UNIVERSIDADE FEDERAL DE PERNAMBUCO
PROGRAMA DE PÓS-GRADUAÇÃO
EM CIÊNCIA DA INFORMAÇÃO
MESTRADO EM CIÊNCIA DA INFORMAÇÃO

APLICAÇÕES DE CERTIFICAÇÃO DIGITAL NO RECIFE: PERSPECTIVAS EM CIÊNCIA DA INFORMAÇÃO

Sânderson Lopes Dorneles

Orientador: Prof. Dr. Renato Fernandes Corrêa

Recife
2011

SÂNDERSON LOPES DORNELES

APLICAÇÕES DE CERTIFICAÇÃO DIGITAL NO RECIFE: PERSPECTIVAS EM CIÊNCIA DA INFORMAÇÃO

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Universidade Federal de Pernambuco como requisito para obtenção do título de mestre em Ciência da Informação.

Orientador: Prof. Dr. Renato Fernandes Corrêa

Área de Concentração: Informação, Memória e Tecnologia

Recife
2011

Catalogação na fonte
Bibliotecária Gláucia Cândida da Silva, CRB4-1662

D713a Dorneles, Sânderson Lopes.
Aplicações de certificação digital no Recife: perspectivas em Ciência da Informação / Sânderson Lopes Dorneles. – Recife: O autor, 2011.
172 p. : il.

Orientador: Renato Fernandes Corrêa.
Dissertação (Mestrado) – Universidade Federal de Pernambuco, CAC. Ciência da Informação, 2011.
Inclui bibliografia, anexos e apêndices.

1. Ciência da informação. 2. Tecnologia da Informação. 3. Memória. Documentos eletrônicos. I. Corrêa, Renato Fernandes (Orientador). II. Titulo.

020 CDD (22.ed.) UFPE (CAC 2011-91)

Dissertação de Mestrado apresentada por Sânderson Lopes Dorneles a Pós-graduação em Ciência da Informação do Centro de Artes e Comunicação da Universidade Federal de Pernambuco, sob o título "**Aplicações de certificação digital no Recife: perspectivas em Ciência da Informação**" orientada pelo Prof. Dr. Renato Fernandes Corrêa e aprovada pela Comissão Examinadora formada pelos professores:

_____

Prof. Dr. Renato Fernandes Corrêa

Departamento de Ciência da Informação / UFPE

_____

Prof. Dr. Ricardo Bastos Cavalcante Prudêncio

Centro de Informática / UFPE

_____

Prof. Dr. Fábio Mascarenhas e Silva

Departamento de Ciência da Informação / UFPE

Autor:

_____

Sânderson Lopes Dorneles

Ao meu pai Jorge Luiz Souza Dorneles (in memorian), minha referência de caráter e responsabilidade.

À minha esposa Valéria e nossa filha Ana Clara, minhas fontes de inspiração e dedicação.

AGRADECIMENTOS

À minha mãe pelo incentivo em todas as minhas empreitadas e pela palavra de conforto nos momentos difíceis.

À minha esposa, exemplo de companheirismo e carinho. A mulher que eu amo e me faz muito feliz.

À minha irmã, que sempre torce por mim.

Ao meu orientador, Professor Renato, pelas orientações e revisões do meu trabalho.

À Professora Maria Cristina, pelo apoio em momentos difíceis.

Ao Professor Marcos Galindo, pelas primeiras orientações.

Aos demais professores do Programa de Pós Graduação em Ciência da Informação que contribuíram na minha formação.

À secretaria do Programa de Pós Graduação em Ciência da Informação, na figura da Suzana sempre prestativa e de ótimo humor.

Às minhas colegas do Programa de Pós Graduação em Ciência da Informação com as quais aprimorei meu conhecimentos.

À colega Ângela Nascimento, pela amizade e a sua ajuda na consecução da minha pesquisa.

Aos entrevistados que contribuíram para a elaboração deste trabalho.

Às chefias do meu serviço que foram flexíveis em relação ao meu horário de trabalho.

E, a todos que diretamente ou indiretamente me ajudaram para a realização deste trabalho.

RESUMO

O presente trabalho objetiva identificar e analisar aplicações e políticas públicas de certificação digital, desenvolvidas na cidade do Recife, a fim de compreender essa tecnologia da informação e seu uso na gestão de documentos eletrônicos. 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 eletrônico. Com base em pesquisa bibliográfica e estudos de caso, este trabalho aborda os conceitos, tecnologias, as políticas públicas a respeito da certificação digital, a Infraestrutura Brasileira de Chaves Pública (ICP-Brasil) e as políticas de segurança e preservação da informação adotadas por cada aplicação de certificação digital. Pautado em estudos de caso e coleta de dados por meio de entrevistas, as duas aplicações de certificação digital no Recife, 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, local de 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, as diferenças de metodologias adotadas pelos projetos em suas aplicações, as conformidades no que tangem a utilização de certificados digitais pertencentes à Infraestrutura Brasileira de Chaves Públicas e políticas de segurança e preservação da informação concebidas sob os preceitos das Instituições

mantenedoras de cada projeto em análise. E como conclusão, 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.

Palavras-chave: certificação digital. tecnologia da informação. documento eletrônico. memória.

ABSTRACT

The present study aims to identify and analyze applications and digital certification policies, developed in the city of Recife, in order to understand the information technology and its use in the management of electronic documents. The use of digital certification gives credibility to the registration and legal value of information in digital media, contributing to the growing number of such information in the electronic environment. Based on literature research and case studies, this paper discusses the concepts, technologies, public policies regarding the digital certification, the Brazilian Public Key Infrastructure (ICP-Brazil) and security policies and preservation of information taken by each application of digital certification. Lined on case studies and data collection through interviews, the two applications of digital certification in Recife, 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 location of the digitally certified document, legislation, information security, digital preservation and project results. As a result of the study, the existence of federal and state laws that ensure the use of digital certification was verified, as were the different methodologies adopted by the projects in their applications, compliance regarding the use of digital certificates belonging to Infrastructure Brazilian Public Keys and security policies and preservation of information designed under the precepts of the institutions that maintain each project under consideration. It is suggested that the two projects develop and implement more careful standards and policies in terms of the preservation and management of documents (NF-e and birth certificate), and that they define more preservation

strategies and a table of temporality of documents to provide evidence of the terms of destination for each electronic document.

Keywords: digital certification. information technology. electronic document. memory.

LISTA DE SIGLAS

AC - Autoridade Certificadora

AC-Raiz – Autoridade Certificadora Raiz

AIIM - Association of Information and Image Management

AR - Autoridade de Registro

ARPEN - Associação dos Registradores Civis de Pessoas Naturais

ATI - Agência Estadual de Tecnologia da Informação

CCSDS - Consultative Committee for Space Data Systems

CCTA - Central Computer and Telecommunications Agency

CD-ROM - Compact Disc Read-Only Memory

CERTFÓRUM - Fórum de Certificação Digital

CNJ - Conselho Nacional de Justiça

CG - Comitê Gestor

CGJ - Corregedoria-Geral da Justiça de Pernambuco

CISAM - Centro Integrado de Saúde Amaury de Medeiros

CITU - Central IT Unit

CONARQ - Conselho Nacional de Arquivos

CSIRO - Commonwealth Scientific and Industrial Research Organization

DNV - Declaração de Nascido Vivo

e-ARQ Brasil - Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos

ENCAT - Encontro Nacional dos Administradores e Coordenadores Tributários Estaduais

ENAT - Encontro Nacional dos Administradores Tributários

EROS - Electronic Records from Office Systems

DANFE - Documento Auxiliar da Nota Fiscal Eletrônica

ICMS - Imposto sobre Circulação de Mercadorias e Serviços

IPI - Imposto sobre Produtos Industrializados

ICP-Brasil - Infra-Estrutura de Chaves Públicas Brasileira

IDS - Intrusion Detection Systems

InterPARES - International Research on Permanent Authentic Records in Electronic System

IP - Internet Protocol

IPS - Intrusion Prevention Systems

ITI – Instituto Nacional de Tecnologia da Informação

NAA - National Archives of Austrália

NASA - National Aeronautics and Space Administration

NBAD - Network Behaviour Anomaly Detectors

NF-e – Nota Fiscal Eletrônica

OAIS - Open Archival Information System

PDF - Portable Document Format

PKI - Public Key Infrastructure

PROV - Public Record Office Victoria

SEFAZ-PE - Secretaria da Fazenda do Estado de Pernambuco

SERC - Sistema de Registro Civil

SIGAD - Sistema Informatizado de Gestão Arquivística de Documentos

SPED - Sistema Público de Escrituração Digital

SSL - Security Socket Layer

TCP - Transmission Control Protocol

TJPE - Tribunal de Justiça de Pernambuco

UBC - University of British Columbia

UNESCO - United Nations Educational, Scientific and Cultural Organization

VERS - Victorian Electronic Records Strategy

VPN - Virtual Private Networks

XML – Extensible Markup Language

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

As tecnologias da informação e as novas formas de produzir, disseminar e recuperar o conhecimento revolucionaram os processos de criação de documentos. A Internet por sua vez encurtou as noções de tempo e espaço agilizando de forma eficaz a forma de transmitir documentos. Um problema, contudo permanece em aberto, como um alerta aos cientistas e usuários é a questão da legalidade e autenticidade das informações contidas nos registros gerados na forma digital, bem como a discussão das novas formas de preservação dessa memória certificada digitalmente.

O presente trabalho apresenta reflexões pertinentes à aplicação da certificação digital sobre informações registradas em suportes digitais, a fim de garantir a **autenticidade, confidencialidade e integridade** das mesmas diante da reconhecida instabilidade da informação registrada em meio digital.

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 a todos os segmentos da sociedade brasileira.

Isso só será possível se houver uma ampla articulação entre os diversos setores comprometidos com a preservação do patrimônio arquivístico digital, e em cooperação com os organismos nacionais e internacionais.

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. Criados a partir da percepção do Governo Federal da importância de se regulamentar 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.

O certificado digital consiste em uma tecnologia que permite a identificação do autor de uma informação registrada em suporte eletrônico. Para tanto, necessita de outras tecnologias, tais como: algoritmos de criptografia que possibilita o sigilo na troca de informações; bem como a função *hashing* que assegura a integridade do conteúdo registrado em suporte eletrônico; e assinatura digital que é a marca de autoria do emissor de determinada informação digital. Além disso, o certificado deve ser obtido por intermédio de uma Autoridade Certificadora.

Com a adoção da certificação digital na esfera governamental e comercial nos arquivos das organizações, o número de documentos eletrônicos aumentará estrondosamente, e com isso surge a necessidade de se manter esses documentos por longos períodos, em virtude dos seus prazos de guarda.

Neste contexto, o presente trabalho busca identificar e analisar aplicações e políticas públicas de certificação digital desenvolvidas na cidade do Recife, importante capital da região Nordeste do Brasil, que se destaca por ser um polo de formação e desenvolvimento de tecnologias da informação, a fim de compreender essa tecnologia da informação e seu uso na gestão de documentos eletrônicos. Para tanto, traçou-se

como objetivos específicos: Descrever o funcionamento dos programas e políticas públicas de certificação digital; Verificar a conformidade dos programas com a legislação federal; Descrever requisitos de segurança: autenticidade, confidencialidade e integridade; e Avaliar políticas de preservação digital.

À luz da Ciência da Informação e da interdisciplinaridade da Arquivologia e Tecnologia da Informação, serão abordados conceitos relevantes do tema, a fim de analisar dois projetos, como também ressaltar a importância da preservação da memória digital.

Neste sentido, o presente estudo vale-se da pesquisa exploratória, fazendo uso da pesquisa bibliográfica sobre os principais conceitos da certificação digital, a fim de abordar as aplicações de certificação digital no Recife como objetos de estudo. E estudos de caso que consistem do Projeto Nota Fiscal Eletrônica (NF-e) da Secretaria da Fazenda do Estado de Pernambuco (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.

Para tanto, a base teórica do trabalho está estruturada em dois grandes capítulos temáticos: o capítulo 2 versa sobre o documento digital, onde são debatidos conceitos e características, haja vista o documento digital ser objeto da aplicação de certificação digital. Esse capítulo é composto por uma seção que aborda sobre Memória e Preservação Digital de Documentos, outra seção sobre Normas e Políticas de Preservação Digital, e por fim, uma seção sobre Segurança da Informação Digital. Já o capítulo 3 é destinado ao tema principal do trabalho, a certificação digital e os conceitos envolvidos, subdividido em uma seção sobre as políticas

públicas de certificação digital e outra sobre as aplicações desenvolvidas no Recife, dividida em duas subseções: o Projeto Nota Fiscal Eletrônica (NF-e) e o Programa Minha Certidão.

No capítulo 4 são descritos os procedimentos metodológicos utilizados para a elaboração do trabalho. O capítulo 5 traz os resultados dos estudos de caso, onde são apresentados os dados obtidos, bem como é realizada a análise dos mesmos. E, para concluir, são tecidas as considerações finais do trabalho no capítulo 6.

2 DOCUMENTO DIGITAL

Este capítulo versa sobre o documento digital, onde se aborda conceitos e características na seção 2.1.

Na seção 2.2 é abordada a Memória e Preservação Digital de Documentos, onde é discutida a relevância da guarda e conservação das informações registradas em suportes eletrônicos.

A seção 2.3 trata sobre Normas e Políticas de Preservação Digital, que ressalta as estratégias e dispositivos utilizados para a conservação por longo tempo dos documentos eletrônicos.

E por fim, a seção 2.4 aborda sobre Segurança da Informação Digital, temática relevante ao estudo, haja vista a certificação digital ser uma tecnologia que proporciona segurança às informações que são registradas e que tramitam em meio eletrônico.

2.1 CONCEITOS E CARACTERÍSTICAS DO DOCUMENTO DIGITAL

Faz-se necessário para este trabalho definir o que seria o documento digital ou documento eletrônico. Para isto é necessário, compreender um pouco mais o que seria a informação no contexto da Ciência da Informação.

Segundo Capurro e Hjorland (2007) existem muitos conceitos de informação e eles estão inseridos em estruturas teóricas mais ou menos explícitas. O significado é, entretanto, determinado nos contextos social e cultural. Assim sendo, no

tocante ao presente trabalho, o conceito de informação atribuído por Silva (2006 p. 150 - 151) se enquadra na estrutura teórica do trabalho, uma vez que a informação refere-se a um fenômeno humano e social que compreende tanto o dar forma a idéias e a emoções (informar), como a troca, a efetiva interação dessas idéias e emoções entre seres humanos (comunicar). E identifica um objeto científico, a saber: conjunto estruturado de representações mentais e emocionais codificadas (signos e símbolos) e modeladas com/pela interação social, passíveis de serem registradas em qualquer suporte material (papel, filme, banda magnética, disco compacto, etc.) e, portanto, comunicadas de forma assíncrona e multi-direcionada. Em síntese, este objeto científico é o documento, que em linhas gerais, consiste em informação registrada em um suporte.

Partindo desse raciocínio, o documento eletrônico é a informação registrada em suportes eletrônicos, tais como: mídia magnética (englobando fita magnética de computador, tanto em rolo ou carretel quanto em cassetes, discos rígidos de computador e disquetes) e discos ópticos (CD-ROMs, WORM, discos rígidos regraváveis).

Para Santos (2005, p.36):

> Os documentos eletrônicos podem ser registrados sobre suportes tangíveis e intangíveis, sendo que os tangíveis são mais assemelhados aos documentos tradicionais. Teoricamente, porém, sempre haverá um servidor onde as informações disponíveis na Internet estarão armazenadas, mesmo que sua localização seja difícil de identificar. O mesmo ocorre com os demais documentos eletrônicos que, necessariamente, estão registrados em suporte “físico”, seja magnético ou óptico, como disquetes, fitas magnéticas, CD – ROMS, discos rígidos etc.

No tocante aos aspectos jurídicos dos documentos eletrônicos, o principal atributo encontra-se no valor de prova e testemunho pelo qual o documento resguarda. Segundo Guimarães, Nascimento e Furlaneto Neto (2005, p.23) o documento jurídico parece agregar determinados valores ao conter elementos voltados ao seu objetivo probatório e/ou comprobatório, como também parece não deixar dúvidas quanto a sua percepção de documento no âmbito da Ciência da Informação e áreas afins.

Aliado a isso, são necessários os mecanismos que auferem autenticidade, confidencialidade e integridade às informações eletrônicas, como também, dispositivos legais. No que se refere aos mecanismos, a utilização da certificação digital apresenta-se como solução, pois é uma tecnologia baseada em criptografia que garante a autenticidade, confidencialidade e integridade das informações registradas em meio digital, tema melhor explorado no próximo capítulo.

A busca de fundamentação legal para a utilização do suporte digital pode ser vista em diversos países, com avanços significativos na América do Norte e Europa. No Brasil, Pinheiro (2009, p.162) faz referências a leis e decretos do ordenamento jurídico brasileiro a respeito dos documentos eletrônicos. Dentre as quais cita: Medida Provisória nº 2.200, de 28 de junho de 2001 – Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, e dá outras providências; Decreto nº 3.872, de 18 de julho de 2001 – Dispõe sobre o Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira (CG ICP-Brasil) e dá outras providências; Decreto nº 3.996, de 31 de outubro de 2001 – Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

Ainda sobre dispositivos legais, vale ressaltar a afirmação de Pinheiro (2009, p. 160) "... a tecnologia trouxe mais ferramentas para validação jurídica das provas, algo que se busca há muito, e hoje, por certo, já há força legal muito maior numa prova composta por um *e-mail* do que apenas um testemunho oral ou um mero fax; o mesmo para uma assinatura digital ou biométrica do que apenas o número de um RG ou CPF anotados a mão sem conferência do documento, ou cuja foto, normalmente, está desatualizada. Afinal, para todos nós, o teste de DNA continua sendo considerado prova inequívoca de autoria, apesar de não ter lei e não ser 100% de certeza". E para finalizar a autora diz:

> O arquivo original não é mais o papel, mas o dado, que deve ser guardado de modo adequado à preservação de sua autenticidade, integridade e acessibilidade, para que sirva como prova legal. Nessa nova realidade, a versão impressa é a cópia, e as testemunhas são as máquinas. (PINHEIRO, 2009, p. XXXVII).

Com isso, evidencia-se a utilização dos documentos digitais como meio de registro das informações de caráter testemunhal e comprobatório que futuramente poderão ser dotadas de valor histórico. O que demanda cuidados específicos para armazenar e preservar essas informações por longos períodos. Na seção a seguir faz-se uma reflexão sobre a memória e a preservação digital de documentos.

2.2 MEMÓRIA E PRESERVAÇÃO DIGITAL DE DOCUMENTOS

A memória e a preservação digital de documentos podem ser relacionadas à recuperação de informações. Para

Le Goff (2003) o conceito de memória é crucial. Embora o enfoque do autor seja exclusivamente dedicado à memória tal como surge nas ciências humanas (fundamentalmente na história e na antropologia), e se ocupe mais da memória coletiva que nas memórias individuais, ele considera importante descrever sumariamente a nebulosa memória no campo científico global. Assim, a memória como propriedade de conservar certas informações, remete-nos em primeiro lugar a um conjunto de funções psíquicas, graças às quais o homem pode atualizar impressões ou informações passadas, ou que ele representa como passadas. Deste ponto de vista da memória compreende a psicologia, a psicofisiologia, a neurofisiologia, a biologia e, quanto às perturbações da memória, das quais a amnésia é a principal, a psiquiatria.

Neste sentido, é relevante tratar a memória como fato social, não deixando de fazer referência a mencionada plataforma biológica da memória. Segundo Meneses (2007) a memória contribui significativamente para o processo evolutivo da humanidade, haja vista a memória permitir a recuperação de experiências, é ela quem vai possibilitar que as respostas satisfatórias possam ser utilizadas em todas as situações similares. Mas ainda falta alguma coisa, pois mesmo que estas experiências pudessem ser recuperadas e definirem padrões, como a tipologia de artefatos, elas permaneceriam individuais. Essa outra coisa que está faltando, que se associa à memória, é a linguagem. É a linguagem que permite a memória ser um veículo de socialização das experiências individuais. Assim como, são necessários os meios pelos quais será armazenada e divulgada a memória, canalizada por:

> A invenção da imprensa, com tipos móveis, e a urbanização, com mudanças fundamentais na organização e nas relações sociais, nas atividades,

> papéis e percepções do indivíduo, trarão mudanças importantes para a memória individual e coletiva. De uma sociedade baseada na transmissão oral dos saberes necessários ao trabalho e à vida em grupo, novas ocupações relacionadas ao comércio e à vida nas cidades demandam registros de operações, de listas, de transações. Desenvolver-se-ão, a partir daí, artifícios cada vez mais sofisticados para guardar e disseminar a memória em textos e imagens. Este processo culmina com o computador, capaz de guardar grandes quantidades de informações e abarcar todos os meios inventados anteriormente para registrar e armazenar a memória. (KESSEL, 2004, p. 2)

A memória armazenada em computadores necessita de cuidados especiais para perpetuar-se. Para tanto, a preservação que é um conjunto de medidas e estratégias de ordem administrativa, política e operacional que contribuem direta ou indiretamente para a preservação da integridade dos materiais (CASSARES, 2000, p.12) é fundamental, pois se sabe da instabilidade das informações registradas em suportes digitais e do grande número produzido e acumulado. Com isso, a preservação digital é primordial para a conservação da memória de uma sociedade. De acordo com Borba (2009, p.17):

> A preservação digital é uma etapa basilar, e necessariamente posterior ao desenvolvimento das Tecnologias da Informação e Comunicação e do sistema de redes que criou a nova ambiência para a informação em meio digital. Corresponde a certo modo ao fenômeno do desenvolvimento das estratégias e métodos para conservação e preservação de papel e materiais bibliográficos, ocorrida em momento, pós-expansão documental iniciada com o ciclo das grandes guerras mundiais. Neste momento histórico criaram-se os mega-ambientes de arquivos e bibliotecas, induzindo

> a preocupação com a conservação para as gerações futuras dos registros em papel. Em última análise, preservação digital tem a ver com conservação e preservação do patrimônio cultural da humanidade, cuja atenção antes estava voltada apenas para os registros em suportes físicos orgânicos, e que agora aplica-se aos formatos de expressão digital.

