-se necessários outros procedimentos de gestão e de preservação, como a inserção de metadados. Ao se receber um documento assinado digitalmente, deve-se registrar, como metadado de integridade, a informação indicando que o documento foi recebido com tal assinatura e que esta foi verificada. Da mesma maneira, nas sucessivas conversões de formatos, deve-se registrar, também como metadado, o evento de conversão (CONARQ, 2012).

Para os profissionais da Arquivologia é relevante compreender esses processos de produção, tramitação, utilização e armazenamento de documentos digitais. Uma vez que, a correta gestão dos documentos digitais é que permitirá a preservação da memória da

sociedade, devidamente registrada nesse tipo de suporte.

Assim como, defende-se aqui uma inserção maior dos arquivistas em projetos desse gênero, a fim de contribuir com soluções para o gerenciamento dos documentos digitais desde sua produção, utilização, tramitação e destinação final, para convencionar a adoção de mais estratégias para a preservação digital de documentos e estabelecer prazos para as tabelas de temporalidade, instrumento imprescindível para a correta gestão documental.

Segundo Hollós (2010) a informação, hoje gerada em meio digital, trafega em redes cada vez mais velozes e efêmeras. Preservar estas estruturas, ao menos em parte, em termos de conteúdo e ambiência tecnológica é um dos maiores desafios que arquivistas, profissionais da área de tecnologia da informação e conservadores buscam superar.

Além disso, Tammaro e Salarelli (2008) argumentam que a função crítica da preservação digital não diz respeito apenas aos obstáculos da fragilidade do suporte e da obsolescência tecnológica. O problema da preservação é um problema tanto técnico quanto político.

Neste sentido, a compreensão da certificação digital que proporciona autenticidade, integridade e confidencialidade aos novos suportes da informação os quais conservarão a memória da atual sociedade são relevantes para o desenvolvimento de programas e políticas para a preservação da informação digital.

7 CONSIDERAÇÕES FINAIS

A segurança é ativo primordial para a salvaguarda das informações produzidas e recebidas por instituições públicas e privadas, e as informações oriundas de ambiente digital requerem tecnologias que assegurem a autenticidade, a integridade e a confidencialidade dessas informações.

Uma vez que a certificação digital é uma tecnologia que proporciona tais características aos documentos digitais, este trabalho procurou abordar os conceitos e a política relacionada a ela, bem como analisar projetos que aplicam a referida tecnologia.

Dessa forma, o presente trabalho analisou como se dá a aplicação de certificados digitais em documentos eletrônicos e como esses documentos são gerenciados. Assim como, verificou quais os formatos, *softwares* e *hardwares*

utilizados em todo o processo, identificou quais os dispositivos legais que dão respaldo e quais estratégias são utilizadas para a preservação e segurança das informações digitais. Estes estudos de caso proporcionam subsídios a fim de se refletir a melhor forma para organizar, tramitar, utilizar, armazenar e preservar os documentos digitais assinados e certificados digitalmente, que constituem fontes de memória coletiva e individual da sociedade atual.

Neste contexto, o certificado digital é o testemunho da autenticidade, integridade e confidencialidade de uma memória armazenada em meio eletrônico. Com isso, os profissionais da informação devem acompanhar as transformações dos modos de produção e acumulação de registros eletrônicos, bem como refletir e participar da construção de políticas públicas para salvaguarda dos documentos digitais que agora, com o respaldo tecnológico e legal da certificação digital, permanecerão em ambiente eletrônico, não necessitando da migração em suporte papel para ter qualidade legal.

Portanto, devem-se estabelecer estratégias de preservação e gestão documental para que essas informações sejam armazenadas, organizadas, recuperadas e disponibilizadas, garantindo o direito democrático e cultural de acesso às informações de cada cidadão brasileiro, preenchendo assim suas lacunas informacionais.

No que se relaciona aos resultados obtidos em cada estudo de caso, principalmente no que tange a preservação e gestão dos documentos digitais, conclui-se e sugere-se que os dois projetos desenvolvam e apliquem normas e políticas mais criteriosas de preservação e gestão dos documentos (NF-e e Certidão de Nascimento), que defina mais estratégias de preservação e uma tabela de temporalidade de documentos para evidenciar os prazos de destinação de cada documento eletrônico. Como também, desenvolvam ou busquem, por intermédio dos seus profissionais de tecnologia da informação, as soluções necessárias para a manutenção das assinaturas digitais a longos períodos.