Portanto, a memória registrada em suporte digital necessita de preservação a fim de permanecer disponível às atuais e futuras gerações. Assim sendo, são oportunos os questionamentos de Baratin e Jacob (2008):

> Como resguardar esta memória? Como transmitir o saber? A censura, as políticas de acesso a informação (Igreja, Estado), também influenciaram a transmissão e acesso à memória; destas instituições surge à indagação: O que guardar? Para quem guardar? Por que guardar?

A estas questões cabe à sociedade respondê-las, seja através de políticas públicas que assegurem a preservação da memória, os critérios de acesso, disponibilidade e difusão. Para tanto, as Instituições de Memória (Arquivos, Bibliotecas e Museus) podem ser entendidos como o local de guarda de grande produção que remonte a história e a memória de uma nação para servir a determinados grupos. Partindo-se dessa premissa é que o entendimento de Memória para as áreas de Arquivologia, Biblioteconomia e Museologia foi associado ao conjunto das informações registradas, isto é, aos documentos e representações que podem ser consultados, servindo de memória social ou memória de longo prazo. Com efeito, essas três áreas valem-se da memória no sentido de armazenagem e preservação dos saberes (conservação), para a posterior recordação por parte da sociedade.

Seja qual for à especialidade, a memória envolve dois aspectos cruciais e anteriores: diz respeito à linguagem e à mídia, esta entendida como tecnologia da informação e comunicação (CARELLI; MONTEIRO; PICKLER, 2006 p.115). Sendo assim, aí está à relação entre Memória e Preservação para estas áreas da Ciência da Informação, que dentre os objetos de estudo encontra-se a preservação de suportes (no estudo em análise os suportes digitais) os quais são registradas informações integrantes de memórias individuais, coletivas e consequentemente sociais.

A produção e acumulação de informações em ambientes digitais têm aumentado exponencialmente, e isso se atribui às aplicações de tecnologias da informação e comunicação que aumentam a cada dia, em virtude da facilidade com que se produz, armazena, acessa e troca informações.

Para tanto, são utilizadas tecnologias que atribuem requisitos de segurança da informação, tais como a certificação digital, imprescindíveis para a realização de negócios e serviços, aumentando assim, a credibilidade no uso de suportes digitais para o registro de informações. E para essas informações permanecerem disponíveis e seguras por longos períodos, há a necessidade do desenvolvimento de políticas, projetos e normas que assegurem a preservação digital dessas informações. Segundo Ferreira (2006, p. 20) ao longo dos últimos 10 anos, foram muitos os projetos e iniciativas internacionais que contribuíram para a edificação da base de conhecimento que atualmente suporta o domínio científico da preservação digital. Desses projetos resultaram ideias, conceitos e estratégias que conduziram ao reconhecimento universal do problema e à elaboração de possíveis soluções.

Portanto, a informação se configura como o objeto que liga a Memória e a Preservação, uma vez que não há memória registrada sem informações e tão pouco preservação de registros sem informações. Para tanto, as pesquisas de métodos para a preservação de suportes da informação são primordiais para a salvaguarda das memórias produzidas e acumuladas pela sociedade. Dessa forma, é relevante apresentar algumas normas e políticas de preservação digital na seção que segue.

2.3 NORMAS E POLÍTICAS DE PRESERVAÇAO DIGITAL

O Conselho Nacional de Arquivos (CONARQ), órgão colegiado responsável pela elaboração de políticas nacionais de arquivos, em sua 34ª reunião plenária, realizada em 6 de julho de 2004, no Rio de Janeiro, aprovou uma Carta para a Preservação do Patrimônio Arquivístico Digital. Nela o CONARQ convoca os setores públicos e privados, envolvidos com a produção e proteção especial dos documentos em formato digital, a envidarem esforços para garantir sua preservação e acesso contínuo, condição fundamental para a democratização da informação arquivística do Brasil e a preservação da memória nacional.

Dentre as recomendações, a referida Carta alerta os governos, as organizações públicas e privadas, as instituições de ensino e pesquisa e todos os setores da sociedade brasileira comprometidos com a inclusão informacional para diversos problemas. De acordo com o Conarq (2004, p. 2-3) são eles:

a) **Dependência social da informação digital -** O governo, a administração pública e privada, a pesquisa científica e tecnológica e a expressão cultural dependem cada vez mais de documentos digitais, não disponíveis em outra forma, para o exercício de suas atividades.

b) **Rápida obsolescência da tecnologia digital -** A preservação de longo prazo das informações digitais está seriamente ameaçada pela vida curta das mídias, pelo ciclo cada vez mais rápido de obsolescência dos equipamentos de informática, dos *softwares* e dos formatos.

c) **Incapacidade dos atuais sistemas eletrônicos de informação em assegurar a preservação de longo prazo -** Atualmente, não obstante os pesados investimentos em tecnologia da informação há uma crescente debilidade estrutural dos sistemas eletrônicos de informação, que os incapacitam de assegurar a preservação de longo prazo e o acesso contínuo às informações geradas num contexto de rápido avanço tecnológico.

d) **Fragilidade intrínseca do armazenamento digital -** A tecnologia digital é comprovadamente um meio mais frágil e mais instável de armazenamento, comparado com os meios convencionais de registrar informações, tendo um impacto profundo sobre a gestão dos documentos digitais no presente para que se tenha garantia de acesso no futuro.

e) **Complexidade e custos da preservação digital:** A preservação de documentos digitais pressupõe uma constante atualização de suporte e de formato, além de estratégias para possibilitar a recuperação das informações, que passam pela preservação da plataforma de *hardware* e *software* em que foram

criados, pela migração[1] ou pela emulação[2]. Estas são algumas iniciativas que vêm sendo tomadas, mas que não são ainda respostas definitivas para o problema da preservação de longo prazo. Não há soluções únicas e todas elas exigem investimento financeiro elevado e contínuo em infraestrutura tecnológica, pesquisa científica aplicada e capacitação de recursos humanos.

f) Multiplicidade de atores envolvidos: A preservação da informação em formato digital não se limita ao domínio tecnológico, envolve também questões administrativas, legais, políticas, econômico-financeiras e, sobretudo, de descrição dessa informação através de estruturas de metadados que viabilizem o gerenciamento da preservação digital e o acesso no futuro. Desta forma, preservar exige compromissos de longo prazo entre os vários segmentos da sociedade: poderes públicos, indústria de tecnologia da informação, instituições de ensino e pesquisa, arquivos e bibliotecas nacionais e demais organizações públicas e privadas.

---

[1] Migração é a transferência periódica de materiais digitais de uma configuração de *hardware/software* para outra ou, de uma geração de tecnologia computacional para a geração seguinte. O propósito da migração é preservar a integridade dos objetos digitais e assegurar a habilidade dos clientes para recuperar, expor e usá-los de outra maneira diante da constante mudança da tecnologia. (TASK FORCE ON THE ARCHIVING OF DIGITAL INFORMATION *apud* ARELLANO, 2004)

[2] As técnicas de emulação sugerem a preservação do dado no seu formato original, por meio de programas emuladores que poderiam imitar o comportamento de uma plataforma de *hardware* obsoleta e emular o sistema operacional relevante. (ARELLANO, 2004)

Para tanto, o Conarq (2004, p. 3) diz que 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[3] e que assegurem, ao longo do tempo, a autenticidade, a integridade, o acesso contínuo e o uso pleno da informação a todos os segmentos da sociedade brasileira. E considera que isto só será possível se houver uma ampla articulação entre os diversos setores comprometidos com a preservação do patrimônio arquivístico digital, e em cooperação com os organismos nacionais e internacionais.

Desta forma, o CONARQ considera a importância das instituições arquivísticas, do poder público, da indústria de tecnologia da informação e comunicação e das instituições de

[3] A obsolescência tecnológica refere-se tanto a *hardware* quanto a *software* e formatos. O *hardware* obsoleto pode ser, por exemplo, um determinado tipo de suporte (disco óptico, fita magnética, por exemplo), unidades de disco, unidades de fita magnética ou os próprios processadores e componentes utilizados na execução de programas (*software*). As mudanças em *software* – incluindo sistemas operacionais, sistemas de gerenciamento de banco de dados e aplicativos como editores de texto, planilhas eletrônicas, editores de imagem, entre outros – costumam ser bastante freqüentes. Os *softwares* podem ser simplesmente descontinuados, substituídos por outros equivalentes, supostamente melhores, ou ainda ter sua versão atualizada para correção de *bugs* ou acréscimo de novas funcionalidades. Os formatos também sofrem alterações, muitas vezes em função de mudanças ocorridas nos programas (software) aos quais estão associados. Novos programas (*software*) podem ser compatíveis com os formatos antigos, mas também podem apresentar incorreções durante operações de leitura e escrita de dados nesses formatos. (e-ARQ Brasil, p. 81 - 82)

ensino e pesquisa, implementarem ações, especialmente no que concerne aos três tópicos enumerados abaixo:

1 - Elaboração de estratégias e políticas

Gestão arquivística de documentos: Definir procedimentos e estratégias de gestão arquivística de documentos quando da criação, transmissão e preservação de documentos em formatos digitais, com o objetivo de garantir a produção e manutenção de documentos fidedignos, autênticos, acessíveis, compreensíveis e preserváveis.

Instrumentalização dos arquivos: Orientar quanto à criação de infraestrutura nas instituições arquivísticas e nas organizações produtoras e acumuladoras de documentos, no que concerne a equipamentos, sistemas, metodologias e recursos humanos capacitados, para que possam desempenhar um papel ativo na gestão da preservação dos documentos digitais.

Governo eletrônico: Promover a participação de representantes das instituições arquivísticas nos projetos de governo eletrônico, para a definição de estratégias, padrões e normas de gestão, preservação e acesso a documentos e informações, conforme orientação do Conselho Internacional de Arquivos e da UNESCO.

Ações cooperativas: Incentivar programas cooperativos de preservação de documentos digitais para aplicação e compartilhamento de recursos sob a forma de acordos, consórcios, convênios e parcerias.

2 - Estabelecimento de normas

Padrões e protocolos: Definir e/ou recomendar a utilização de padrões e protocolos abertos e de aceitação ampla na criação, uso, transmissão e armazenamento de documentos

digitais; e desenvolver soluções em cooperação com organizações de pesquisa e a indústria de tecnologia da informação e comunicação.

Requisitos funcionais: Definir os requisitos funcionais e estimular sua adoção para orientar o desenvolvimento e a aquisição de sistemas eletrônicos de gestão arquivística, que sejam adequados às especificidades da legislação e das práticas arquivísticas brasileiras.

Metadados: Definir estruturas padronizadas de metadados[4] e determinar a sua utilização nos sistemas eletrônicos de gestão arquivística, com o propósito de gerir a preservação e a acessibilidade dos documentos digitais.

Segurança da informação digital: Definir política de segurança da informação, que considere os aspectos legais, organizacionais, humanos e tecnológicos, de modo a garantir a autenticidade dos documentos digitais e o sigilo da informação, bem como a proteção contra perdas, acidentes e intervenções não autorizadas.

3 - Promoção do conhecimento

Agenda de pesquisa: Desenvolver uma agenda nacional de pesquisa para a preservação e longevidade dos documentos digitais, alinhada com as principais iniciativas nacionais e internacionais, com a participação das agências governamentais de fomento e de amparo à pesquisa, universidades e outras entidades dos setores público e privado.

---

[4] Metadados: são dados estruturados e codificados, que descrevem e permitem acessar, gerenciar, compreender e/ou preservar outros dados ao longo do tempo. (Arquivo Nacional, 2005)

Ensino e formação de recursos humanos: Estimular a inserção do tema Preservação do Patrimônio Arquivístico Digital na formação dos profissionais de informação, especialmente dos arquivistas, nos cursos de graduação e pós-graduação.

Disseminação do conhecimento: Estabelecer ações de identificação, disseminação e compartilhamento do conhecimento e a utilização de metodologias e técnicas para a gestão e a preservação de documentos arquivísticos digitais.

Como se pôde observar, o foco da preservação é a manutenção do acesso, que pode implicar na mudança de suporte e formatos, bem como na atualização do ambiente tecnológico. A fragilidade do suporte digital e a obsolescência tecnológica de *hardware*, *software* e formato exigem essas intervenções periódicas.

Thomaz (2006, p. 120 - 127), no seu artigo sobre preservação de documentos eletrônicos de arquivo, faz referência a importantes projetos e normas sobre preservação digital no mundo, cujo objetivo é a busca de soluções para a preservação de documentos digitais por longos períodos. Assim destacam-se os seguintes projetos e normas:

Functional Requirements for Evidence In Recordkeeping[5] da Universidade de Pittsburgh, EUA, mais conhecido como Projeto de Pittsburgh, conduzido no período de fevereiro de 1993 a janeiro de 1996. Esse projeto apresentou como resultados o conjunto de treze requisitos funcionais necessários a um sistema de arquivos eletrônicos e

[5] Mais informações sobre o projeto, disponível em: <http://www.archimuse.com/papers/nhprc/BACartic.html>. Acesso em 14 ago. 2010

o modelo de metadados em seis camadas, ligadas e mantidas juntamente com o documento, denominado *Business Acceptable Communications* - BAC.

Preservation of The Integrity of Electronic Records[6], mais conhecido como projeto UBC, conduzido na *School of Library*, *Archival and Information Studies da University of British* Columbia, Canadá, de abril de 1994 a março de 1997. Os pesquisadores do projeto UBC trabalharam em colaboração com a *Records Management Task Force* do departamento de defesa norte-americano para identificar os requisitos para criação, manuseio, e preservação de arquivos eletrônicos confiáveis e autênticos na sua fase ativa, isto é, no período em que ainda sejam necessários para o desenvolvimento das atividades rotineiras da organização. O padrão norte-americano DoD 5015.2[7], resultante desse projeto, está sendo usado pela agência de sistemas de informação de defesa para certificar fornecedores de aplicações de gerenciamento de arquivos.

Projeto InterPARES - *International Research on Permanent Authentic Records in Electronic System (*Pesquisa Internacional sobre Documentos Arquivísticos Autênticos em Sistemas Eletrônicos*),* coordenado pela *University of British* Columbia, Canadá, tem desenvolvido conhecimento teórico-metodológico essencial para a preservação de longo prazo de documentos arquivísticos digitais autênticos. O projeto teve início em 1999 e, atualmente, encontra-se em sua terceira fase. O Projeto InterPARES é integrado por uma equipe de professores e pesquisadores da Europa, Ásia, África e

---

[6] Mais informações sobre o projeto, disponível em: <http://www.interpares.org/UBCProject/intro.htm.> Acesso em 14 ago. 2010.

[7] Norma norte-america que estabelece requisitos para a Gestão de Registros Eletrônicos.

Américas, de diferentes disciplinas como ciência e tecnologia da informação, Arquivologia, Biblioteconomia, Direito e História. A primeira fase do projeto, **InterPARES 1,** teve como objetivo identificar requisitos conceituais para avaliar e manter a autenticidade dos documentos digitais "tradicionais" produzidos e recebidos no curso das atividades administrativas e legais. Esta fase, iniciada em 1999 e concluída em 2001, gerou diversos produtos como: requisitos conceituais para avaliar a autenticidade dos documentos arquivísticos digitais; modelos de processos de seleção e preservação de documentos arquivísticos digitais autênticos; glossário; sítio na Internet e a publicação intitulada *The long term preservation of authentic electronic records: findings of InterPARES Project*[8].

Em sua segunda fase, denominada **InterPARES 2**, realizada no período de 2002 a 2006, o projeto teve por foco documentos arquivísticos digitais gerados no contexto de atividades artísticas, científicas e governamentais, em sistemas experimentais, interativos e dinâmicos. Nesta fase os produtos gerados foram: base de dados de terminologia; modelos conceituais de preservação; registro e análises de diversos esquemas de metadados; diretrizes para produção, manutenção e preservação de documentos digitais autênticos e um conjunto de estratégias voltadas para a preservação de documentos digitais de longo prazo. No ano de 2007 teve início a terceira fase do projeto, agora denominada **InterPARES 3**, com término previsto para o ano de 2012. Esta fase tem por objetivo capacitar programas e organizações (públicas ou privadas), responsáveis pela produção e

[8] Disponível em: <http://www.imaginar.org/dppd/DPPD/82%20pp%20The%20Long-term%20Preservation%20of%20Authentic%20Electronic.pdf>. Acesso em 14 ago. 2010.

manutenção de documentos arquivísticos digitais, a desenvolver estratégias de preservação e acesso de longo prazo a esses documentos. Para tanto será aplicado o conhecimento teórico-metodológico desenvolvidos nas duas primeiras fases.

***Victorian Electronic Records Strategy* (VERS)** [9] - conduzido pelo *Public Record Office Victoria* (PROV) em parceria com a *Australian Commonwealth Scientific and Industrial Research Organisation* – CSIRO e a *Ernst & Young*. O desenvolvimento do VERS começou em 1994 quando o PROV entendeu que estava diante de desafio significativo para a preservação de documentos eletrônicos produzidos pelas agências do governo do estado australiano de Victoria. O resultado final foi o relatório *Victorian electronic records strategy* publicado em 1999. Esse relatório concluiu que "a captura de documentos eletrônicos em formato de longo prazo é possível e alcançável com tecnologia corrente e que o arquivamento de documentos eletrônicos é possível e alcançável na atualidade", formando a base para a primeira versão do padrão VERS. O padrão VERS[10] foi formalmente lançado pelo PROV em abril de 2000. Ao final da investigação técnica, o *National Archives of Australia* - NAA publicou seu padrão de metadados, decidindo-se, por razões práticas, adaptar porção significativa dos metadados VERS ao seu padrão. O padrão VERS encontra-se em segunda versão publicada em 31 de julho de 2003. O PROV lançou oficialmente em 13 de dezembro de 2005 seu *Digital Archives*

---

[9] Mais informações sobre o projeto, disponível em: <http://www.prov.vic.gov.au/vers/>. Acesso em 14 ago. de 2010.

[10] Padrão de Gestão de Registros Eletrônicos. Disponível em: <http://www1.unece.org/cefact/platform/download/attachments/31850501/Explanation_99-7_Advice_ver_2-0.pdf?version=1>. Acesso em 14 ago. de 2010.

para gerenciar, preservar e oferecer acesso a VERS – *compliant digital records* (VEOs) gerados pelo governo australiano de Victoria e atualmente está desenvolvendo um conjunto de ferramentas para auxiliar usuários do VERS a construírem VEOs.

Electronic Records from Office Systems **(EROS)**[11] - estabelecido pelo *Public Record Office* - PRO em 1995 para produzir liderança do governo do Reino Unido no gerenciamento de documentos eletrônicos de arquivo. O programa, apoiado por um comitê plurisetorial composto pelos gerentes *seniors* dos principais departamentos, representantes da *Central Computer and Telecommunications Agency* - CCTA e *Central IT Unit* - CITU e presidido pelo mantenedor dos documentos públicos de arquivo, definiu como objetivo geral garantir o acesso futuro a documentos eletrônicos de arquivo de valor permanente produzidos no âmbito do governo do Reino Unido. O programa produziu até o momento, dentre outros, o guia de gerenciamento, avaliação e conservação de documentos eletrônicos; requisitos e metadados para sistemas gerenciadores de documentos eletrônicos de caráter arquivístico; ferramentas para inventário, avaliação, classificação, conservação, gerenciamento de documentos eletrônicos de escritório, gerenciamento de correspondências eletrônicas e gerenciamento de documentos Web.

[11] Mais informações no *site* do Arquivo Nacional do Reino Unido. Disponível em: <http://www.pro.gov.uk/recordsmanagement/eros/default.htm>. Acesso em 14 ago. 2010.

Norma ISO 14721:2003[12] - estabeleceu uma estrutura de termos e conceitos comuns que constituem o sistema aberto de arquivamento de informação – SAAI (*Open Archival Information System* – OAIS), um sistema encarregado de preservar em longo prazo e manter o acesso à informação digital de qualquer natureza. Foi desenvolvido pelo *Consultative Committee for Space Data Systems* (CCSDS) para o *National Aeronautics and Space Administration* (NASA), EUA. O modelo de referência SAAI aborda os modelos de dados usados para representar a informação e o conjunto completo de funções arquivísticas para a preservação da informação, envolvendo admissão, arquivamento, gerenciamento de dados, acesso e disseminação, além da migração de informação digital para novas mídias e formatos e o intercâmbio de informação digital entre arquivos. Com o modelo de referência SAAI, as instituições arquivísticas passarão a entender os conceitos arquivísticos necessários para a preservação em longo prazo e acesso à informação digital. O modelo de referência SAAI também servirá de base para desenvolvimento de grande quantidade de padrões relacionados.

Norma ISO 19005-1 - publicada no dia 13 de setembro de 2005, especificou o formato *Portable Document Format* - PDF16 como padrão universal para arquivamento de documentos eletrônicos em longo prazo. Esse *Portable Document Format* (PDF) é chamado PDF/*Archive* ou simplesmente PDF/A. Foram três anos de trabalho de um comitê formado por mais de 300 pessoas para a conclusão da

[12] Uma norma ISO é um documento, estabelecido e aprovado por consenso, que provê, para uso comum, regras, guias e/ou características para uma atividade ou seus resultados, com o objetivo de alcançar o grau de excelência num dado contexto. (Fonte: *site* da ISO *Social Responsibility archives* http://www.iso.org)

norma, incluindo profissionais de governo, da indústria de tecnologia da informação e de associações como a *Association of Information and Image Management* - AIIM. Baseada na versão 1.4 do PDF da *Adobe Systems*, a norma define o que pode e o que não pode estar em um formato PDF, eliminando dos documentos códigos de programação, elementos externos, fontes não desejadas. Com o PDF/A, as instituições arquivísticas poderão intercambiar seus conteúdos digitais com muita facilidade, pois o formato possui uma série de recursos que facilitam essa tarefa, tais como, suporte interno a metadados em XML, imagens supercomprimidas, imagens pesquisáveis pelo conteúdo, conexões de hipertexto etc. A expectativa é de que o formato PDF/A torne-se preferencial em projetos nos quais a permanência dos documentos seja fundamental, substituindo definitivamente os formatos de escritório proprietários.

E-ARQ[13] - No Brasil, merece destaque o e-ARQ Brasil, neste documento é apresentado um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil - que foi elaborado no âmbito da Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos no período de 2004 a 2006. O e-ARQ Brasil estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos – SIGAD- independente da plataforma tecnológica em que for desenvolvido e/ou implantado. O e-ARQ Brasil especifica todas as atividades e operações técnicas da gestão arquivística de documentos desde a produção, tramitação, utilização e arquivamento até a sua destinação final. Todas essas atividades poderão ser desempenhadas pelo SIGAD, o

[13] Disponível em : <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/earqbrasilv1.pdf.> Acesso em 14 ago. 2010.

qual conferirá credibilidade à produção e à manutenção de documentos arquivísticos (preservação digital).

Sendo assim, e para melhor visualização, segue abaixo um quadro resumo dos projetos e normas apresentados:

TÍTULO	ORIGEM	PERÍODO	RESULTADO
Projeto Pittsburgh	Universidade de Pittsburgh, EUA	De 1993 a 1996	- Treze requisitos funcionais; - Modelo de metadados; e - Documento denominado *Business Acceptable Communications (*BAC).
Projeto UBC	*School of Library, Archival and Information Studies da University of British,* Columbia, Canadá	De 1994 a 1997	- Padrão norte-americano DoD 5015.2.
Victorian Electronic Records Strategy – VERS	Conduzido pelo *Public Record Office Victoria* – PROV, Estado de Victoria, Austrália	De 1994 até os dias atuais.	- Padrão *Victorian electronic records strategy* (VERS).

Electronic Records from Office Systems – EROS	*Public Record Office* – PRO, Reino Unido.	De 1995 até os dias atuais.	- Guia de gerenciamento, avaliação e conservação de documentos eletrônicos; - Requisitos e metadados para sistemas gerenciadores de documentos eletrônicos de caráter arquivístico; e - Ferramentas para inventário, avaliação, classificação, conservação, gerenciamento de documentos eletrônicos de escritório, gerenciamento de correspondências eletrônicas e gerenciamento de documentos Web.
Projeto InterPARES	Pesquisa internacional coordenada pela *University of British* Columbia, Canadá	O projeto teve início em 1999 e, atualmente, encontra-se em sua terceira fase	- Primeira fase: requisitos conceituais para avaliar a autenticidade dos documentos arquivísticos digitais, modelos de processos de seleção e preservação de documentos arquivísticos digitais

			autênticos, glossário, sítio na Internet e uma publicação intitulada *The long term preservation of authentic electronic records: findings of InterPARES Project*. - Em sua segunda fase, foram gerados os seguintes produtos: base de dados de terminologia, modelos conceituais de preservação, registro e análises de diversos esquemas de metadados, diretrizes para produção, manutenção e preservação de documentos digitais autênticos e um conjunto de estratégias voltadas para a preservação de documentos digitais de longo prazo. - Terceira fase do projeto, capacitar programas e organizações a desenvolver estratégias de preservação e acesso de longo prazo a esses documentos.

Norma ISO 14.721- Modelo de Referência OAIS (*Open Archival Information System Reference Model*)	*Consultative Committee for SpaceData Systems* (CCSDS), EUA.	2002	– Modelo de referência OAIS.
Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil)	Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos, Brasil.	De 2004 a 2006	- Modelo de Requisitos da gestão arquivística de documentos
Norma ISO 19005-1	*Association of Information and Image Management* – AIIM.	2005	– Norma PDF/A

Quadro 1 – Resumo de projetos e normas

Com isso, observa-se que as iniciativas são recentes. Elas são oriundas, principalmente, da década de 90, cujo período demarca a popularização e propagação do uso da Internet, que em muito influencia na produção e acumulação de documentos digitais. Segundo levantamento do ***Internet World Stats***[14], sítio da web especializado em estatísticas

[14] Disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em 30 jun 2011.

sobre Internet no mundo, são 2 bilhões de usuários da Internet espalhados pelo mundo, cerca de 30,2% do total de habitantes do planeta, e no Brasil são 75,9 milhões de usuários, dados atualizados até 31 de março de 2011. Tudo isso, reforça a relevância das tecnologias da informação no cotidiano das pessoas, bem como valida a preocupação para a salvaguarda dos documentos eletrônicos que circulam em sistemas informatizados.

De acordo com as orientações apresentadas, será possível elaborar boas estratégias para a estruturação de planos de preservação digital. E, consequentemente, conservar os registros informatizados os quais se tornarão fontes primordiais de memória histórica.

2.4 SEGURANÇA DA INFORMAÇÃO DIGITAL

A segurança da informação[15] é atributo imprescindível aos sistemas de informações quer sejam pessoais ou institucionais. Sistemas informatizados são alvos de ameaças naturais (inundação, terremotos, tremores de terra, furacão, tempestade elétrica); humanas (pessoas mal intencionadas que invadem sistemas e/ou produzem vírus computacionais para alterar, destruir ou subtrair dados); e ambientais (poluição, fuligem, vazamento de líquidos tóxicos, elementos radioativos). Para tanto, Organismos Internacionais e Nacionais criaram requisitos para o desenvolvimento de políticas de segurança da informação, dentre as quais

[15] O objetivo da segurança da informação é proteger a organização detentora da informação dos diversos tipos de ameaças para garantir a continuidade dos seus negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. (SILVA *et al*, 2008, p. 4)

merecem destaque a Norma Internacional ISO/IEC 17799:2000.

Segundo Gonçalves (2004), a Norma de Segurança da Informação trouxe mais do que vários controles de segurança, ela permitiu a criação de um mecanismo de certificação das organizações, semelhante as certificações ISO já existentes, contudo esta nova certificação "afirma" que a organização certificada manipula os seus dados e os dados dos clientes de forma segura, independentemente da forma como eles estão armazenados.

A Associação Brasileira de Normas Técnicas (ABNT), que é a responsável pelo Fórum Nacional de Normalização, em abril de 2001, disponibilizou para consulta pública o Projeto 21:204.01-010, que daria origem a norma nacional de segurança da informação: NBR ISO/IEC 17799. A versão final da NBR ISO/IEC-17799, foi homologada em setembro de 2001 e sua publicação inclui oficialmente o Brasil no conjunto de países que, de certa forma, adotam e apóiam o uso da norma de Segurança da Informação. A NBR ISO/IEC 17799 a partir de 2005 passou a ser chamada NBR ISO/IEC 27002.

Para garantir o objetivo da segurança da informação, a proteção do capital informacional das entidades contra ameaças e ataques de terceiros ou até mesmo de pessoas internas de uma organização, a NBR ISO/IEC 27002 define as principais características da segurança da informação: a Confidencialidade, a Integridade e a Disponibilidade das Informações.

A **Confidencialidade -** é definida pela NBR como sendo: a garantia de que a informação só pode ser acessada e manipulada por pessoas autorizadas, ou seja, ela é restrita a um conjunto de entidades, que podem ser seres humanos ou podem ser um sistema eletrônico.

A **Integridade -** implica que toda vez que uma informação é manipulada ela está consistente, ou seja, que não foi alterada ou adulterada por um acesso legal ou ilegal.

A **Disponibilidade -** é a garantia de que uma informação sempre poderá ser acessada, pelas pessoas e processos autorizados, independentemente do momento em que ela é requisitada e do local no qual está armazenada.

Segundo Pinheiro (2009, p. 119) alguns autores defendem o acréscimo de mais dois aspectos: a autenticidade e a legalidade[16]. Para Semola (2003, p.46) os referidos aspectos são características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

Além desses, Carvalho (2006, p. 472) cita outro termo, que é bastante usado em segurança da informação: Não-Repúdio. Valendo-se, ainda, de Carvalho (2006) é relevante citar os conceitos de autenticidade e Não-Repúdio dados pelo autor:

---

[16] Na linguagem política, entende-se por legalidade um atributo e um requisito do poder, daí dizer-se que um poder é legal ou age legalmente. É importante ressaltar que a legalidade reflete fundamentalmente o acatamento a uma estrutura normativa posta, vigente e positiva. A legalidade, como acatamento a uma ordem normativa oficial, não possui uma qualidade de justa ou injusta. Compreende a existência de leis, formal e tecnicamente impostas, que serão obedecidas por condutas sociais presentes em determinada situação institucional. (BOBBIO, 2004)

A **Autenticidade** – é a garantia da identidade de uma pessoa (física ou jurídica) ou de um servidor (computador) com quem se estabelece uma transação (de comunicação, como um *e-mail*, ou comercial, como uma venda *on-line*). Essa garantia, normalmente, só é de 100% efetiva quando há um terceiro de confiança (uma instituição com esse fim: certificar a identidade de pessoas e máquinas) atestando a autenticidade de quem pergunta (ex: quando se comunica, pela Internet, com o *site* de banco, tem-se a completa certeza que é com o banco que se está travando aquela troca de informações?). Quando se puder associar, de forma única e certeira, um ato ou documento digital a uma pessoa física (cidadão) ou jurídica, será possível estabelecer regras jurídicas para as transações digitais.

O **Não-Repúdio** – é a garantia de que um agente não consiga negar falsamente um ato ou documento de sua autoria. Essa garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não-repúdio quando houver Autenticidade e Integridade (ou seja, quando for possível determinar quem mandou a mensagem e quando for possível garantir que a mensagem não foi alterada). Novamente, entra-se no mérito de que só haverá tal garantia 100% válida, se houver uma instituição que emita essas garantias.

De posse de tais atributos, que norteiam os requisitos básicos de segurança das informações, devem-se estabelecer as políticas de segurança da informação, ações que são ou não permitidas durante a operação de um sistema, pautadas na avaliação de risco dos bens da organização, ou seja, um estudo deve ser feito sobre a probabilidade de possíveis ameaças acontecerem, analisando as vulnerabilidades do sistema e qual o impacto potencial que causará à organização se esses riscos acontecerem. Logo após a análise dos riscos,

pode-se escolher os controles de segurança, baseados nos custos de implementação em relação aos riscos que serão reduzidos e nas perdas potenciais caso as falhas na segurança ocorram. Porém, fatores não financeiros, como a reputação da organização, a memória institucional, também devem ser levados em consideração. (SILVA *et al*, 2008).

Os controles devem considerar os aspectos físicos, lógicos e humanos. No que tange ao controle físico, são barreiras que limitam o acesso aos suportes físicos das informações, podem ser utilizados salas com mecanismos de acesso biométricos de identificação, senhas, grades, monitoramento por câmeras de vídeo e alarmes. A escolha dos mecanismos depende dos recursos financeiros disponíveis de organização para aplicação. Já os controles lógicos, são barreiras para impedir ou limitar o acesso às informações em ambientes digitais, vale-se de inúmeras ferramentas, dentre as quais podem ser divididas em três grupos (ZAPATER e SUZUKI, 2005): gestão de identidade, defesa contra ameaças e criptografia das informações.

1) Gestão de Identidade: ferramentas que permitem a correta identificação de um usuário para lhe conferir acesso de acordo com seu perfil.

Identificação/Autenticação: permitem identificar unicamente um usuário e verificar a autenticidade da sua identidade através de mecanismos variados, como, por exemplo, senhas pré-definidas, certificados digitais, biometria ou dispositivos portáteis (*tokens, smart cards*).

Autorização/Controle de acesso: possibilitam especificar as ações permitidas e níveis de privilégio diferenciados para cada usuário através do estabelecimento de políticas de uso.

Public Key Infrastructure (PKI)*/Certification Authority*: realizam a geração e gestão de chaves e certificados digitais que conferem autenticidade aos usuários ou à informação. Outra aplicação dessa categoria de ferramentas é o fornecimento de chaves para suportar soluções de criptografia.

2) Defesa contra Ameaças: diversas soluções atuando, de forma preventiva ou corretiva, na defesa contra ameaças à segurança de uma corporação.

Proteção de perímetro: permitem definir uma fronteira, lógica ou física, em torno de um conjunto de ativos de informação e implementar as medidas necessárias para evitar a troca de informação não autorizada através do perímetro. Os *firewalls* representam as soluções mais comuns de proteção de perímetro, podendo realizar inspeção e filtragem de pacotes de dados, analisando as diversas camadas até o nível da aplicação. Segundo Alecrim (2004) existem dois tipos básicos de conceitos de *firewalls*: o que é baseado em filtragem de pacotes e o que é baseado em controle de aplicações. O *firewall* que trabalha na filtragem de pacotes é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de *firewall* determina que endereços IPs e dados podem estabelecer comunicação e/ou transmitir/receber dados. Enquanto, *firewalls* de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são conhecidos como *proxy*. Este tipo não permite comunicação direta entre a rede e a Internet. Tudo deve passar pelo *firewall*, que atua como um intermediador. Este tipo de *firewall* é mais complexo, porém muito seguro, pois todas as aplicações precisam de um *proxy*. Caso não haja um *proxy*, a aplicação simplesmente não funciona. O *firewall* de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a

Internet (ou entre a rede e outra rede). Tais características deixam claro que este tipo de *firewall* é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

Detecção de anomalias e intrusão: realizam o monitoramento de redes, plataformas e aplicações visando a detecção de atividades não autorizadas, ataques, mau uso e outras anomalias de origem interna ou externa. Empregam métodos sofisticados de detecção que variam desde o reconhecimento de assinaturas, que identificam padrões de ataques conhecidos, até a constatação de desvios nos padrões de uso habituais dos recursos de informação. Os *Intrusion Detection Systems* (IDS) são as ferramentas mais utilizadas nesse contexto e atuam de maneira passiva, sem realizar o bloqueio de um ataque, podendo atuar em conjunto com outros elementos (ex.: *firewalls*) para que eles realizem o bloqueio. Uma evolução dos IDS são os *Intrusion Prevention Systems* (IPS), elementos ativos que possuem a capacidade de intervir e bloquear ataques. Tanto IDS como IPS podem existir na forma de aplicações de segurança, instalados na rede, ou na forma de host IDS/IPS, que podem ser instalados nas estações de trabalho e servidores. Outras ferramentas importantes nesta categoria são os *Network Behaviour Anomaly Detectors* (NBAD) que, espalhados ao longo da rede, utilizam informações de perfil de tráfego dos diversos roteadores e *switches* para imediatamente detectar ataques desconhecidos, ataques distribuídos (*Distributed Denial of Service* – DDoS) e propagação de *worms*.

Proteção contra pragas virtuais: garantem que os sistemas e os recursos de informação neles contidos não sejam contaminados. Incluem, principalmente, os antivírus e filtros de conteúdo. Os antivírus ganham cada vez mais sofisticação, realizando a detecção e combate de ameaças que vão além

dos vírus, incluindo *trojans*, *worms*, *spyware* e *adware*. Os filtros de conteúdo aplicam políticas de utilização da web, examinando conteúdo consumido durante a navegação (ex.: programas executáveis, *plug-ins*). Existem também os filtros de conteúdo voltados para *e-mails*, chamados ferramentas anti-spam. As ferramentas de proteção contra infecção são instaladas tipicamente nas estações de trabalho e servidores, mas já existem versões voltadas para a rede, ou seja, eliminam ameaças antes de chegarem ao usuário, bloqueando na própria rede os pacotes infectados.

Identificação de vulnerabilidades: ferramentas utilizadas pelos profissionais de segurança para identificar vulnerabilidades nos sistemas existentes (*vulnerability scanners*). Realizam uma varredura nos sistemas em busca de falhas de segurança, a partir de uma base de conhecimento de vulnerabilidades existentes em elementos de rede, sistemas e aplicações.

Backup/recovery: permitem o *backup*, de forma automatizada, de informações contidas em estações de trabalho e servidores. Além disso, possuem funcionalidades de recuperação e restauração de informações perdidas em caso de incidentes.

3) Criptografia das informações [17] : mecanismos que garantem a confidencialidade da informação em diversas camadas, através da aplicação de algoritmos de criptografia. Variam desde a criptografia das informações gravadas em dispositivos de memória (ex.: discos rígidos, *storage)* até criptografia das informações em trânsito visando à comunicação segura. Os equipamentos mais conhecidos para

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

a comunicação segura são os chamados concentradores de VPN (*Virtual Private Networks*), que permitem a formação de redes virtuais seguras nas quais todo o tráfego trocado (entre dois nós de rede – *site-to-site* – ou entre uma estação remota e um nó de rede – *client-to-site*) é criptografado utilizando algoritmos como o IPSec ou, mais recentemente, o SSL (*Security Socket Layer*).

Com relação aos controles humanos, que são barreiras para impedir o acesso de pessoas mal intencionadas às informações, requerem uma atenção especial a sua aplicação, haja vista a dificuldade de controle de pessoas. É comum se preocupar com pessoas externas às organizações, porém deve-se ter cuidado, também, com os próprios colaboradores das organizações que se aproveitam das facilidades de acesso para sabotarem e/ou subtraírem informações sigilosas das instituições. Para tanto, é primordial um controle de acesso às áreas físicas de armazenamento de equipamentos computacionais e rigorosas seleções de pessoas autorizadas à manipulação de determinadas informações.

Ainda, sobre a questão de controles humanos, Marciano e Marques (2006, p.97) enfatizam o enfoque social da segurança da informação, haja vista toda informação ter característica social. Uma vez que a informação está intimamente ligada à construção do conhecimento, e por essa via torna-se um instituinte cultural, gerador de mudanças ou reprodutor estabelecido. Neste caso, entendendo a sociedade como produto humano e o homem como produto social, buscamos captar e interpretar o fenômeno informacional em seu movimento dialético entre ambos. Assim “toda informação é social” (CARDOSO, 1994). Para Cardoso (1994) este entendimento está contido num recurso pedagógico que permite identificar o conhecimento e analisar metodologias

acerca da produção, organização, disseminação, consumo e incorporação da informação, enfatizando a diversidade de processos e relações que ocorrem no cotidiano de pessoas, segmentos, classes e instituições sociais.

Corroborando com essa discussão, Marteleto (1986) afirma que a informação, sua geração, comunicação e uso constituem um fenômeno de difícil previsão, explicação ou mensuração. Pois a maior parte dos estudiosos que se ocupam em analisá-la concorda que se trata de um fenômeno social, pois ocorre entre indivíduos e grupos que vivem socialmente, ou seja, é o resultado das relações sociais. Neste sentido, voltando aos aspectos inerentes à segurança da informação, Marciano e Marques (2006, p. 97) sintetizam muito bem a relação social do homem com a problemática da segurança da informação. Pois segundo os mesmos, o crescimento alarmante dos incidentes relacionados à segurança da informação alerta para a premente necessidade de uma visão fundamentada em bases sólidas para este problema, a qual extrapola em muito o âmbito da tecnologia. Esta é capaz de apresentar soluções para alguns dos problemas apresentados, mas falha clamorosamente quanto é apresentada a vários outros. Para tanto, deve-se analisar adequadamente os papéis representados pelos usuários e suas interações diante dos sistemas de informação, reforçando assim o aspecto social da segurança da informação.

Portanto, não se esgota aqui toda a discussão a cerca de segurança da informação. Porém, foi possível demonstrar a relevância deste atributo para a salvaguarda do capital informacional gerado por organizações e particulares.

Segue um quadro resumo que sintetiza a relação entre cada característica da informação e cada tipo de controle.

CARACTERÍSTICAS DA SEGURANÇA DA INFORMAÇÃO	TIPOS DE CONTROLES		
	Físico	Lógico	Humano
Confidencialidade	Controla o acesso aos suportes físicos das informações, garantindo assim a confidencialidade das informações	Controla mecanismos que garantem a confidencialidade da informação, através de algoritmos de criptografia	Seleciona as pessoas que terão acesso às informações sigilosas
Integridade	Impede que informações registradas em suportes eletrônicos sejam adulteradas sem a devida permissão.	Utiliza *softwares* específicos que dificultam e acusam a adulteração de informações (*função hashing*)	-
Disponibilidade	Controle de *hardwares*	Controle de *softwares*	-
Autenticidade	-	Permite identificar unicamente um usuário e verificar a autenticidade da sua identidade através de mecanismos variados, por	-

		exemplo, senhas pré-definidas, certificados digitais e biometria.	
Legalidade	-	-	Controle a partir de dispositivos legais (leis, decretos, regulamentos e normas)
Não-Repúdio	-	-	Fiscaliza por intermédio de uma Autoridade Certificadora

Quadro 2 – Características da Segurança da Informação X Tipos de Controles

De posse das abordagens desenvolvidas nesse capítulo, que foram relevantes para a introdução da temática principal do trabalho, cabe agora, discutir no capítulo que segue a certificação digital.