Neste contexto, ressalta-se o importante papel que a Arquivologia desempenha a partir dos seus estudos sobre gerenciamento e preservação de documentos digitais. Os estudos da Arquivologia sobre a preservação por longos períodos dos documentos digital

certificados digitalmente são de grande relevância.

Trabalhos futuros podem explorar quais outras estratégias de preservação que poderiam ser utilizadas pelos projetos estudados e elaborar tabela de temporalidade de documentos como proposta de aplicação. Como também outros estudos podem abordar a aplicabilidade da certificação digital em outros tipos de documentos, não só administrativos para atribuir valor de prova, mas como em publicações digitais de documentos de informação científica, tais como dissertações, teses, artigos e livros, a fim de analisar quais os benefícios que a assinatura digital traria para estes documentos e como se daria a sua preservação nos respectivos repositórios.

ELECTRONIC DOCUMENT MANAGEMENT IN DIGITAL CERTIFICATION APPLICATIONS

ABSTRACT

The present article aims to identify and analyze applications of digital certification in order to understand this information technology and its use in digital record management. The use of digital certification gives credibility and legal value to registered information in digital media, contributing to the growing number of such information in the digital environment. Based on literature research this paper discusses the concepts, technologies, public policies regarding the digital certification and the Brazilian Public Key Infrastructure (PKI-Brazil). Lined on case studies and data collection through interviews and literature research, the applications of digital certification Electronic Invoice (NF-e) and My Certificate Program are analyzed for compliance with the ICP-Brazil, programs and formats used in the process of digital certification, procedures used for issuing certificates and digital signature verification, storage of the digitally certified document, legislation, information security, digital preservation and project results. As a result of the study, was verified the existence of federal and state laws that ensure the use of digital certification, differences in application of digital certification, compliance regarding the use of digital certificates belonging to Infrastructure Brazilian Public Keys, as well as differences in security and digital preservation policies designed under the precepts of the institutions that maintain each project under consideration. As conclusions, it is suggested that the projects that made digital certified documents develop and implement more careful standards and policies in terms of the preservation and management of documents.

Keywords: Digital certification. Digital record. Digital record management. Digital preservation.

REFERÊNCIAS

ADAMS, Carlisle; JUST, Mike. **PKI**: Ten Years Later. In: 3rd Annual PKI R&D Workshop, p. 69 - 84, abr. 2004.

ALONSO, Luiza Beth Nunes; FERNEDA, Edilson; BRAGA, Lamartine Vieira. Governo Eletrônico e Políticas Públicas: análise sobre o uso da certificação digital no Brasil. **Informação & Sociedade**, João Pessoa, v.21, n.2, p. 13-24, maio/ago. 2011. Disponível em: <http://www.ies.ufpb.br/ojs2/index.php/ies/article/view/4066/5959>. Acesso em: 20 jul. 2011.

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

BARBEDO, Francisco *et al*. **Recomendações para a produção de Planos de Preservação Digital**. Lisboa: Direção Geral de Arquivos – DGARQ, 2008. Disponível em: < http://dgarq.gov.pt/files/2008/10/PlanoPreservacaoDigital_V2-02.pdf> Acesso em 09 dez. 2013.

BODÊ, Ernesto Carlos. Assinaturas Digitais e Arquivologia. **Arquivística.net**, Rio de Janeiro, v.2, n.1, p.52-69, jan./jun. 2006. Disponível em: <http://www.arquivistica.net/ojs/viewarticle.php?id=51 >. Acesso em: 23 jul. 2011.

BRASIL. Medida provisória nº 2.200-2, de 24 de agosto de 2001. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 ago. 2001. Seção 1, p. 65.

BRASIL. Decreto nº 6.605, de 14 de outubro de 2008. **Diário Oficial da República Federativa do Brasil**, Poder Executivo, Brasília, DF, 15 out. 2008. Seção 1, p. 2.

CARVALHO, Hugo Eiji Tibana. **PKI – Infra-estrutura de chaves públicas**. Trabalho desenvolvido para a disciplina Redes de Computadores II, da UFRJ, no período 2008.2, adaptado. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2008_2/hugo/Criptografia.html> Acesso em: 04 dez. 2013.