3 CERTIFICAÇÃO DIGITAL

O presente capítulo é o tema principal deste trabalho. E como tal, é necessário explorar os conceitos e características que o envolvem. Neste sentido, a seção 3.1 aborda o conceito de certificação digital e as tecnologias da informação inerentes à temática. Na seção 3.2 são descritas as políticas públicas de certificação digital adotadas no Brasil que proporcionam o amparo legal para sua consolidação. Por fim, a seção 3.3 traz dois estudos de caso sobre aplicações de certificação digital desenvolvidas no Recife. A Nota Fiscal Eletrônica da Secretaria da Fazenda de Pernambuco e o Programa Minha Certidão cujo Sistema de Registro Civil foi desenvolvido pela Agência Estadual de Tecnologia da Informação do Estado de Pernambuco.

3.1 O CONCEITO DE 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. Para tanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade, integridade e não repúdio às informações eletrônicas.

Segundo MacNeil *apud* Rondinelli (2002, p. 66),

> ... 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.

A certificação digital é a tecnologia que provê estes mecanismos. No cerne da certificação digital está o certificado digital, um documento eletrônico assinado digitalmente por uma terceira parte confiável, 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 8 *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 *ISSO/International Electrotechnical Commission* (IEC), segundo Adams e Just (2004) o padrão X.509 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, onde se deu efetivamente o início da *Public Key Infrastructure* (PKI) (apesar de que a sigla ainda não havia sido inventada). Atualmente encontra-se na terceira versão (v3), lançada em 1996, com a possibilidade de usar campos de extensão.

A seguir seguem a Figura 1 que ilustra o formato de certificado X.509 v3 e o Quadro 3 que descreve os campos do certificado.

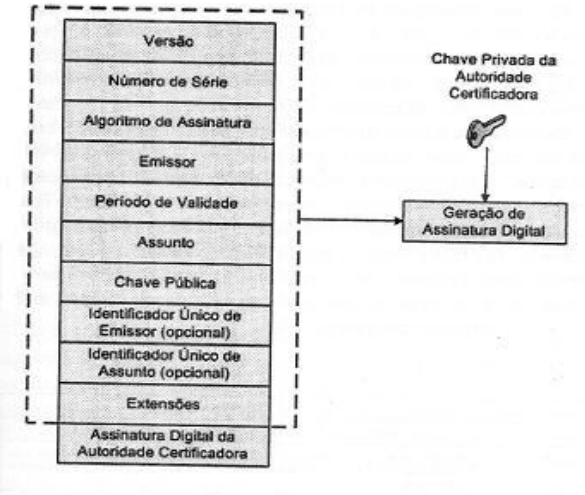

Fig. 1 – Certificado Digital no Padrão X.509 v3. Fonte: SILVA *et al* (2008).

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 de 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 reuso de um emissor com o tempo.
Identificador Único de Assunto (opcional)	Campo opcional para permitir o reuso de um assunto com o tempo.
Extensões (opcional)	Campos complementares com informações adicionais personalizadas.

Quadro 3 – Descrição dos campos de um certificado no formato X.509 v3. Fonte: SILVA *et al* (2008).

Para implementar as funcionalidades da certificação digital, é necessário planejar cuidadosamente uma infraestrutura para gerenciar os certificados digitais. Uma infraestrutura de chave pública, *Public Key Infrastructure* (PKI) em inglês, é uma base sobre a qual outros aplicativos, componentes de segurança do sistema e de rede são construídos. Uma PKI é um componente essencial de uma estratégia global de segurança que devem 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) faz 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 toda a empresa de rede. Uma típica ICP de empresa engloba a emissão de certificados digitais para usuários individuais e servidores, usuário final de *software* de inscrição, integração com diretórios certificados, ferramentas de gestão, renovação e revogação de certificados, bem como serviços de apoio. A infraestrutura de chave pública é baseada na tecnologia de criptografia de chave pública. Criptografia de chave pública é a tecnologia por trás das modernas técnicas de assinatura digital. Ela tem características únicas que a tornam de valor inestimável, como base para as funções de segurança em sistemas distribuídos.

Neste contexto, para melhor compreender a certificação digital é necessário discutir conceitos relevantes que fazem parte desta temática, tais como, criptografia[18] 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 no

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

que tangem a autenticidade, a confidencialidade, a integridade e o não-repúdio das informações eletrônicas.

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.

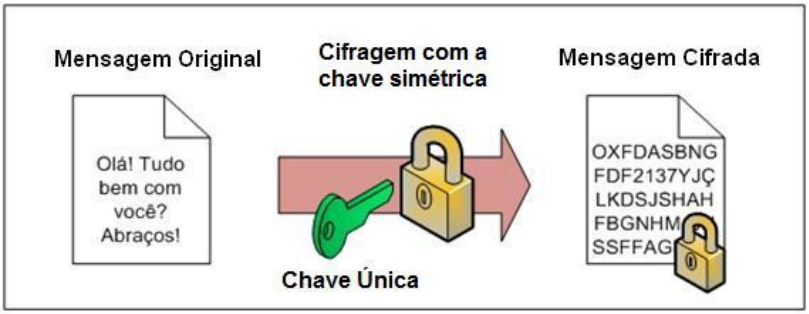

Figura 2 – Criptografia Simétrica: cifragem

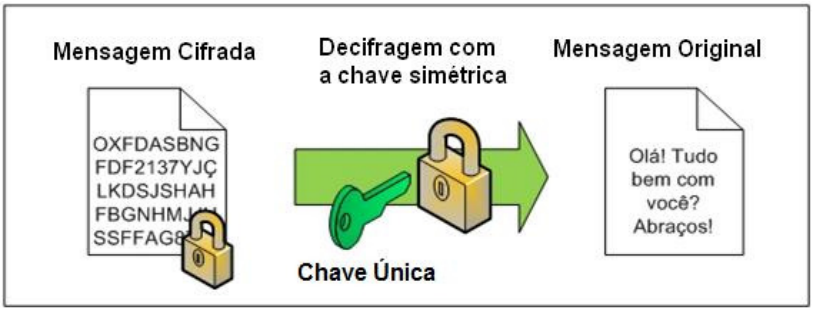

Figura 3 – Criptografia Simétrica: decifragem

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.

Para auferir maior segurança na utilização de chaves, é utilizada a criptografia assimétrica que operam com duas chaves distintas: chave privada e chave pública. Essas chaves são geradas simultaneamente e são relacionadas 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.

Abaixo segue esquema da cifragem (Fig. 4) e decifragem (Fig. 5) com chaves assimétricas:

Figura 4 - Criptografia assimétrica: cifragem com a chave pública do destinatário.

Figura 5 - Criptografia assimétrica: decifragem com a chave privada do destinatário.

Segundo Maia e Pagliusi (2011), a grande vantagem deste sistema é permitir que qualquer um possa enviar uma

mensagem secreta, apenas utilizando a chave pública 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 assimétrica e difere da mesma 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 sua assinatura utilizando a chave pública do remetente, garantindo assim sua **autenticidade**.

Com isso, o uso de assinaturas digitais baseadas em criptografia assimétrica oferece a possibilidade tecnológica de nivelar os documentos eletrônicos ao mesmo *status* de documentos em suportes tradicionais, como o papel, no que tange a sua autenticidade, integridade e sigilo. O número de documentos eletrônicos, portanto, que podem ser alçados ao patamar de documento com valor arquivístico tende a crescer ao longo do tempo. Isto deve ocorrer, na medida em que, além dos fatores técnicos e tecnológicos, estes 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 observação social pode ser vista por intermédio dos projetos (Programa Minha Certidão e Nota Fiscal Eletrônica) analisados neste trabalho, que se utilizam da certificação digital.

Voltando a discussão sobre os conceitos, a **integridade** é conquistada por meio da função *hashing*[19](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

[19]A tradução para *hash* é misturar, confundir. Funções criptográficas *hash* são usadas em vários contextos, por exemplo, para computar um resumo de mensagem. As funções "*hash*" geram uma saída de comprimento fixo a partir de um documento de entrada de qualquer tamanho. Este documento de saída fixo é o resumo do documento. (SILVA *et al*, 2008 p. 10)

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 4, 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[20], que funcionam como verdadeiros cartórios digitais.

[20] Uma autoridade certificadora (AC) é uma organização confiável, que aceita aplicações certificadas de certa entidade, autentica aplicações, emite certificados e mantêm atualizadas informações sobre os estados dos certificados (SILVA et al, 2008, p.30).

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

Quadro 4 – Característica de Segurança X Mecanismo de Segurança

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.

> A base de uma ICP consiste em políticas de segurança, operacionais, serviços e protocolos de interoperabilidade e apoio à utilização de chave pública criptografia para a gestão de chaves e certificados. A geração, distribuição e gestão de chaves públicas e certificados associados normalmente ocorre através do uso de Autoridades Certificadoras (ACs), Autoridades de Registro[21] (ARs), e serviços de diretório, que pode ser usado para estabelecer uma hierarquia ou cadeia de confiança. Autoridade Certificadora, Autoridade de

[21] Autoridade de Registro (AR) - O objetivo principal de uma AR é verificar a identidade de uma entidade final (pessoa física ou jurídica) e determinar se uma entidade final tem direito a ter um certificado de chave pública. (WEISE, 2001)

> Registro, e serviços de diretório permitem a implementação dos certificados digitais que podem ser usados para identificar diferentes entidades. A ICP permite o estabelecimento de uma hierarquia de confiança. Este é um dos principais princípios de uma ICP. O conceito de confiança, em relação a uma ICP, pode ser explicado pelo papel da AC. No ambiente da Internet, entidades desconhecidas uma das outras não tem confiança suficiente estabelecida entre elas para realizar negócios, contratos, formas jurídicas, ou outras transações. A implementação de uma ICP usando uma AC fornece esta confiança. Entidades que são desconhecidas entre si, cada uma individualmente estabelece uma relação de confiança com uma AC. A AC realiza algum nível de autenticação de uma entidade, de acordo com suas regras estabelecidas como observou em sua Declaração de Práticas de Certificação[22] (DPC). O Certificado digital é assinado pela AC e, portanto, garante a identidade dos indivíduos. Indivíduos desconhecidos podem agora utilizar os seus certificados para estabelecer a confiança entre eles porque a confiança da AC foi estabelecida. E a assinatura da AC dos certificados atesta esse fato. Um dos grandes benefícios de uma ICP é o estabelecimento de uma hierarquia de confiança. (WEISE, 2001)

---

[22] Declaração de Prática de Certificação - os detalhes de uma declaração política deve ser publicado em uma Declaração de Práticas de Certificado (DPC). A DPC é uma declaração das práticas que emprega uma AC em emissão de certificados de chave pública. O documento enumera as DPC processuais e práticas operacionais de uma ICP. A DPC deve detalhar todos os processos dentro do ciclo de vida de um certificado de chave pública, incluindo a sua gestão de emissão, geração, armazenamento, distribuição e revogação. O objetivo da DPC é incutir confiança na ICP de tal forma que a comunidade de usuários em geral terão confiança suficiente para participar. (WEISE, 2001)

Resumidamente, o usuário faz seu credenciamento junto a uma Autoridade Certificadora (AC) a fim de registrar o seu certificado digital e poder 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 para sua proteção, tais 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 1 ano até 4 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) comenta que depois de terminado o período de validade, o certificado se torna inválido. Porém, 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 Ciência da Informação na aplicação dessa tecnologia. Segundo Bodê (2006) o uso de assinaturas digitais, baseadas em chaves públicas e ICP`s confiáveis com respaldo legal pode agregar ainda mais valor e aplicabilidade aos documentos eletrônicos, cujas consequencias 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 eletrônicos, a presença nas organizações de documentos eletrônicos autênticos e com valor legal, aumenta ainda mais a carga de responsabilidade para sua correta administração.

A perspectiva em Ciência da Informação deste trabalho se concentra no modo como os projetos, que serão analisados mais a frente, lidam com a produção, tramitação e preservação desses documentos assinados digitalmente, principalmente quanto:

- Conformidade dos certificados com a Infraestrutura de Chaves Públicas do 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 leitura do conteúdo, ou seja, da informação;

- Procedimentos adotados para emissão de certificados e verificação da assinatura digital - relaciona-se a autenticidade, integridade, confidencialidade e não-repúdio;
- Local de armazenamento do documento certificado digitalmente - relaciona-se a preservação do *hardware*;
- 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 - relaciona-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.

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

Na seção a seguir será discutida como é estruturada a política de certificação digital da Infraestrutura de Chaves Públicas do Brasil que é dotada de respaldo legal.

3.2 POLÍTICAS PÚBLICAS DE CERTIFICAÇÃO DIGITAL

No Brasil, a Medida Provisória Nº 2.200-2, de 24 de agosto de 2001 institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a confidencialidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. A Medida Provisória (MD) estabelece que a ICP-Brasil será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz (AC Raiz), pelas Autoridades Certificadoras (AC) e pelas Autoridades de Registro (AR). O que pode ser visualizado na figura a seguir:

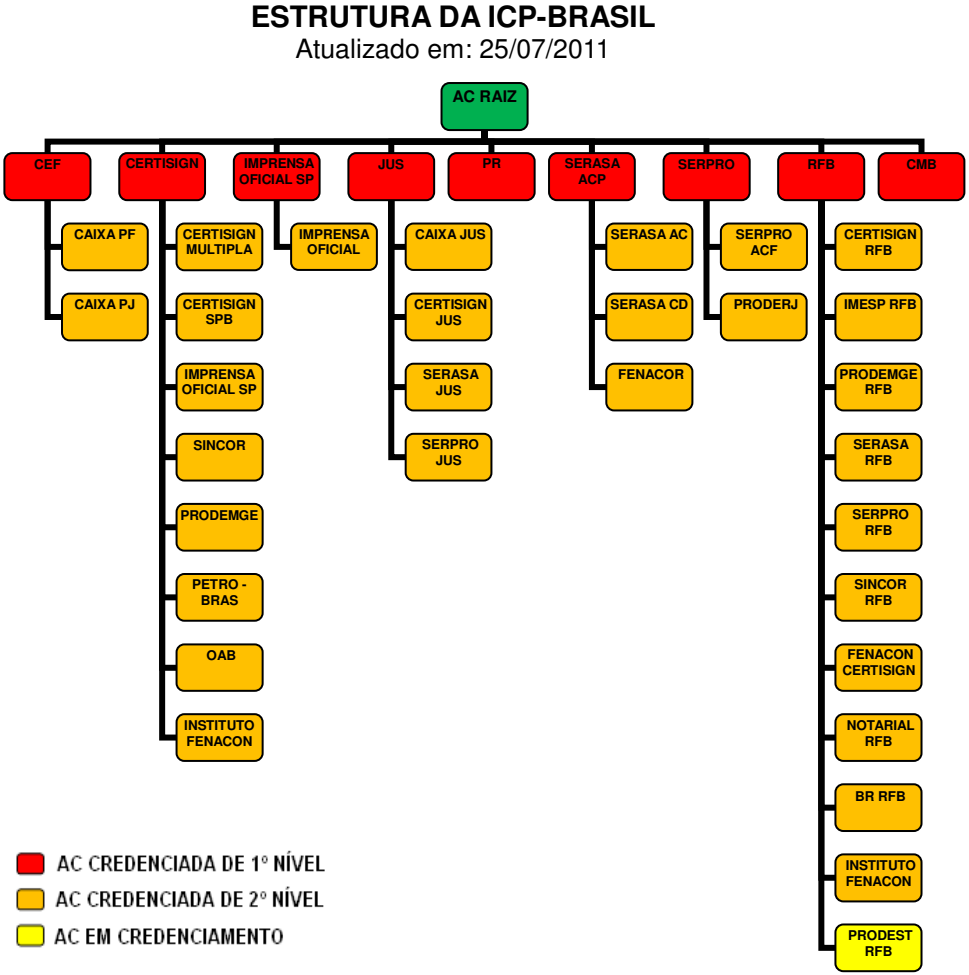

Fig. 6 - Estrutura Resumida com as Autoridades Certificadoras de 1º Nível e de 2º Nível da ICP-Brasil Fonte: Instituto Nacional de Tecnologia da Informação, 2011.

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 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;
- Casa Civil da Presidência da República; e
- Gabinete de Segurança Institucional da Presidência da República.

O Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – CG ICP-Brasil, instituído pela MD 2.200-2, e regulamentado pelo Decreto nº. 6.605, de 14 de outubro de 2008, exerce a função de autoridade gestora de políticas da referida Infraestrutura, vinculado à Casa Civil da Presidência da República. Ele tem por finalidade atuar na formulação e controle da execução das políticas públicas relacionadas à Infraestrutura de Chaves Públicas Brasileira - 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.

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. Compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subseqüente 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), entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Com relação às Autoridades de Registro (AR), entidades operacionalmente vinculadas à 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 públicos e as pessoas jurídicas de direito privado.

3.3 APLICAÇÕES DE CERTIFICAÇÃO DIGITAL NO RECIFE

No Brasil, para se ter uma idéia, o número de certificados digitais emitidos aumentou 50% em apenas sete meses. Em agosto de 2009, foram emitidos 45.085 certificados. Já em março de 2010, o número atingiu 105.659 (ITI, 2010 p. 6).

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)

Além da Receita Federal e o Poder Judiciário os certificados digitais estão sendo utilizados em várias aplicações (ITI, 2009), tais como:

a) Sistema de Pagamentos Brasileiro (SPB);
b) Automatização da prestação de informações fiscais à Receita Federal do Brasil;
c) Nota fiscal eletrônica;
d) Assinatura de documentos digitais;
e) Informatização do Poder Judiciário;
f) Informatização de Serviços Cartoriais;
g) Informatização de processos para a abertura de empresas;
h) Informatização de prontuários médico-odontológicos;

i) Programas do Governo, como PROUNI;

j) Autenticação dos servidores para ao acesso aos sistemas de diferentes órgãos federais, tais como da Receita Federal do Brasil;

k) Automatização de procedimentos que exigem autorização de despesas, usando assinatura digital, como ocorre no Sistema de Controle de Diárias e Passagens do Governo Federal;

l) Compras governamentais por pregão eletrônico e Compras-net.

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 que seguem abaixo.

3.3.1 O 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. 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, no Manual de Integração do Contribuinte (2009, p.10) 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 sobre 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 (são utilizadas, em regra, para documentar transações comerciais com mercadorias entre pessoas jurídicas), e está sendo emitida, apenas, por grandes contribuintes desde abril de 2008. Esses contribuintes são obrigados pelo Protocolo ICMS 68/2008.

No Guia Básico[23] para o contribuinte iniciar o processo de emissão da NF-e é descrito o processo e as fases de emissão de Nota Fiscal Eletrônica para os contribuintes de ICMS estabelecidos no Estado de Pernambuco.

---

[23] Disponível em: http://www.sefaz.pe.gov.br/sefaz2/flexpub/versao1/filesdirectory/systems4604.pdf. Acesso em: 05 abr. 2010

O primeiro passo é o contribuinte adquirir junto a uma AC o seu certificado digital, logo, deve realizar o seu credenciamento no *site* da SEFAZ-PE (www.sefaz.pe.gov.br), acessando o menu ARE VIRTUAL para efetuar o *login*, informando o CPF e o certificado digital do responsável junto à SEFAZ –PE. Para então, clicar em Nota Fiscal Eletrônica, Credenciamento de Contribuinte e finalmente Solicitação de Credenciamento. Ver (Fig.7)

Figura 7: Credenciamento de Contribuinte. Fonte: Guia Básico da SEFAZ-PE

O credenciamento é realizado em duas etapas. Num primeiro momento o contribuinte irá solicitar credenciamento

em ambiente de homologação, para então, emitir no mínimo 10 NF-e em ambiente de testes. Após isso, poderá solicitar credenciamento em ambiente de produção, devendo realizar 10 testes e não havendo nenhum outro impedimento no cadastro do contribuinte, será concedido o Credenciamento em Ambiente de Produção da NF-e no prazo máximo de 24h após a data da solicitação.

Então, o contribuinte já pode fazer gratuitamente o *download* dos *softwares* do Ministério da Fazenda, disponibilizados no portal da NF-e (http://www.nfe.fazenda.gov.br/portal/principal.aspx), para emitir, assinar e visualizar as NF-e.

Para tanto deve dispor de uma infraestrutura tecnológica mínima composta por:

- **Requisitos de Sistema**

Processador: Pentium III ou AMD K6 450 *Megahertz* ou superior

Memória RAM: 256 *Megabytes* ou superior (512 *Megabytes* recomendado)

Espaço em disco: 98 *Megabytes* (Java - JRE 6) + 30 *Megabytes* (Software Emissor NF-e)

- **Sistemas Operacionais**

Windows 2000 (SP4+), Windows XP (SP1 SP2), Vista, Windows 2003

Red Hat Linux, SUSE Linux, JDS

Solaris SPARC, Solaris x86

- **Impressora**

A impressora recomendada é a impressora a laser (utilizada para imprimir o DANFE que será explicado abaixo).

De maneira simplificada, a empresa emissora de NF-e gerará um arquivo eletrônico contendo as informações fiscais da operação comercial, o qual deverá ser assinado digitalmente, de maneira a garantir a integridade dos dados e a autoria do emissor. Este arquivo eletrônico, que corresponderá à Nota Fiscal Eletrônica (NF-e), será então transmitido, via Internet, para a SEFAZ-PE, que fará uma pré-validação do arquivo e devolverá uma Autorização de Uso, sem a qual não poderá haver o trânsito da mercadoria.

Após o recebimento da NF-e, a SEFAZ-PE disponibiliza a consulta, através do seu *site*, para o destinatário e outros legítimos interessados, que detenham a chave de acesso do documento eletrônico.

Este mesmo arquivo da NF-e será ainda transmitido através da Secretaria de Fazenda Estadual para:

- A Receita Federal, que será repositório nacional de todas as NF-e emitidas;
- No caso de uma operação interestadual, a Secretaria de Fazenda Estadual de destino da operação; e,
- Quando aplicável, os Órgãos e Entidades da Administração Pública Federal Direta e Indireta que tenham atribuição legal de regulação, normatização, controle e fiscalização, tais como a Superintendência da Zona Franca de Manaus (SUFRAMA), por exemplo.

Para acompanhar o trânsito da mercadoria será impressa uma representação gráfica simplificada da Nota Fiscal Eletrônica, intitulada DANFE (Documento Auxiliar da

Nota Fiscal Eletrônica), geralmente em papel comum, em única via. O DANFE conterá impressos, em destaque, a chave de acesso e o código de barras linear tomando-se por referência o padrão CODE-128C, para facilitar e agilizar a consulta da NF-e na Internet e a respectiva confirmação de informações pelas unidades fiscais e contribuintes destinatários. A legislação poderá prever casos em que seja permitida a impressão de mais de uma via do DANFE, como a contingência utilizando formulários de segurança, por exemplo.

O DANFE não é nota fiscal, nem a substitui, servindo apenas como instrumento auxiliar para consulta da NF-e, pois contém a chave de acesso da NF-e, que permite ao detentor desse documento confirmar, através da página da Secretaria de Fazenda Estadual, ou da Receita Federal do Brasil, a efetiva existência de uma NF-e que tenha tido seu uso regularmente autorizado.

Abaixo, segue um esquema que ilustra todo o processo descrito.

Figura 8 – Esquema para a emissão de NF-e. Fonte: SOLLUTA, disponível em: <http://www.solutta.com/solucao.asp?id=11>. Acesso em 28 jun 2011.

Com isso a SEFAZ-PE busca a substituição da sistemática atual de emissão do documento fiscal em papel que atualmente acoberta as operações com mercadorias entre empresas (modelos 1 e 1A), almejando os seguintes benefícios:

1) Benefícios para o Contribuinte Vendedor (Emissor da NF-e)

- Redução de custos de impressão;

- Redução de custos de aquisição de papel;

- Redução de custos de envio do documento fiscal;

- Redução de custos de armazenagem de documentos fiscais;

- Simplificação de obrigações assessórias, como dispensa de AIDF;

- Redução de tempo de parada de caminhões em Postos Fiscais de Fronteira;

- Incentivo a uso de relacionamentos eletrônicos com clientes (B2B).

2) Benefícios para o Contribuinte Comprador (Receptor da NF-e)

-Eliminação de digitação de notas fiscais na recepção de mercadorias;

-Planejamento de logística de entrega pela recepção antecipada da informação da NF-e;

-Redução de erros de escrituração devido a erros de digitação de notas fiscais;

-Incentivo a uso de relacionamentos eletrônicos com fornecedores (B2B).

3) Benefícios para a Sociedade

- Redução do consumo de papel;

-Incentivo ao comércio eletrônico e ao uso de novas tecnologias;

-Padronização dos relacionamentos eletrônicos entre empresas;

- Surgimento de oportunidades de negócios e empregos na prestação de serviços ligados a NF-e, tais como, pessoal contratado para trabalhar em Autoridades Certificadoras e

Registradoras, bem como a comercialização de certificados digitais.

4) Benefícios para as Administrações Tributárias

- Aumento na confiabilidade da Nota Fiscal;

- Melhoria no processo de controle fiscal, possibilitando um melhor intercâmbio e compartilhamento de informações entre os fiscos;

- Redução de custos no processo de controle das notas fiscais capturadas pela fiscalização de mercadorias em trânsito;

- Diminuição da sonegação e aumento da arrecadação;

- Suporte aos projetos de escrituração eletrônica contábil e fiscal da Secretaria da Receita Federal do Brasil (Sistema Público de Escrituração Digital – SPED).

No capítulo 5 serão abordados os demais detalhes sobre o projeto.

3.3.2 O Programa Minha Certidão

A Corregedoria-Geral da Justiça de Pernambuco (CGJ), 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 lançou, em 2008, o Programa Minha Certidão. O objetivo é erradicar o sub-registro, facilitando o recebimento da certidão de nascimento, que será emitida na maternidade, no dia do nascimento da criança.

Todo o procedimento 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 (fonte 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 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 (SUS) 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)

No 9º Forúm de Certificação Digital (CERTFÓRUM), realizado em Recife no dia 14 de abril de 2011, a ATI na oportunidade representada por Carolina Freitas e Verlaynne Rocha, apresentou as suas iniciativas em certificação digital

dentre as quais o Programa Minha Certidão, onde foi esclarecido como funciona o processo de emissão das certidões de nascimento.

As palestrantes explicaram que o fluxo é iniciado na Maternidade onde o Responsável pelo Posto de Atendimento de Registro Civil solicitará documentos necessários a emissão da Certidão de Nascimento ao Declarante. Ver (Fig. 9)

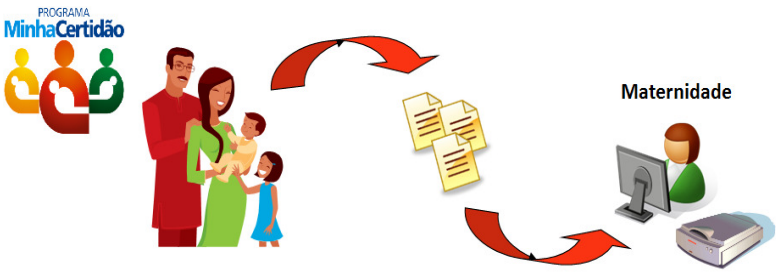

Figura 9 – Apresentação de Documentação. Fonte: FREITAS e ROCHA (2011)

Após o cadastro dos dados apresentados na Declaração de Nascido Vivo (DNV), os dados dos envolvidos (pai, mãe, declarante, representante e testemunhas) que constarão na Certidão de Nascimento, são registrados e seus documentos são digitalizados, assinados digitalmente e anexados, compondo assim as informações necessárias ao pré-registro civil. Ver (Fig. 10)

Figura 10 – Digitalização da Documentação. Fonte: FREITAS e ROCHA (2011)

Após o registro das informações no sistema, o Responsável pelo Posto de Atendimento, deverá emitir a Minuta do Termo de Nascimento e entregar ao Declarante, para conferência das informações registradas. Ver (Fig.11)

Figura 11 – Emissão da Minuta do Termo de Nascimento. FREITAS e ROCHA (2011)

Já no Cartório, após a submissão dos documentos, o Oficial poderá visualizar o novo registro em sua Caixa de

Entrada, podendo selecioná-lo para verificação da documentação (Ver Fig. 12).

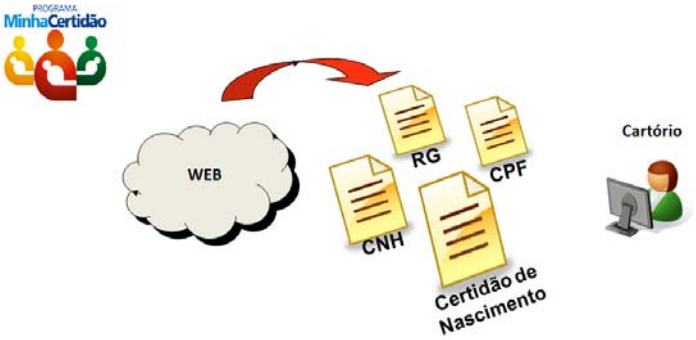

Figura 12 – Verificação da Documentação. Fonte: FREITAS e ROCHA (2011)

Com todos os documentos verificados, o Oficial conclui o processo assinando digitalmente a Certidão de Nascimento gerada pelo SERC que fica disponível para a Maternidade, já com número da lavratura da folha, livro e termo (nº matrícula) (Ver Fig. 13).

Figura 13 – Assinatura Digital da Certidão de Nascimento. Fonte: FREITAS e ROCHA (2011)

O funcionário da maternidade de posse da Certidão de Nascimento liberada pelo Cartório imprime o Termo de Nascimento, para ser assinado, e a Certidão de Nascimento para ser entregue ao Declarante. Ver (Fig. 14)

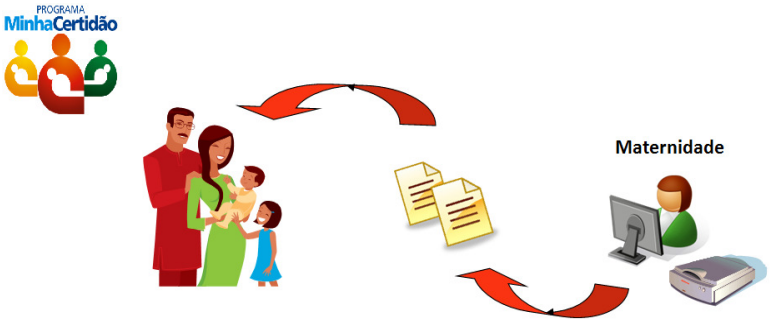

Figura 14 – Impressão do Termo de Nascimento e da Certidão de Nascimento. Fonte: FREITAS e ROCHA (2011)

Ainda, de acordo com Freitas e Rocha (2011) o SERC é composto pelos seguintes recursos (Fig. 15):

- Data Center (Servidores de Aplicação, Dados e de Serviços e rotinas de *backup*)
- Serviço de Internet
- Equipamentos (Estações de Trabalho e multifuncionais)
- Certificados Digitais A-3[24] (e-CPF – *Smart Card* ou *Token*)
- Software de aplicação (SERC)
- Software de WebService (Para o servidor de serviço)
- Software Assinador (para as estações de trabalho)

[24] Na ICP-Brasil, estão previstos 8 tipos de certificados digitais destinados a usuários finais, sendo que 4 estão relacionados com assinatura digital (A1, A2, A3 e A4) e quatro com sigilo (S1, S2, S3 e S4). Os certificados do tipo A3 utilizam como mídia de armazenamento e portabilidade um hardware criptográfico, que pode ser um cartão inteligente (*smart card*) ou um *token* USB. Nos chips desses dispositivos são armazenadas as informações referentes ao certificado do usuário. O acesso a essas informações é feito por meio de uma senha pessoal, determinada pelo titular. Disponível em: < http://www.bb.com.br/portalbb/page251,105,5567,0,0,1,1.bb?codigoNoticia=2014&codigoMenu=567&codigoRet=1640>. Acesso em: 05 jul. 2011.

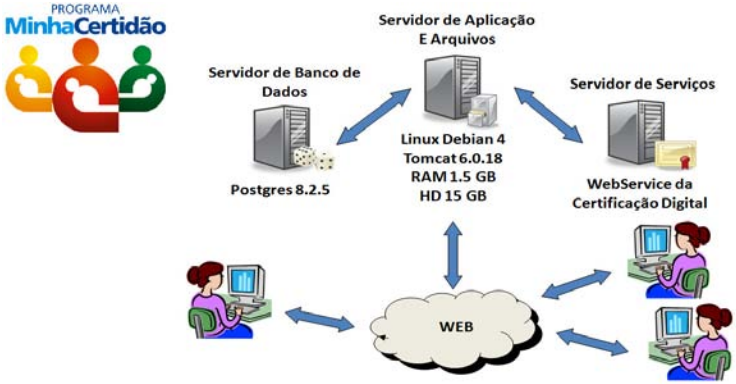

Figura 15 – Infraestrutura SERC. Fonte FREITAS e ROCHA (2011)

Vale ressaltar que o certificado digital é utilizado em dois momentos:

- Na assinatura dos documentos - Assinatura dos documentos escaneados dos Pais, do Declarante, das Testemunhas e do Representante, esses documentos podem ser: RG, CPF, Certidão de Nascimento, Certidão de Casamento, Habilitação e outros.
- Na assinatura do Registro de Nascimento - Assinatura do Registro de Nascimento feita pelos oficiais do Cartório.

No que diz respeito ao local de armazenamento do Registro de Nascimento Digital, o mesmo será armazenado no Data Center da ATI em formato de BMP. Segundo Enildo Chagas, entrevistado da ATI que prestou esclarecimentos sobre o projeto, o BMP foi escolhido devido ao seu formato

ser lido por vários programas e já estar consolidado, além de ser um formato público e não proprietário, e que provavelmente conseguirá ser lido no futuro. No que se refere ao tamanho, o arquivo é pequeno (tamanho médio de 100 KB).

Utilizando esta metodologia, o SERC está contribuindo para a rápida emissão de certidões de nascimento, corroborando para a erradicação dos sub-registros. Dessa forma, ganhou destaque nacional e hoje é utilizado por outros estados da federação, tais como Mato Grosso e Acre. E está disponível no Portal do Software Público (www.softwarepublico.gov.br) para que outros estados brasileiros possam requisitar a sua implantação.

No ano de 2009, o SERC ganhou o Prêmio e-GOV na categoria e-Serviços Públicos. Esse prêmio é promovido pelo governo federal para reconhecer os melhores trabalhos desenvolvidos em Tecnologia da Informação e Comunicação no Brasil.

Portanto, verifica-se a relevância social que o projeto representa para a população do Estado de Pernambuco e para o resto do país. Uma vez que o projeto agiliza o processo de emissão de certidões de nascimento, evitando o deslocamento dos declarantes aos cartórios de registro civil. Para tanto, o projeto será melhor detalhado no capítulo 5.

4 PROCEDIMENTOS METODOLÓGICOS

O presente trabalho tem como objetivo principal identificar e analisar aplicações e políticas públicas de certificação digital desenvolvidas na cidade do Recife, a fim de compreender essa tecnologia da informação e seu uso na gestão de documentos eletrônicos. Para tanto, traçou-se os seguintes objetivos específicos:

- Descrever o funcionamento dos programas e políticas públicas de certificação digital;
- Verificar a conformidade dos programas com a legislação federal;
- Descrever requisitos de segurança: autenticidade, confidencialidade e integridade; e
- Avaliar políticas de preservação digital.

Neste sentido, o trabalho é uma análise sob a ótica da Ciência da Informação e em especial da arquivística a respeito do problema em questão, haja vista que o objeto da Ciência da Informação são as informações, para ROBREDO (2003) a Ciência da Informação, no sentido mais amplo possível, significa o registro e transmissão do conhecimento, o armazenamento, processamento, análise, organização e recuperação da informação registrada, e os processos e técnicas relacionadas.

Para atingir os objetivos da trabalho, foi realizada a partir do ano de 2009 uma pesquisa de caráter exploratório. Conforme Gil (2009, p. 41),

> As pesquisas exploratórias têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de idéias ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos. Embora o planejamento da pesquisa exploratória seja bastante flexível, na maioria dos casos assume a forma de pesquisa bibliográfica ou de estudo de caso.

Dessa forma, a pesquisa bibliográfica e o estudo de caso foram os métodos utilizados para este trabalho. 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. Para adentrar no tema buscou-se no capítulo 2 debater os conceitos e características do documento digital, haja vista o documento digital ser objeto da aplicação de certificação digital. Esse capítulo é composto pela seção 2.1 Memória e Preservação Digital de Documentos que aborda a relação entre as duas e suas relevâncias, a seção 2.2 Normas e Políticas de Preservação Digital que faz referência à normas, políticas e estratégias de preservação digital em

âmbito nacional e internacional, e por fim, a seção 2.2 Segurança da Informação Digital que identifica as características e os principais mecanismos aplicados para a segurança da informação.

Após essa contextualização, partiu-se para a identificação e abordagem dos conceitos, tecnologias e políticas públicas de certificação digital, cujo resultado desta pesquisa bibliográfica pode ser conferido no capítulo 3 Certificação Digital e nas seções: 3.1 O Conceito de Certificação Digital e 3.2 Políticas Públicas de Certificação Digital. Já 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: Nota Fiscal Eletrônica – *site* da Secretaria da Fazenda do Estado de Pernambuco e Programa Minha Certidão – *site* da Agência Estadual de Tecnologia da Informação. Além disso, foi possível observar o projeto Nota Fiscal Eletrônica no 8º CERTFÓRUM etapa Recife, fórum de certificação digital realizado pelo Instituto Nacional de Tecnologia da Informação (ITI) no dia 20 de maio de 2010. Nessa oportunidade, o projeto foi apresentado pelo Arquiteto de Software Jonysberg Peixoto Quintino que também prestou esclarecimentos sobre o projeto neste trabalho. Já no 9º CERTFÓRUM etapa Recife, realizado no dia 14 de abril de 2011. Foi possível observar os esclarecimentos sobre o Sistema Estadual de Registro Civil (SERC) da Agência Estadual de Tecnologia da Informação (ATI) que viabiliza o Programa Minha Certidão, apresentado por Carolina Freitas e Verlaynne Rocha, que trabalham na Gerência de Normatização e Desenvolvimento da ATI. Essas informações estão textualizadas na seção 3.3 Aplicações de Certificação Digital no Recife, bem como nas subseções 3.3.1 O Projeto Nota Fiscal Eletrônica (NF-e) e 3.3.2 O Programa

Minha Certidão.

Já o estudo de caso, que é uma modalidade de pesquisa amplamente utilizada nas ciências biomédicas e sociais, e que consiste no estudo profundo e exaustivo de um ou poucos objetos, de maneira que permita seu amplo e detalhado conhecimento (GIL, 2009 p. 54), foi delimitado pela coleta de dados sobre cada projeto através de 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 entrevistas semi-estruturadas foram realizadas no ano de 2011 junto aos responsáveis pelas referidas aplicações de certificação digital com questionamentos sobre: 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, local de armazenamento do documento certificado digitalmente, legislação concernente, segurança da informação, preservação digital e resultados dos projetos. Os oito questionamentos formulados, que se encontram no APÊNDICE “A” nortearam a coleta de dados sobre cada projeto. Para tanto, foram assinados os Termos de Consentimento Livre e Esclarecido (APÊNDICE B) junto a Secretaria da Fazenda de Pernambuco e junto a Agência Estadual de Tecnologia da Informação de Pernambuco, a fim do consentimento necessário para a realização das entrevistas. Em um segundo momento foi necessária a aplicação de outro roteiro com questionamentos a respeito do gerenciamento eletrônico de documentos (APÊNDICE C) 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 para assim contribuir com o aprimoramento sobre o tema certificação digital que revoluciona os métodos de autenticação e transmissão de documentos. Os resultados e a análise dos estudos de caso podem ser observados no capítulo 5 Análise dos Estudos de Caso, subdivido em 5.1 Dados Obtidos e 5.2 Análise dos Dados.

5 ANÁLISE DOS ESTUDOS DE CASO

Neste capítulo, são descritos e analisados os dados obtidos sobre os projetos Nota Fiscal Eletrônica e Programa Minha Certidão.

5.1 DADOS OBTIDOS

De acordo com os objetivos deste trabalho foram elaborados os questionamentos (APÊNDICE A) 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.

Os questionamentos versam sobre os seguintes tópicos: conformidade com a ICP-Brasil, programas e formatos de computadores utilizados no processo de certificação digital, procedimentos adotados para a emissão de certificados e verificação da assinatura digital, local de armazenamento do documento certificado digitalmente, legislação concernente, segurança da informação, preservação digital e resultados dos projetos.

Assim sendo, no quadro abaixo seguem as respostas obtidas, descritas por cada tópico mencionado:

DESCRITORES	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	Os programas para emitir, assinar e visualizar são livres e podem ser obtidos no *site* do portal nacional da NF-e disponível em: <http://www.nfe.fazenda.gov.br>	O programa para emitir é o sistema web SERC[25], para assinar é o BRY Sgner[26] e para visualizar é por intermédio do 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 NFe , 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

[25] URL: https://www.programaminhacertidao.pe.gov.br/serc/
[26] URL: http://signer.bry.com.br/pg1_brysigner.html.

		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 8 maternidades e 19 cartórios, bem como já foram emitidas mais de dez mil certidões de nascimento.

Quadro 5 – Aplicações de Certificação Digital no Recife

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 5. Principalmente se os referidos documentos estão sujeitos a tabelas de temporalidade[27], bem como se após o prazo de guarda estes ainda serão conservados ou não por caráter histórico.

[27] Instrumento de destinação, aprovado por autoridade competente, que determina prazos e condições de guarda tendo em vista a transferência, recolhimento, descarte ou eliminação de documentos. (ARQUIVO NACIONAL, 2005)

Neste sentido, foi necessária a submissão de outro roteiro de entrevista (APÊNDICE C) com perguntas mais pontuais sobre esses aspectos da gestão documental, obtendo-se os seguintes dados:

DESCRITORES	**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.

Quadro 6 – Gestão Documental

Com isso, é possível observar o panorama geral de cada projeto e a metodologia adotada por cada um.

5.2 ANÁLISE DOS DADOS

Diante das repostas 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 diferenças.

Enquanto a NF-e permanece em meio digital, a Certidão de Nascimento assinada eletronicamente migra para o suporte em papel, utilizando o processo de certificação digital apenas para a elaboração do documento que será impresso.