CARVALHO, João Antônio. **Informática para concursos**: teoria e questões. 2. ed. Rio de Janeiro: Elsevier, 2006.

CONSELHO NACIONAL DE ARQUIVOS – CONARQ. **Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais.** Rio de Janeiro: Câmara Técnica de Documentos Eletrônicos, 2012. Disponível em: < http://www.conarq.arquivonacional.gov.br/media/diretrizes_presuncao_autenticidade_publicada.pdf> Acesso em 09 dez. 2013.

FREITAS, Carolina e ROCHA, Verlaynne. Iniciativas da ATI em Certificação Digital. In: 9º CERTFÓRUM, 2011, Recife. **Palestras...** Recife: ATI, 2011. Disponível em: < http://www2.ati.pe.gov.br/web/site-ati/palestra-certforum>. Acesso em: 05 jul. 2011.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed.13. reimpr. São Paulo: Atlas, 2009.

GONÇALVES, Rui. **Programa Minha Certidão chega ao Barão de Lucena**.

Recife, Folha de Pernambuco Digital. Disponível em: < http://189.1.14.127/index.php/component/content/category/20-cidadania-saude?layout=blog&limit=9&month=11&year=2010&start=195>. Acesso em: 04 jul. 2011.

HOLLÓS, Adriana Lucia Cox. **Preservação e memória social**. In: Rubens Ribeiro Gonçalves da Silva; Aurora Leonor Freixo; Iole Costa Terso; Ricardo Sodré de Andrade. (Org.). Cultura, representação e informação digitais. Salvador: Editora da Universidade Federal da Bahia, 2010, p. 29-40.

INNARELLI, H. C. **Os dez mandamentos da preservação digital**. In: SANTOS, V. B.; INNARELLI, H. C.; SOUSA, T. R. B. Arquivística: temas contemporâneos. Brasília: SENAC, 2007.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **O que é certificação digital**. Cartilha, ITI, Brasília, 2005. Disponível em: <http://www.iti.gov.br/images/publicacoes/cartilhas/cartilhaentenda.pdf>. Acesso em: 30 nov. 2013.

_____. Brasil e evolução Virtual, **Revista Digital**, Brasília, ano 1, nº 3, 1º semestre 2010. Disponível em: < http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/revistadigital1_semestre_2010.pdf>. Acesso em: 15 ago. 2010.

KUHN, D. R.; HU , V. C.; POLK , W. T.; Chang, S.-J.. Introduction to public key technology and the federal PKI infrastructure. **NIST**, February 2001.

MAIA, Luiz Paulo; PAGLIUSI, Paulo Sergio. **Criptografia e Certificação Digital**. Disponível em < http://www.training.com.br/lpmaia/pub_seg_cripto.htm>. Acesso em 01 mar 2011.

MINISTÉRIO DA FAZENDA. **Manual de Integração do Contribuinte**. Versão 4.0.1, Nov 2009. Disponível em: <http://www.nfe.fazenda.gov.br/portal/listaConteudo.aspx?tipoConteudo=33ol5hhSYZk=> . Acesso em: 24 jul. 2010.

MIRANDA, Rosa. **Minha Certidão - Software pernambucano é modelo nacional.** Assessoria de Comunicação Social do Tribunal de Justiça de Pernambuco**.** Recife, 15 abr. 2009. Disponível em: <http://direito2.com/tjpe/2009/abr/15/minha-certidao---software-pernambucano-e-modelo-nacional >. Acesso em: 04 jul. 2011.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos**: uma abordagem teórica da diplomática arquivística contemporânea. Rio de Janeiro: Editora FGV, 2002.

SILVA, Luiz Gustavo *et al*. **Certificação Digital**: Conceitos e Aplicações. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

TAMMARO, Anna Maria; SALARELLI, Alberto. **A Biblioteca Digital**. Brasília: Briquet de Lemos/Livros, 2008.

WEISE, Joel. Public Key Infrastructure Overview. **Sun BluePrints OnLine**, USA, ago. 2001. Disponível em: < http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf> Acesso em 22 Jul. 2011.

Artigo submetido em: 06 ago. 2013 **Artigo aceito em: 19 fev. 2014**