No que se refere a formatos e *softwares*, também são distintos. Enquanto a SEFAZ-PE utiliza a NF-e em XML[28] e

[28] **XML**, do inglês eXtensible Markup Language, é uma linguagem de marcação recomendada pela W3C para a criação de documentos com dados organizados hierarquicamente, tais como textos, banco de dados ou desenhos vetoriais. A linguagem XML é classificada como extensível porque permite definir os elementos de marcação. Linguagem de marcação é um agregado de códigos que podem ser aplicados a dados ou textos para serem lidos por computadores ou pessoas. O XML traz uma sintaxe básica que pode ser utilizada para compartilhar informações entre diferentes computadores e aplicações. Quando combinado com outros padrões, torna possível definir o conteúdo de um documento separadamente de seu formato, tornando simples para reutilizar o código em outras aplicações para diferentes propósitos. Portanto, uma das suas principais características é sua portabilidade, pois, por exemplo, um banco de dados pode escrever um arquivo XML para que outro banco consiga lê-lo. Fonte: *site* TECNOMUNDO. Disponível em: <http://www.tecmundo.com.br/1762-o-que-e-xml-.htm>. Acesso em: 06 jul. 2011.

dispõe dos *softwares* livres do Ministério da Fazenda para assinar e visualizar o documento, a ATI utiliza as certidões de nascimento em BMP[29] 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, realizadas nos formulários web utilizados no SERC.

O embasamento legal da SEFAZ-PE está fundamentado no Protocolo ICMS 10 de 18 de abril de 2007, a 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, a 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). O referido decreto encontra-se em anexo (ANEXO A), pois nele está especificada toda a sistemática da NF-e em Pernambuco.

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

---

[29] O formato Bitmap Image File (**BMP)** é um dos formatos mais simples, desenvolvido conjuntamente pela Microsoft e pela IBM, o que explica que seja particularmente usado nas plataformas Windows e OS/2. Um arquivo BMP é um arquivo bitmap, ou seja, um arquivo de imagem gráfico que armazena os pixéis sob a forma de quadro de pontos e gerindo as cores, quer em cor verdadeira, quer graças a uma paleta indexada. O formato BMP foi estudado de maneira a obter um bitmap independente do periférico de afixação (DIB, Device independent bitmap). Fonte: *site* Kioskea.net. Disponível em: <http://pt.kioskea.net/contents/video/format-bmp.php3>. Acesso em: 06 jul. 2011.

- 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.

Para tanto, e para melhor compreensão do programa, é relevante visualizar o Provimento nº 13, de 3 de agosto de 2010 do CNJ (ANEXO B), que sintetiza muito bem a sistemática de emissão da Certidão de Nascimento. Por oportuno, é relevante mencionar que o SERC foi modelo dessa sistemática, haja vista sua implantação de dois anos antes.

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. No tocante 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)[30], que tem o objetivo de padronizar e estabelecer requisitos mínimos, a fim de proporcionar condições que assegurem a integridade, a confidencialidade, a disponibilidade, bem como a legalidade da informação no âmbito do ambiente computacional da ATI.

No que concerne a preservação da informação digital. 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, os quais podem ser observadas na palestra proferida por Freitas e Rocha (2011) que discrimina formas de *backup*:

- *Backup* do Servidor de Dados: No Servidor de Dados 2 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.

[30] Disponível em: http://www2.ati.pe.gov.br/c/document_library/get_file?p_l_id=77706&folderId=77701&name=DLFE-24954.pdf Acesso em: 06 jul. 2011.

- *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.

Os resultados de cada projeto são bem significativos para o sistema financeiro e social do Estado de Pernambuco.

A NF-e apresenta os seguintes 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).

Já o Programa Minha Certidão apresenta os seguintes resultados:

- O projeto está implantado em 8 maternidades e 19 cartórios; e
- Foram emitidas mais de dez mil certidões de nascimento.

Com isso a NF-e contribui para a redução dos gastos com impressão de notas fiscais e a redução da sonegação de impostos. Enquanto 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, integridade e confidencialidade, proporcionadas pela utilização de certificados digitais da ICP-Brasil cujo amparo

legal está contido na Medida Provisória nº 2.200-2, de 24 de agosto de 2001 que institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), para garantir a autenticidade, a confidencialidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

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, descrita no quadro 6, os dados revelam que, muito embora as instituições não apliquem uma tabela de temporalidade aos documentos eletrônicos, essas demonstram a preocupação de armazenar os documentos permanentemente. São adotadas rotinas de cópia de segurança pela ATI e migração e cópias de segurança pela SEFAZ-PE afim de salvaguardar a documentação. Ressalta-se aqui o primoroso senso de preservação de cada instituição pesquisada, mesmo que a responsabilidade legal para a guarda 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.

No entanto, fica evidente a necessidade de profissionais da Ciência da Informação para participar de projetos desse gênero, a fim de contribuir com soluções para o gerenciamento dos documentos eletrônicos desde sua produção, utilização, tramitação e destinação final, a fim de 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.

Para os profissionais da Ciência da Informação é relevante compreender esses processos de produção, tramitação, utilização e armazenamento de documentos digitais. Uma vez que, a correta gestão dos documentos eletrônicos é que permitirá a preservação da memória da sociedade, devidamente registrada nesse tipo de suporte.

Segundo Hollós (2010) a informação, hoje gerada em meio eletrônico, 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.

Tammaro e Salarelli (2008) complementam dizendo que:

> A preservação tem a finalidade de garantir o acesso à informação digital e aos pontos de acesso a ela (metadados). Assim como, é uma função crítica, e os obstáculos a superar não dizem respeito apenas à fragilidade do suporte e à 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 é relevante para o desenvolvimento de programas e políticas para a preservação da informação digital.

6 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 se apresenta para proporcionar tais características dos documentos digitais, este trabalho procurou abordar os conceitos e a política relacionada a ela, bem como descrever projetos que aplicam a referida tecnologia.

A utilização da certificação digital contribui para o crescente número de documentos armazenados em meio digital, demandando assim o desenvolvimento de políticas, normas e procedimentos para preservação da informação documentada em formato eletrônico, que são as fontes de memória coletiva e individual de uma sociedade.

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 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.

Neste contexto, ressalta-se o importante papel que a Ciência da Informação desempenha a partir dos seus estudos sobre gerenciamento e preservação de documentos digitais, onde tais estudos podem ser encontrados em literaturas da área e anais de congressos. Para a certificação digital que atribui maior credibilidade ao documento digital e permite que o mesmo permaneça nesse tipo de suporte, os estudos da Ciência da Informação são de grande relevância para soluções necessárias à preservação desses documentos por longos períodos.

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* são utilizados em todo o processo, bem como 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 os subsídios a fim de se refletir a melhor forma para organizar, tramitar,

utilizar, armazenar e preservar os documentos digitais assinados e certificados digitalmente.

Trabalhos futuros podem ainda explorar que outras estratégias de preservação 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.

7 REFERÊNCIAS

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

ALECRIM, Emerson. **Firewall**: conceitos e tipos. Disponível em <http://www.infowester.com/firewall.php>. Acesso em: 02 mai 2011.

ARELLANO, Miguel Ángel Márdero. **Preservação de Documentos Digitais**. Ci. Inf., Brasília, v. 33, n. 2, p. 15-27, 2004. Disponível em: <http://revista.ibict.br/index.php/ciinf/article/viewArticle/305>. Acesso em 15 ago 2010.

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

BARATIN, Mare; JACOB, Chistian (Org.). **O poder das bibliotecas**: a memória dos livros no Ocidente. 3 ed. Rio de Janeiro: Editora UFRJ, 2008. 352p.

BOBBIO, Norberto; MATTEUCCI, Nicola. **Dicionário de política**. v.2. 5.ed. São Paulo: Imprensa Oficial, 2004.

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/include/ getdoc. php?id=187&article=51>. Acesso em: 23 jul. 2011.

BORBA, Vildeane da Rocha. **Modelo orientador para construção de estratégias de Preservação digital**: o estudo

de caso no Banco de Teses e Dissertações da UFPE. 2009. 134 f. Dissertação (Mestrado em Ciência da Informação) – Programa de Pós-graduação em Ciência da Informação (PPGCI) do Centro de Ciências Sociais Aplicadas (CCSA) da Universidade Federal da Paraíba, João Pessoa. 2009. Disponível em: <http://dci2.ccsa.ufpb.br:8080/jspui/bitstream/123456789/165/1/Dissertacao_VILDEANE_PPGCI_UFPB.pdf>. Acesso em: 18 ago. 2010.

CAPURRO, R.; HJORLAND, B. O conceito de informação. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 12, n. 1, 2007. Disponível em: <http://www.eci.ufmg.br/pcionline/index.php/pci/article/viewFile/54/47>.

CARDOSO, A.M.P. **Retomando possibilidades conceituais**: uma contribuição à sistematização do campo da informação social. R.Esc. Biblioteconomia UFMG, Belo Horizonte, v.23, p.107 – 114, jul./dez.1994.

CARELLI, Ana; MONTEIRO, Silvana Drumond; PICKLER, Maria Elisa. **Representação e memória no ciberespaço**. Ci. Inf., Brasília, v. 35, n. 3, p. 115-123, set./dez. 2006. Disponível em < http://revista.ibict.br/pbcib/index.php/pbcib/article/view/579 > Acesso em 15 ago 2010.

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

CASSARES, Norma Cianflone. **Como Fazer Conservação Preventiva em Arquivos e Bibliotecas**. São Paulo: Arquivo do Estado e Imprensa Oficial, 2000.

CONARQ. **Carta para a Preservação do Patrimônio Arquivístico Digital Preservar para garantir o acesso.** Rio de Janeiro, 34ª reunião plenária, 06 jul. 2004. Disponível em: https://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm. Acesso em: 05 jul 2010.

e-ARQ Brasil: **Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos** / Câmara Técnica de Documentos Eletrônicos. 1.1. versão. - Rio de Janeiro : Arquivo Nacional, 2011. Disponível em: https://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm. Acesso em: 05 jan 2011.

FERREIRA, Miguel. **Introdução à preservação digital**: Conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006.

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, Luís Rodrigo de Oliveira. **O surgimento da Norma Nacional de Segurança de Informação [NBR ISO/IEC-1779:2001]**. Lockabit Segurança em Sistemas de Informação, 2004. Disponível em: <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=85>. Acesso em 03 jun 2010.

GONÇALVES, Rui. **Programa Minha Certidão chega ao Barão de Lucena**. Recife, Folha de Pernambuco Digital. Disponível em: < http://www2.folhape.com.br/index.php/saude/584534-programa-minha-certidao-chega-ao-barao-de-lucena->. Acesso em: 04 jul. 2011.

GUIMARÃES, José Augusto Chaves; NASCIMENTO, Lúcia Maria Barbosa do; FURLANETO NETO, Mario. **Aspectos Jurídicos e Diplomáticos dos Documentos Eletrônicos**. São Paulo: Associação de Arquivistas de São Paulo, 2005.

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.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **Revista Digital,** Brasília, ano 1, nº 1. 1º semestre 2009. Disponível em: <http://www.icpbrasil.gov.br/twiki/pub/Certificacao/CartilhasCd/Digital.pdf>. Acesso em: 25 ago. 2009.

_____. Brasil e Revolução 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.

_____. **O que é certificação digital**. Cartilha, ITI, Brasília, 2005. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>. Acesso em: 24 jul. 2010.

KESSEL**,** Zilda**: Memória e Memória coletiva**. Disponível em: www.memoriaeducaçao.hpg.ig.com.br. Acesso em 05 jul 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.

Disponível em: <http://www.csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>. Acesso em: 22 jul. 2011.

LE GOFF, J. **História e memória:** escrita e literatura. Campinas: Ed. Unicamp, 2003.

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.

MARCIANO, João Luiz; MARQUES, Mamede Lima. **O enfoque social da segurança da informação**. Ci. Inf., Brasília, v. 35, n. 3, p. 97, set./dez. 2006 Disponível em: <http://www.scielo.br/pdf/ci/v35n3/v35n3a09.pdf>. Acesso em 10 jul 2010.

MARTELETO, Regina Maria. **Educação e Informação**: A distribuição da informação na sociedade. Ver. TB. Rio de Janeiro, 1986, p. 46-60.

MENESES Ulpiano Bezerra de. **Os paradoxos da Memória** In MIRANDA Danilo Santos de Memória e Cultura: A importância na formação cultural humana. São Paulo: SESC, 2007.

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://www.tjpe.gov.br/noticias_ascomSY/ver_noticia.asp?id=5929&argumento=pern>. Acesso em: 04 jul. 2011.

NBR ISO/IEC 17799 – **Tecnologia da Informação:** Código de Prática para a Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas – ABNT, 2001/2005. Disponível para aquisição no site: <http://www.abnt.gov.br>. Acesso em 03 jun 2010.

PETUCO, Gelson. Data Warehouse. **Baguete Jornalismo Digital**, Porto Alegre, 05 jul. 2006. Seção de Artigos. Disponível em: <http://www.baguete.com.br/artigos/206/gelson-petuco/05/06/2006/data-warehouse>. Acesso em: 27 jul. 2011.

PINHEIRO, Patricia Peck. **Direito Digital**. 3 ed. rev. atual e ampl. São Paulo: Saraiva, 2009.

ROBREDO, Jaime. **Da Ciência da Informação revisitada aos sistemas humanos de nformação.** Brasília: Thesaurus; SSRR Informações, 2003.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos**: uma abordagem teórica da

diplomática arquivística contemporânea. Rio de Janeiro: Editora FGV, 2002.

SANTOS, Vanderlei Batista dos. **Gestão de documentos eletrônicos**: uma visão arquivística. 2ª Ed. Ver. Aum. Brasíli: ABARQ, 2005.

SECRETARIA DE FAZENDA DE PERNAMBUCO. **Guia Básico**. Disponível em: <http://www.sefaz.pe.gov.br/sefaz2/flexpub/versao1/filesdirectory/systems4604.pdf>. Acesso em: 05 abr. 2010.

SEMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. Rio de Janeiro: Elsevier, 2003. p.46.

SILVA, A. M. da. **A Informação**: da compreensão do fenómeno e construção do objecto científico. Porto, Afrontamento, 2006.

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.

TERRIBILI, Armando. O Business Intelligence pode ir além da área de negócios. **Baguete Jornalismo Digital**, Porto Alegre, 13 jul. 2009. Seção de Artigos. Disponível em: <http://www.baguete.com.br/artigos/137/armando-terribili-filho/13/07/2009/o-business-intelligence-pode-ir-alem-da-area-de-negoc>. Acesso em: 27 jul. 2011.

THOMAZ, Kátia P. **Gestão e preservação de documentos eletrônicos de Arquivo**: revisão de literatura – parte 2. Arquivística.net, Rio de Janeiro, v.2, n.1, p.114-131, jan./.jun. 2006. Disponível em: <http://www.arquivistica.net>. Acesso em: 05 jul 2010.

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.

ZAPATER, Marcio; SUZUKI, Rodrigo. Segurança da Informação: Um diferencial determinante na competitividade das corporações. **Promon Business & Technology Review**, 2005. Disponível em: <http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf.> Acesso em 03 jun 2010

APÊNDICE A – ROTEIRO DE ENTREVISTA

UNIVERSIDADE FEDERAL DE PERNAMBUCO
PROGRAMA DE PÓS-GRADUAÇÃO
EM CIÊNCIA DA INFORMAÇÃO
MESTRADO EM CIÊNCIA DA INFORMAÇÃO

Título da Dissertação: Aplicações de Certificação Digital no Recife: Perspectivas em Ciência da Informação.

ENTREVISTA

Questionamentos:

1) O processo de certificação digital utiliza-se de qual Autoridade Certificadora da ICP-Brasil?
2) Quais os programas de computador utilizados para o processo de certificação digital e quais são os formatos dos documentos?
3) Qual o procedimento utilizado para emitir o certificado digital e como se verifica a legitimidade da assinatura digital?

4) O documento permanece em meio eletrônico ou migra para o meio físico?
5) Qual o respaldo legal que garante a fé pública ao documento?
6) Com relação à segurança da informação, quais tecnologias e políticas são empregadas?
7) Quais as técnicas e políticas são empregadas para a preservação digital dos documentos?
8) Quais os resultados do Projeto e as perspectivas futuras?

APÊNDICE B – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

UNIVERSIDADE FEDERAL DE PERNAMBUCO
PROGRAMA DE PÓS-GRADUAÇÃO
EM CIÊNCIA DA INFORMAÇÃO
MESTRADO EM CIÊNCIA DA INFORMAÇÃO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado para participar da pesquisa Aplicações de Certificação Digital no Recife: Perspectivas em Ciência da Informação. Sua participação não é obrigatória. A qualquer momento você pode desistir de participar e retirar seu consentimento. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou a instituição. Os objetivos deste estudo são identificar aplicações e políticas públicas de certificação digital desenvolvidas na cidade do Recife. Sua participação nesta pesquisa consistirá em prestar esclarecimento sobre o Projeto _____. Os riscos relacionados com sua participação não trarão complicações legais, bem como os procedimentos adotados nesta pesquisa obedecem aos Critérios da Ética em Pesquisa com Seres Humanos conforme Resolução nº 196/96 do Conselho Nacional de Saúde. Nenhum dos procedimentos usados oferece riscos à sua dignidade. Os benefícios são relacionados ao registro e divulgação do projeto em tela. A sua identidade será guardada. As informações obtidas por meio desta pesquisa serão publicadas e asseguro o sigilo

sobre sua participação. Os dados não serão divulgados de forma a possibilitar sua identificação, apenas serão divulgadas as informações inerentes ao projeto no que tange à certificação digital. No entanto, nada impede que você permita a divulgação de sua identificação. Receberá uma cópia deste termo onde consta o telefone e o endereço do pesquisador principal, e do CEP, podendo tirar suas dúvidas sobre o projeto e sua participação, agora ou a qualquer momento.

_____

Sânderson Lopes Dorneles - Pesquisador
Telefone (81) 9795-9948; Endereço Rua Cel. Roberto Pessoa Ramos, nº 371, casa C, Piedade, Jaboatão dos Guararapes – Pernambuco; CEP 54400-280.

Declaro que entendi os objetivos, riscos e benefícios de minha participação, e concordo, voluntariamente, em participar. Podendo ser identificado:

( ) Sim ( ) Não

_____

Entrevistado

Recife, de de 2011.

APÊNDICE C – ROTEIRO DE ENTREVISTA SOBRE GESTÃO ELETRÔNICA DE DOCUMENTOS

UNIVERSIDADE FEDERAL DE PERNAMBUCO
PROGRAMA DE PÓS-GRADUAÇÃO
EM CIÊNCIA DA INFORMAÇÃO
MESTRADO EM CIÊNCIA DA INFORMAÇÃO

Título da Dissertação: Aplicações de Certificação Digital no Recife: Perspectivas em Ciência da Informação.

ENTREVISTA SOBRE GESTÃO ELETRÔNICA DE DOCUMENTOS

Projeto: _____

Questionamentos:

1) É aplicada alguma tabela de temporalidade de documentos que estabelece o prazo de guarda do documento digital?

   ( ) Não ( ) Sim Qual o prazo:_____

2) Qual é a destinação do documento digital após cumprir o prazo de guarda?

   ( ) Eliminação ( ) Guarda Permanente

3) Quais das estratégias abaixo são utilizadas para a preservação do documento digital durante longos períodos?

( ) cópia de segurança

( ) migração[31]

( ) emulação[32]

( ) publicação de plano de preservação digital

( ) outras (Especificar) _____

Observações:

_____
_____
_____
_____
_____
_____
_____
_____

[31] Migração é a transferência periódica de materiais digitais de uma configuração de *hardware/software* para outra ou, de uma geração de tecnologia computacional para a geração seguinte. O propósito da migração é preservar a integridade dos objetos digitais e assegurar a habilidade dos clientes para recuperar, expor e usá-los de outra maneira diante da constante mudança da tecnologia. (TASK FORCE ON THE ARCHIVING OF DIGITAL INFORMATION apud ARELLANO, 2004)

[32] As técnicas de emulação sugerem a preservação do dado no seu formato original, por meio de programas emuladores que poderiam imitar o comportamento de uma plataforma de *hardware* obsoleta e emular o sistema operacional relevante. (ARELLANO, 2004)

REFERÊNCIA:

ARELLANO, Miguel Ángel Márdero. **Preservação de Documentos Digitais**. Ci. Inf., Brasília, v. 33, n. 2, p. 15-27, 2004. Disponível em: <http://revista.ibict.br/index.php/ciinf/article/viewArticle/305>. Acesso em 15 ago 2010.

ANEXO A – DECRETO ESTADUAL Nº 31.612

DECRETO Nº 31.612, DE 03 DE ABRIL DE 2008.

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.

O GOVERNADOR DO ESTADO, no uso das atribuições que lhe são conferidas pelo artigo 37, inciso IV, da Constituição Estadual,

CONSIDERANDO os Ajustes SINIEF 07/2005, 11/2005, 02/2006, 04/2006 e 08/2007, publicados no Diário Oficial da União de 05 de outubro de 2005, de 21 de dezembro de 2005, de 29 de março de 2006, de 12 de julho de 2006 e de 03 de outubro de 2007, respectivamente,

DECRETA:

Art. 1º Fica instituída a Nota Fiscal Eletrônica - NF-e, a ser utilizada por contribuinte do ICMS previamente credenciado pela Secretaria da Fazenda - SEFAZ, em substituição à Nota Fiscal modelo 1 ou 1-A, observando-se entre outras normas específicas previstas no Ajuste SINIEF 07/2005 e alterações:

I - será emitida e armazenada eletronicamente, tendo existência apenas digital, para documentar operações e prestações;

II - terá sua validade jurídica garantida pela assinatura digital do emitente e pela autorização de uso concedida pela SEFAZ;

III - considerar-se-á emitida no momento em que for concedida a respectiva autorização de uso, devendo ser efetivada antes da ocorrência do fato gerador;

IV - poderá ser estabelecida a obrigatoriedade de sua emissão pela SEFAZ ou mediante Protocolo ICMS.

Parágrafo único. Aplicam-se à NF-e, no que couber, as normas da legislação do ICMS referentes a documentos fiscais relativos a operação de circulação de mercadoria e a prestação de serviço.

Art. 2º Em decorrência do disposto no art. 1º deste Decreto, o Decreto nº 14.876, de 12 de março de 1991, e alterações, passa a vigorar com as seguintes modificações, incluindo-se o artigo 129-A no seu Título II, Capítulo III:

"Art. 85. Serão emitidos, de acordo com a operação ou prestação realizada, os seguintes documentos fiscais:

.....

XXIX – a partir de 01 de abril de 2008, Nota Fiscal Eletrônica - NF-e (Ajuste SINIEF 07/2005).

.....

§ 32. É vedada a emissão de Nota Fiscal - modelo 1 ou 1-A por contribuinte credenciado para emitir NF-e, exceto quando autorizada pela Secretaria da Fazenda - SEFAZ. (ACR)

.....

Art. 129-A. Relativamente à NF-e prevista no art. 85, XXIX, utilizada em substituição a NF modelo 1 ou 1-A pelo contribuinte do ICMS, previamente credenciado pela SEFAZ, serão observadas as seguintes normas (Ajustes SINIEF 07/2005, 11/2005, 02/2006, 04/2006 e 08/2007): (ACR)

I - considera-se NF-e o documento fiscal emitido e armazenado eletronicamente, de existência apenas digital, para documentar operações e prestações, cuja validade jurídica é garantida pela assinatura digital do emitente e respectiva autorização de uso, que deve ser efetivada pela SEFAZ antes da ocorrência do fato gerador;

II - para a concessão da Autorização de Uso da NF-e, serão analisados os seguintes elementos:

a) a regularidade fiscal do emitente;

b) o credenciamento do emitente para emissão de NF-e, conforme previsto no § 1º;

c) a autoria da assinatura do arquivo digital da NF-e;

d) a integridade do arquivo digital da NF-e;

e) a observância ao leiaute do arquivo estabelecido no Ato COTEPE/ICMS nº 72, de 20 de dezembro de 2005;

f) a numeração do documento;

III - com base no resultado da análise referida no inciso II, a unidade fazendária cientificará o emitente:

a) da rejeição do arquivo da NF-e, em decorrência das seguintes situações:

1. falha na recepção ou no processamento do arquivo;

2. falha no reconhecimento da autoria ou da integridade do arquivo digital;

3. não-credenciamento do remetente para emissão da NF-e;

4. duplicidade de número da NF-e;

5. falha na leitura do número da NF-e;

6. outras falhas no preenchimento ou no leiaute do arquivo da NF-e;

7. uso de certificado digital divergente do emissor, revogado, expirado ou de uma certificadora não autorizada;

b) da denegação da Autorização de Uso da NF-e, em virtude da irregularidade fiscal do emitente;

c) da concessão da Autorização de Uso da NF-e;

IV - a ciência de que trata o inciso III será efetuada mediante protocolo transmitido ao emitente, via INTERNET, contendo, conforme o caso, a chave de acesso prevista no § 2º, II, "b" deste artigo, o número da NF-e, a data e a hora do recebimento da solicitação, pela SEFAZ, e o número do protocolo, observando-se:

a) o referido protocolo poderá ser autenticado mediante assinatura digital gerada com certificação digital da SEFAZ ou outro mecanismo de confirmação de recebimento;

b) no caso de rejeição do arquivo de NF-e ou da denegação da autorização de uso, conforme previsto no inciso III, "a" ou "b", o referido protocolo conterá informações que indiquem o motivo que tenha impedido a concessão da Autorização de Uso da NF-e, observando-se:

1. no caso de rejeição, não será arquivado na SEFAZ para consulta, sendo permitido ao interessado transmitir novamente o referido arquivo nas hipóteses dos itens 1, 2 e 5 da alínea "a" do inciso III;

2. no caso de denegação:

2.1 o arquivo digital transmitido ficará arquivado na SEFAZ, para consulta, nos termos do inciso V, "b", 2, identificado como Denegada a Autorização de Uso;

2.2 não será possível sanar a irregularidade e solicitar nova Autorização de Uso da NF-e que contenha a mesma numeração;

V - concedida a Autorização de Uso da NF-e, que não implica validação das informações nela contidas:

a) a NF-e não poderá ser alterada, observado o disposto na alínea "h" e no § 13;

b) a SEFAZ deverá:

1. transmitir a NF-e para a Secretaria da Receita Federal do Brasil e para:

1.1. Unidade da Federação de destino das mercadorias, no caso de operação interestadual;

1.2. Unidade da Federação onde deva processar-se o embarque da mercadoria na saída para o exterior;

1.3. Unidade da Federação de desembaraço aduaneiro, tratando-se de operação de importação de mercadoria ou bem do exterior;

1.4. Superintendência da Zona Franca de Manaus – SUFRAMA, quando a NF-e referir-se a operações nas áreas beneficiadas;

2. disponibilizar consulta relativa à NF-e no endereço eletrônico www.sefaz.pe.gov.br, pelo prazo mínimo de 180 (cento e oitenta) dias, observando-se:

2.1. após o mencionado prazo, a consulta à NF-e poderá ser substituída pela prestação de informações parciais que identifiquem o documento quanto ao número, à data de emissão, ao CNPJ/MF do emitente e do destinatário e ao valor e respectiva situação, que ficarão disponíveis pelo prazo decadencial;

2.2. a consulta à NF-e poderá ser efetuada pelo interessado:

2.2.1. mediante informação da chave de acesso da NF-e;

2.2.2. subsidiariamente, no ambiente nacional disponibilizado pela Receita Federal do Brasil;

c) a SEFAZ da Unidade da Federação do emitente poderá transmitir a NF-e para:

1. administrações tributárias municipais, nos casos em que a NF-e envolva serviços, mediante prévio convênio ou protocolo de cooperação;

2. outros órgãos e entidades da administração direta, indireta, inclusive fundações, que necessitem de informações da NF-e para desempenho de suas atividades, mediante prévio convênio ou protocolo de cooperação;

d) o emitente poderá solicitar o cancelamento do referido documento, desde que não tenha havido a circulação da respectiva mercadoria ou prestação de serviço, observadas as demais normas da legislação pertinente;

e) o cancelamento de que trata a alínea "d" somente poderá ser efetuado mediante Pedido de Cancelamento de NF-e, transmitido pelo emitente, à SEFAZ, conforme leiaute estabelecido no Ato COTEPE/ICMS nº 72, de 20 de dezembro de 2005, devendo o referido cancelamento:

1. ser efetivado via INTERNET, por meio de protocolo de segurança ou criptografia;

2. conter a assinatura digital do emitente certificada por entidade credenciada pela Infra-estrutura de Chaves Públicas Brasileira - ICP-Brasil, indicando-se o CNPJ/MF do estabelecimento emitente ou da matriz, a fim de garantir a autoria do documento digital;

3. ser realizado por meio de "software" desenvolvido ou adquirido pelo contribuinte ou disponibilizado pela SEFAZ;

f) a ciência do resultado do Pedido de Cancelamento de NF-e será feita mediante protocolo de que trata a alínea "e",

1, disponibilizado ao emitente ou a terceiro autorizado pelo emitente, via INTERNET, contendo, conforme o caso, a chave de acesso, o número da NF-e, a data e a hora do recebimento da solicitação, e o número do protocolo, podendo este ser autenticado mediante assinatura digital gerada com certificação digital da SEFAZ ou outro mecanismo de confirmação de recebimento;

g) a SEFAZ deverá transmitir à Secretaria da Receita Federal do Brasil ou a outra Unidade da Federação, os respectivos documentos de cancelamento de NF-e;

h) o emitente poderá sanar erros em campos específicos da NF-e, observado o disposto no art. 115, por meio de Carta de Correção Eletrônica - CC-e, nos termos do § 13, transmitida à SEFAZ;

VI - o contribuinte credenciado para emitir NF-e não poderá utilizar Nota Fiscal modelo 1 ou 1-A, observado o disposto no § 32 do art. 85;

VII - a obrigatoriedade de sua emissão poderá ser estabelecida pela SEFAZ ou mediante Protocolo ICMS, sendo vedada ao destinatário a aceitação de qualquer outro documento em sua substituição, exceto nos casos previstos na legislação em vigor;

VIII - a NF-e que acobertar operação interestadual de mercadoria ou relativa ao comércio exterior estará sujeita ao registro de passagem eletrônica, observando-se:

a) o disposto no Protocolo ICMS 10/2003, e alterações;

b) o registro será disponibilizado para a Unidade da Federação de origem e destino da mercadoria, bem como para a Unidade da Federação de passagem que o requisitar;

IX - a NF-e cancelada, denegada e os números inutilizados devem ser lançados, sem valores monetários, de acordo com as regras gerais de escrituração.

§ 1º Relativamente ao credenciamento, pela SEFAZ, para emissão da NF-e:

I - deverá ser solicitado pelo contribuinte, previamente, através do endereço eletrônico da SEFAZ na INTERNET: www.sefaz.pe.gov.br;

II - será vedado quando o contribuinte não utilizar sistema eletrônico de processamento de dados, nos termos dos arts. 275 a 312;

III - será dispensado na hipótese de contribuinte obrigado à emissão da NF-e;

IV - será concedido nos termos de portaria do Secretário da Fazenda.

§ 2º A NF-e deverá ser emitida com base em leiaute estabelecido pelo Ato COTEPE/ICMS nº 72, de 20 de dezembro de 2005, observadas as seguintes formalidades:

I – relativamente ao arquivo digital da NF-e:

a) deverá ser elaborado no padrão XML – "Extended Markup Language";

b) deverá ser transmitido via INTERNET, por meio de protocolo de segurança ou criptografia, com utilização de "software" desenvolvido ou adquirido pelo contribuinte ou disponibilizado pela SEFAZ;

c) sua transmissão, nos termos da alínea "b", implicará solicitação de concessão de Autorização de Uso da NF-e;

d) só poderá ser utilizado como documento fiscal após:

1. ser transmitido eletronicamente à SEFAZ, nos termos da alínea "b";

2. ter seu uso autorizado por meio de Autorização de Uso da NF-e, nos termos do inciso II do "caput";

II – relativamente à NF-e:

a) terá numeração seqüencial, de 1 a 999.999.999, por estabelecimento e por série, devendo ser reiniciada quando atingido esse limite;

b) deverá conter um código numérico, gerado pelo emitente, que comporá a chave de acesso de identificação da referida NF-e, juntamente com o CNPJ/MF do emitente, número e série do referido documento fiscal;

c) deverá ser assinada pelo emitente, com a assinatura digital certificada por entidade credenciada pela ICP-Brasil, contendo o CNPJ/MF do referido emitente ou da matriz, a fim de garantir a autoria do documento digital;

d) a série será designada por algarismo arábicos, em ordem crescente, a partir de 1, vedada a utilização de subsérie, podendo ser restringida pela SEFAZ a quantidade de séries;

e) ainda que formalmente regular, não será considerada documento fiscal idôneo quando tiver sido emitida ou utilizada com dolo, fraude, simulação ou erro, que possibilitem o não-pagamento do imposto ou qualquer outra vantagem indevida, ainda que por parte de terceiros;

f) quando não considerada documento idôneo, nos termos da alínea "e", os vícios ali referidos, para os efeitos fiscais,

contaminam também o respectivo Documento Auxiliar da Nota Fiscal Eletrônica - DANFE, impresso nos termos do § 9º.

§ 3º O contribuinte deverá solicitar, à SEFAZ, a inutilização de números da NF-e não utilizados, na eventualidade de quebra de seqüência da numeração dos referidos documentos, mediante Pedido de Inutilização de Número da NF-e, que deverá ser formulado até o 10º (décimo) dia do mês subseqüente àquele da ocorrência da mencionada quebra, observando-se:

I – o Pedido de Inutilização de Número da NF-e deverá ser assinado pelo emitente com assinatura digital certificada por entidade credenciada pela ICP-Brasil, contendo o CNPJ/MF do referido emitente ou da matriz, a fim de garantir a autoria do documento digital;

II – a transmissão do Pedido de Inutilização de Número da NF-e será efetivada via INTERNET, por meio de protocolo de segurança ou criptografia.

§ 4º A ciência do resultado do Pedido de Inutilização de Número da NF-e será feita mediante protocolo transmitido ao emitente, via INTERNET, contendo, conforme o caso, o número da NF-e, a data e a hora do recebimento da solicitação pela SEFAZ e o número do protocolo, podendo este ser autenticado mediante assinatura digital gerada com certificação digital da SEFAZ ou outro mecanismo de confirmação de recebimento.

§ 5º O emitente e o destinatário das mercadorias deverão manter em arquivo digital a NF-e, pelo prazo estabelecido na legislação para a guarda dos documentos fiscais, devendo ser apresentada à SEFAZ, quando solicitada.

§ 6º O destinatário de mercadoria deverá verificar a validade e autenticidade da NF-e e a existência de Autorização de Uso da NF-e.

§ 7º Caso o destinatário não seja contribuinte credenciado para a emissão de NF-e, deverá manter em arquivo o Documento Auxiliar da Nota Fiscal Eletrônica - DANFE, previsto no § 9º, relativo à NF-e da operação, devendo o referido DANFE ser apresentado à SEFAZ, quando solicitado.

§ 8º O destinatário da mercadoria deverá confirmar o recebimento das mercadorias e serviços constantes da NF-e, nos termos estabelecidos em portaria do Secretário da Fazenda.

§ 9º Para efeito de acompanhar mercadorias em trânsito e facilitar a consulta relativa à NF-e, prevista no inciso V, "b", 2, do "caput", será utilizado o Documento Auxiliar da Nota Fiscal Eletrônica - DANFE, conforme leiaute estabelecido pelo Ato COTEPE/ICMS nº 72, de 20 de dezembro de 2005, observando-se:

I - será impresso em papel, exceto papel jornal, no tamanho A4 (210 x 297 mm), podendo ser utilizadas folhas soltas, formulário de segurança, formulário contínuo ou formulário pré-impresso;

II - conterá código de barras, conforme padrão definido em Ato COTEPE;

III - conterá outros elementos gráficos, desde que não prejudiquem a leitura do seu conteúdo ou do código de barras por leitor óptico;

IV - somente será utilizado para transitar com as mercadorias após a concessão da Autorização de Uso da NF-e, de que

trata o inciso III, "c", do "caput", ou na hipótese prevista no § 12;

V - será escriturado, em substituição à NF-e, no caso de destinatário não-credenciado para emissão de NF-e, observado o disposto nos §§ 5º a 7º;

VI - será emitido com o número de cópias que atenda ao que a legislação exigir, quando esta prever a utilização de vias adicionais ou utilização específica para as vias das Notas Fiscais;

VII - terá os títulos e informações dos campos grafados de modo que seus dizeres e indicações estejam bem legíveis;

VIII - terá a aposição de carimbo no verso, quando do trânsito da mercadoria;

IX - permitirá indicação de informações complementares de interesse do emitente, impressas no verso, reservando o espaço, com a dimensão de 10x15 cm, em qualquer sentido, para aposição de carimbo, prevista no inciso VIII;

X - poderá ter seu leiaute alterado, quando solicitado pelo contribuinte e autorizado pela SEFAZ, desde que mantidos os campos obrigatórios da NF-e constantes do referido DANFE.

§ 10. Quando, em decorrência de problemas técnicos, não for possível transmitir a NF-e ou obter a resposta da Autorização de Uso da NF-e, o contribuinte deverá gerar novo arquivo, conforme definido em Ato COTEPE, informando que a respectiva NF-e foi emitida em contingência e adotar uma das seguintes alternativas:

I – transmitir a NF-e para a Receita do Brasil nos termos do § 2º, I, "b", "d" e II;

II – imprimir o DANFE em formulário de segurança que atenda às disposições previstas no art. 293, dispensando relativamente às vias adicionais de que trata o inciso VI do § 9º;

§ 11. Não será permitida a utilização de formulário de segurança para outra destinação, quando adquirido para a impressão de DANFE, devendo, o fabricante do mencionado formulário de segurança, observar as disposições dos §§ 3º e 4º do art. 293.

§ 12. Na hipótese do § 10:

I - relativamente ao disposto no inciso I, a SEFAZ poderá autorizar a NF-e utilizando-se da infra-estrutura tecnológica da Receita Federal do Brasil ou de outra Unidade da Federação;

II - relativamente a emissão do DANFE, nos termos do inciso II:

a) deverá ser impressa a denominação "DANFE", sendo vedada a utilização da expressão "Nota Fiscal";

b) deverá ser emitido em 2 (duas) vias, que devem ser mantidas em arquivo pelo destinatário ou emitente, conforme o caso, pelo prazo estabelecido na legislação tributária para guarda de documentos fiscais, tendo as mencionadas vias a seguinte destinação:

1. uma via acompanhará o trânsito das mercadorias até que sejam sanados os problemas técnicos;

2. a outra ficará em poder do emitente;

c) deverá constar no corpo do documento a expressão: "DANFE em contingência, impresso em decorrência de problemas técnicos".

§ 13. Imediatamente após a cessação dos problemas técnicos referidos no § 10, a NF-e gerada em contingência deverá ser transmitida à SEFAZ, observando-se:

I – caso seja rejeitada pela SEFAZ, o contribuinte deverá:

a) gerar novamente o arquivo com a mesma numeração e série, sanando a irregularidade;

b) solicitar nova autorização de uso da NF-e;

c) imprimir em formulário de segurança o DANFE correspondente à NF-e autorizada;

II – caso a geração saneadora da irregularidade da NF-e tenha promovido alguma alteração no DANFE, providenciar, junto ao destinatário, a entrega da NF-e autorizada bem como do novo DANFE impresso nos termos do inciso I, "c";

III - comunicação do fato à SEFAZ se no prazo de 30 (trinta) dias do recebimento da mercadoria não puder confirmar a existência da Autorização de Uso da NF-e;

IV – lavratura de termo no livro Registro de Documentos Fiscais e Termos de Ocorrência, modelo 6, informando o motivo da entrada em contingência, número dos formulários de segurança utilizados, a data e hora do seu início e seu término, bem como a numeração e série das NF-e geradas no período.

§ 14. A fim de garantir a autoria do documento digital, a CC-e prevista no inciso V, "h", do "caput", deverá atender ao leiaute estabelecido em Ato COTEPE e ser assinada pelo emitente com assinatura digital certificada por entidade credenciada pela ICP–Brasil, contendo o CNPJ/MF do estabelecimento emitente ou da matriz, observando-se ainda as seguintes normas:

I - transmissão da CC-e será efetivada via INTERNET, por meio de protocolo de segurança ou criptografia;

II - a ciência da recepção da CC-e será feita mediante protocolo disponibilizado ao emitente, via INTERNET, contendo, conforme o caso, a chave de acesso, o número da NF-e, a data e a hora do recebimento da solicitação e o número do protocolo, podendo este ser autenticado mediante assinatura digital gerada com certificação digital da SEFAZ ou outro mecanismo de confirmação de recebimento;

III - o emitente deverá consolidar, havendo mais de uma CC-e para a mesma NF-e, na última, as informações anteriormente retificadas;

IV - a SEFAZ deverá transmitir a CC-e para as entidades previstas no inciso V, "b" do "caput";

V – o recebimento da CC-e, prevista no inciso II, não implica validação das informações contidas do referido documento.

§ 15. A SEFAZ disponibilizará à empresa autorizada à sua emissão, consulta eletrônica referente à situação cadastral dos contribuintes do ICMS, conforme padrão estabelecido em Ato COTEPE.

§ 16. Aplicam-se à NF-e, no que couber, as normas da legislação do ICMS referentes a documentos fiscais relativos a operação de circulação de mercadoria e a prestação de serviço.

.....
.....".

Art. 3º Este Decreto entra em vigor na data de sua publicação.

Art. 4º Revogam-se as disposições em contrário.

PALÁCIO DO CAMPO DAS PRINCESAS, em 03 de abril de 2008.

EDUARDO HENRIQUE ACCIOLY CAMPOS

Governador do Estado

DJALMO DE OLIVEIRA LEÃO

LUIZ RICARDO LEITE DE CASTRO LEITÃO

FRANCISCO TADEU BARBOSA DE ALENCAR

ANEXO B - PROVIMENTO Nº 13 DO CNJ

Conselho Nacional De Justiça
Corregedoria

PROVIMENTO Nº 13

Dispõe sobre a emissão de certidão de nascimento nos estabelecimentos de saúde que realizam partos

O CORREGEDOR NACIONAL DE JUSTIÇA, Ministro Gilson Dipp, no uso de suas atribuições legais e regimentais,

CONSIDERANDO os termos dos arts. 236 e 103–B, § 4º, III, da Constituição Federal,

CONSIDERANDO os termos dos arts. 37 e 38 da Lei n. 11.977, de 07 de julho de 2009,

CONSIDERANDO o disposto no art. 8º, X, do Regimento Interno do Conselho Nacional de Justiça, dotado de força normativa, na forma do art. 5º, § 2º, da Emenda Constitucional nº 45, de 30 de dezembro de 2004, e

CONSIDERANDO que é o registro de nascimento perante as serventias extrajudiciais do registro civil das pessoas naturais

que confere, em primeira ordem, identidade ao cidadão e dá início ao seu relacionamento formal com o Estado, conforme dispõem os arts. 2º e 9º do Código Civil em vigor;

CONSIDERANDO a instituição do Compromisso Nacional pela Erradicação do Sub–registro Civil de Nascimento e a ampliação do acesso à Documentação Básica, por meio do Decreto nº 6.289, de 6 de dezembro de 2007, e da publicação dos Protocolos de Cooperação Federativa – Compromissos: Mais Nordeste pela Cidadania e Mais Amazônia pela Cidadania, que estabelecem a intensificação das ações para erradicar o sub–registro civil de nascimento nas respectivas regiões, até o final de 2010, incluída o registro de nascimento e a emissão de certidão de nascimento nos estabelecimentos de saúde antes da alta hospitalar;

CONSIDERANDO a parceria firmada entre a Secretaria de Direitos Humanos da Presidência da República, o Conselho Nacional de Justiça, o Ministério da Justiça, a Associação dos Notários e Registradores do Brasil e a Arpen Brasil – Associação Nacional dos Registradores de Pessoas Naturais, por meio do Acordo de Cooperação, processo nº 00005.003503/2007–71, publicado no Diário Oficial em 3 de janeiro de 2008, o qual objetiva cooperação com vistas à implantação do Plano Social de Registro Civil de Nascimento e Documentação Básica, destinado à erradicação do sub–registro civil de nascimento;

CONSIDERANDO a participação do Conselho Nacional de Justiça no Grupo de Trabalho que discute a criação e implantação do SIRC – Sistema de Informações de Registro Civil, de acordo com Portaria Conjunta SEDH/PR/MJ/CNJ, publicada em 18 de fevereiro de 2009;

CONSIDERANDO a participação do Conselho Nacional da Justiça (CNJ), da Corregedoria Nacional de Justiça e das Corregedorias – Gerais de Justiça dos Estados e Distrito Federal nas ações de Mobilização Nacional pela Certidão de Nascimento;

CONSIDERANDO a publicação do Decreto nº 7.231 de 14 de julho de 2010 e dos provimentos nº 02 de 27 de abril de 2009, nº 03 de 17 de novembro de 2009 e nº 10 de 13 de julho de 2010 da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça;

CONSIDERANDO que a Associação dos Registradores das Pessoas Naturais do Brasil (ARPEN–BR) sugeriu a possibilidade de formação de consórcio de empregadores urbanos para a contratação de preposto capaz de atuar em parte dos estabelecimentos de saúde;

CONSIDERANDO o entendimento de que a aplicação analógica do artigo 25–A da Lei n. 8.212/1991 não encontra óbice legal (art. 5º, II, da CF) e contribui para a obtenção do pleno emprego e para o incremento do bem–estar e da justiça social (art. 170, VIII e 193, ambos da Constituição Federal);

CONSIDERANDO, por fim, a conveniência de uniformizar e aperfeiçoar o registro de nascimento e a emissão da respectiva certidão nos estabelecimentos de saúde, antes da alta hospitalar da mãe ou da criança;

RESOLVE:

Art. 1º A emissão de certidão de nascimento nos estabelecimentos de saúde que realizam partos será feita por

meio da utilização de sistema informatizado que, via rede mundial de computadores, os interligue às serventias de registro civil existentes nas Unidades Federativas e que aderiram ao Sistema Interligado, a fim de que a mãe e/ou a criança receba alta hospitalar já com a certidão de nascimento.

§ 1º O posto de remessa, recepção de dados e impressão de certidão de nascimento que funciona em estabelecimentos de saúde que realizam partos e que está conectado pela rede mundial de computadores às serventias de registro civil das pessoas naturais é denominado “Unidade Interligada”.

§ 2º A Unidade Interligada que conecta estabelecimento de saúde aos serviços de registro civil não é considerada sucursal, pois relaciona–se com diversos cartórios.

§ 3º Todo processo de comunicação de dados entre a Unidade Interligada e os cartórios de registro civil das pessoas naturais, via rede mundial de computadores, deverá ser feito com o uso de certificação digital, desde que atenda aos requisitos da Infraestrutura de Chaves Públicas Brasileira – ICP.

Art. 2º A implantação das Unidades Interligadas dar–se–á mediante convênio firmado entre o estabelecimento de saúde e o(s) registrador(es) da cidade ou distrito onde estiver localizado o estabelecimento, com a supervisão e a fiscalização das Corregedorias Gerais de Justiça dos Estados e Distrito Federal, bem como da Corregedoria Nacional de Justiça.

§ 1º A Unidade Interligada deverá ser cadastrada no Sistema Justiça Aberta mediante solicitação à Corregedoria Nacional de Justiça, formulada por qualquer dos registradores conveniados. A solicitação deverá ser conter certificação digital e ser encaminhada para o endereço: justiça.aberta@cnj.jus.br.

§ 2º Da solicitação de cadastro da Unidade Interligada no Sistema Justiça Aberta, ou de adesão à unidade, obrigatoriamente deve constar o nome completo e o CPF do (s) registrador (es) e dos substitutos ou escreventes autorizados a nela praticar atos pertinentes ao registro civil e que possuam a certificação digital exigida, inclusive daqueles contratados na forma dos artigos 3º e 4º deste Provimento.

§ 3º A instalação de Unidade Interligada deverá ser comunicada pelo (s) registrador (es) conveniado (o) à Corregedoria Geral de Justiça do Estado ou Distrito Federal responsável pela fiscalização.

§4º Mediante prévia comunicação ao juízo competente pela sua fiscalização e devido cadastramento no Sistema Justiça Aberta por meio do endereço eletrônico www.cnj.jus.br/corregedoria/seguranca/, qualquer registrador civil do País poderá aderir ou se desvincular do Sistema Interligado, ainda que não esteja conveniado a uma Unidade Interligada. Da adesão do registrador ao Sistema Interligado obrigatoriamente deve constar o nome completo e o CPF do registrador e dos substitutos ou escreventes autorizados praticar atos pertinentes ao registro civil e que possuam a certificação digital exigida.

§ 5º Todos os Cartórios de Registro Civil do País deverão manter atualizado, no Sistema Justiça Aberta: a) informação sobre a sua participação ou não no Sistema Interligado que permite o registro de nascimento e a expedição das respectivas certidões na forma deste Provimento; b) o nome e o CPF do oficial registrador (titular ou responsável pelo expediente); c) o nome dos substitutos e dos escreventes autorizados a praticar atos relativos ao registro civil (art. 20 e §§ da Lei n. 8.935/1994) e; d) o endereço completo de sua sede, inclusive com identificação de bairro e CEP quando existentes.

Art. 3º O profissional da Unidade Interligada que operar, nos estabelecimentos de saúde, os sistemas informatizados para transmissão dos dados necessários à lavratura do registro de nascimento e emissão da respectiva certidão será escrevente preposto do registrador, contratado nos termos do artigo 20 da Lei n. 8.935, de 18 de novembro de 1994. Caso os registradores interessados entendam possível a aplicação analógica do disposto no art. 25–A da Lei nº 8.212, de 24 de julho de 1991, o escrevente preposto poderá ser contratado por consórcio simplificado, formado pelos registradores civis interessados.

Parágrafo único. Na hipótese de o estabelecimento de saúde estar localizado em cidade ou distrito que possua mais de um registrador civil, e inexistindo consenso para que preposto de apenas um deles, ou preposto contratado por meio de consórcio, atue na unidade interligada, faculta–se a execução do serviço pelo sistema de rodízio entre substitutos ou escreventes prepostos, no formato estabelecido pelos próprios registradores e comunicado à Corregedoria Geral de Justiça da respectiva unidade da federação.

Art. 4º Não ocorrendo a designação de preposto na forma do art. 3º, poderão ser indicados empregados pelos estabelecimentos de saúde, o qual deverá ser credenciado por ao menos um registrador civil da cidade ou do distrito no qual funcione a unidade interligada.

§ 1º No caso da indicação prevista no "caput" deste artigo, e sem prejuízo do disposto nos artigos 22 e seguintes da Lei 8.935, de 1994 em relação aos credenciadores, o estabelecimento de saúde encaminhará termo de compromisso para a Corregedoria Geral de Justiça de sua unidade da federação, pelo qual se obriga a:

I – responder civilmente pelos erros cometidos por seus funcionários.

II – noticiar à autoridade competente a ocorrência de irregularidades quando houver indícios de dolo.

III – aceitar a supervisão pela Corregedoria Geral de Justiça e pela Corregedoria Nacional de Justiça sobre os empregados que mantiver na Unidade Interligada.

§ 2º Cópia da comunicação do estabelecimento de saúde à Corregedoria Geral de Justiça, com o respectivo comprovante da entrega, permanecerá arquivada na unidade interligada.

§ 3º O Juízo competente para a fiscalização do serviço solicitará, de ofício ou a requerimento de registrador civil, a substituição de tais empregados quando houver indícios de desídia ou insuficiência técnica na operação da unidade interligada.

Art. 5º Os custos de manutenção do equipamento destinado ao processamento dos registros de nascimento, bem como os custos da transmissão dos dados físicos ou eletrônicos para as serventias de Registro Civil, quando necessário serão financiados:

I – com recursos de convênio, nas localidades onde houver sido firmado entre a unidade federada e a Secretaria de Direitos Humanos da Presidência da República;

II – com recursos da maternidade, nas localidades não abrangidas pelo inciso anterior;

III – com recursos de convênios firmados entre os registradores e suas entidades e a União, os Estados, o DF ou os Municípios.

Art. 6º Todos os profissionais das Unidades Interligadas que forem operar os sistemas informatizados, inclusive os empregados dos estabelecimentos de saúde referidos no caput do artigo 4º deste Provimento, devem ser previamente credenciados junto a registrador (es) civil (is) conveniado (s) da unidade e capacitados de acordo com as orientações fornecidas pelo (s) registrador (es) conveniados (s) à unidade ou por suas entidades representativas, sem prejuízo de parcerias com a Secretaria de Direitos Humanos da Presidência da República e supervisão pelas Corregedorias locais e pela Corregedoria Nacional de Justiça.

Parágrafo Único. A capacitação necessariamente contará com módulo específico sobre a identificação da autenticidade das certificações digitais.

Art. 7º Aos profissionais que atuarão nas Unidades Interligadas incumbe:

I – receber os documentos comprobatórios da declaração de nascimento, por quem de direito, na forma do art. 8º deste Provimento;

II – acessar o sistema informatizado de registro civil e efetuar a transmissão dos dados preliminares do registro de nascimento;

III – receber o arquivo de retorno do cartório contendo os dados do registro de nascimento;

IV – imprimir o termo de declaração de nascimento, colhendo a assinatura do declarante e das testemunhas, se for o caso, na forma do art. 37 e seguintes da Lei nº 6.015, de 1973;

V – transmitir o Termo de Declaração para o registrador competente;

VI – imprimir a primeira via da certidão de nascimento, já assinada eletronicamente pelo Oficial de Registro Civil competente com o uso de certificação digital;

VII – apor o respectivo selo, na forma das respectivas normas locais, se atuante nas unidades federativas onde haja sistema de selo de fiscalização;

VIII – zelar pela guarda do papel de segurança, quando obrigatória sua utilização (Provimento 03 da Corregedoria Nacional de Justiça);

§ 1º – Em registro de nascimento de criança apenas com a maternidade estabelecida, o profissional da Unidade Interligada facultará à respectiva mãe a possibilidade de declarar o nome e prenome, profissão, identidade e residência do suposto pai, reduzindo a termo a declaração positiva ou negativa. O oficial do registro remeterá ao juiz competente de sua Comarca certidão integral do registro, a fim de ser averiguada a procedência da declaração positiva (Lei n. 8.560/1992).

§ 2º As assinaturas apostas no termo de declaração de nascimento de que trata o inciso IV deste artigo suprem aquelas previstas no "caput" do art. 37 da Lei nº 6.015, de 1973.

§ 3º As unidades federativas, quando empreguem o sistema de selos de fiscalização, fornecerão os documentos às unidades interligadas, na forma de seus regulamentos, sob critérios que evitem a interrupção do serviço registral.

Art. 8º O profissional da Unidade Interligada que operar o sistema recolherá do declarante do nascimento a documentação necessária para que se proceda ao respectivo registro.

§ 1º Podem declarar o nascimento perante as unidades interligadas:

I – o pai maior de 16 (dezesseis) anos, desde que não seja absolutamente incapaz, ou pessoa por ele autorizada mediante instrumento público;

II – a mãe maior de 16 anos, desde que não seja absolutamente incapaz;

§ 2º Caso a mãe seja menor de 16 anos, ou absolutamente incapaz, ou esteja impedida de declarar o nascimento, seus representantes legais podem fazê–lo

§ 3º A paternidade somente poderá reconhecida voluntariamente:

I – por declaração do pai, desde que maior de 16 anos e não seja absolutamente incapaz;

II – por autorização ou procuração do pai, desde que formalizada por instrumento público;

III – por incidência da presunção do artigo 1.597 do Código Civil, caso os pais sejam casados.

Art. 9º O registro de nascimento por intermédio da Unidade Interligada depende, em caráter obrigatório, da apresentação de:

I – declaração de Nascido Vivo – DNV, com a data e local do nascimento;

II – documento oficial de identificação do declarante;

III – documento oficial que identifique o pai e a mãe do registrando, quando participem do ato;

IV – certidão de casamento dos pais, na hipótese de serem estes casados e incidir a presunção do art. 1.597 do Código Civil;

V – termo negativo ou positivo da indicação da suposta paternidade firmado pela mãe, nos termos do § 1º do art. 7º deste Provimento, quando ocorrente a hipótese.

§ 1º O registro de nascimento solicitado pela Unidade Interligada será feito em cartório da cidade ou distrito de residência dos pais, se este for interligado, ou, mediante expressa opção escrita do declarante e arquivada na unidade interligada, em cartório da cidade ou distrito em que houver ocorrido o parto.

§ 2º Caso o cartório da cidade ou distrito de residência dos pais não faça parte do sistema interligado, e não haja opção do declarante por cartório do lugar em que houver ocorrido o parto, deve–se informar ao declarante quanto à necessidade de fazer o registro diretamente no cartório competente.

Art. 10 Não poderá ser obstada a adesão à Unidade Interligada de qualquer registrador civil do município ou distrito no qual se localiza o estabelecimento de saúde que realiza partos, desde que possua os equipamentos e certificados digitais necessários ao processo de registros de nascimento e emissão da respectiva certidão pela rede mundial de computadores.

§ 1º A adesão do registrador civil a uma Unidade Interligada será feita mediante convênio, cujo instrumento será remetido à Corregedoria Nacional de Justiça nos moldes dos parágrafos 1º e 2º do artigo 2º deste Provimento.

§ 2º No caso de o cartório responsável pelo assento ser diverso daquele que remunera o preposto atuante na unidade interligada, o ato será cindido em duas partes. A primeira será praticada na unidade integrada e formada pela qualificação, recebimento das declarações e entrega das certidões; a segunda será praticada pelo cartório interligado responsável pelo assento e formada pela conferência dos dados e a lavratura do próprio assento.

§ 3º O ressarcimento pelo registro de nascimento, no caso do parágrafo anterior, deve ser igualmente dividido, na proporção de metade para o registrador ou consórcio responsável pela remuneração do preposto que atua na unidade interligada, e metade para o registrador que efetivar o assento.

§ 4º Caso o operador da unidade interligada seja remunerado por pessoa diversa dos registradores ou de seus consórcios, o ressarcimento será feito na proporção de metade para o (s) registrador (es) responsável (is) pelo credenciamento do preposto que atua na unidade interligada, e metade para o registrador que efetivar o assento.

Art. 11 Os documentos listados no art. 7º, V, e no art. 9º, serão digitalizados pelo profissional da Unidade Interligada e remetidos ao cartório de registro civil das pessoas naturais, por meio eletrônico, com observância dos requisitos da Infraestrutura de Chaves Públicas Brasileira – ICP.

Parágrafo único. O Oficial do Registro Civil, recebendo os dados na forma descrita no “caput”, deverá conferir a adequação dos documentos digitalizados para a lavratura do registro de nascimento e posterior transmissão do termo de declaração para a unidade interligada.

Art. 12 O Oficial do Registro Civil responsável pela lavratura do assento, frente à inconsistência ou dúvida em relação à documentação ou declaração, devolverá ao profissional da Unidade Interligada, por meio do sistema informatizado, o requerimento de registro, apontando as correções ou diligências necessárias à lavratura do registro de nascimento.

Art. 13 A certidão do assento de nascimento conterá a identificação da respectiva assinatura eletrônica, propiciando sua conferência na rede mundial de computadores pelo preposto da unidade interligada, que nela aporá a sua assinatura, ao lado da identificação do responsável pelo registro, antes da entrega aos interessados.

Parágrafo único. A certidão somente poderá ser emitida depois de assentado o nascimento no livro próprio de registro, ficando o descumprimento deste dispositivo sujeito às responsabilidades previstas nos artigos 22/24 e 31 e seguintes da Lei 8.935, de 1994, e art. 47 da Lei 6.015, de 1973.

Art. 14 A certidão de nascimento deverá ser entregue, pelo profissional da Unidade Interligada, ao declarante ou interessado, nos moldes padronizados, com o número de matrícula (Provimentos 02 e 03 da Corregedoria Nacional de Justiça) e sempre antes da alta da mãe e/ou da criança registrada.

Art. 15 O profissional da Unidade Interligada, após a expedição da certidão, enviará em meio físico, ao registrador que lavrou o respectivo assento, a DNV e o Termo de Declaração referidos nos artigos 7º, V, e 9º, I, deste Provimento.

Parágrafo único. Os cartórios de registro civil das pessoas naturais que participem do Sistema Interligado deverão manter sistemática própria para armazenamento dos documentos digitais referidos nos artigos 7º, V, e 9º deste Provimento. E arquivo físico para o armazenamento dos termos de declaração de nascimento e respectivas DNVs.

Art. 16 Sem prejuízo dos poderes conferidos à Corregedoria Nacional de Justiça e às Corregedorias dos Tribunais de Justiça, a fiscalização judiciária dos atos de registro e emissão das respectivas certidões, decorrentes da aplicação deste Provimento, é exercida pelo juízo competente, assim definido na órbita estadual e do Distrito Federal (art. 48 da Lei n. 6.015/1973), sempre que necessário, ou mediante representação de qualquer interessado, em face de atos praticados pelo oficial de registro seus prepostos ou credenciados.

Art. 17 Ficam preservados, por um ano da publicação deste provimento, os serviços de registro civil já prestados nesta data nos estabelecimentos que realizam partos sob forma diversa daquela ora regulamentada, desde que tenham o seu funcionamento autorizado pelo Juízo competente para a fiscalização dos trabalhos.

Art. 18 Este Provimento entra em vigor 30 (trinta) dias após a sua publicação.

Brasília, 3 de setembro de 2010.

MINISTRO GILSON DIPP
Corregedor Nacional de Justiça

ANEXO C - TRANSCRIÇÃO DAS RESPOSTAS OBTIDAS NAS ENTREVISTAS

1 – Conformidade com a ICP-Brasil:

SEFAZ – PE: O projeto da NFe, como também o sistema corporativo e-Fisco, aceitam todos os certificados emitidos segundo o padrão da ICP-Brasil, que é a ACRaiz do Brasil e de qualquer AC certificadora que esteja abaixo dela.

ATI: SERASA para os certificados digitais pessoais A3 e CERTISIGN para os certificados digitais para servidor web SSL ICP-Brasil.

2 - Programas e formatos de computadores utilizados no processo de certificação digital:

SEFAZ – PE: No projeto da NFe, a assinatura dos documentos XML que serão enviados e validados pela aplicação autorizadora da SEFAZ, é de responsabilidade do contribuinte, conforme legislação vigente e manuais de integração com o contribuinte, disponíveis no site nacional do projeto, www.nfe.fazenda.gov.br.

ATI: O formato do documento final é Bitmap (BMP) e são utilizados para assinar e verificar os documentos: BRY Sgner[33] e ViaCert[34].

---

[33] O BRY Signer é um *software* que tem o objetivo básico de realizar as operações de assinatura digital e carimbo de tempo de documentos eletrônicos e de verificar documentos assinados digitalmente (Fonte *site* BRY Signer: http://signer.bry.com.br/pg1_brysigner.html)

[34] Na qualidade de *proxy*, o ViaCert agrega a geração e conferência de assinaturas digitais, para que possam ser feitas diretamente em formulários

3 - Procedimentos adotados para emissão de certificados e verificação da assinatura digital:

SEFAZ – PE: A SEFAZ-PE não é uma AC, portanto não emite certificados digitais. Quanto à forma de se verificar a legitimidade de um certificado digital, passa por dois momentos: A verificação da validade do certificado, contra as listas de certificados revogados, atualizadas diariamente, pelas AC´s, como também, quanto a validade da assinatura do documento, através de mecanismos que permitem calcular se um documento foi de fato assinado pelo certificado nele informado e que não tenha sido alterado ao longo do processo de transmissão e recepção.

ATI: O certificado digital pessoal é emitido através da empresas credenciadas do ICP-BRASIL, no caso estamos usando a AC-SERASA. A legitimidade da assinatura digital é verificada através do próprio assinador / verificador que são softwares feitos de acordo com as especificações do ICP-BRASIL.

4 – Local de armazenamento do documento certificado digitalmente:

SEFAZ – PE: A NFe recebida é armazenada sempre em meio eletrônico.

ATI: Por um motivo cultural de ter o “papel fisico” é impressa a certidão de nascimento na maternidade, essa impressão é

---

web e provê melhorias ao acesso de sites seguros. Fonte: site FINEP. Disponível em: http://www.jurozero.finep.gov.br/jurozero_prod/WebHelpPortal/O_ViaCert_Como_um_Proxy.htm. Acesso em: 08 jul. 2011.

feita com papel especial homologado pela casa da moeda e com toda regulamentação prevista na lei, esse documento tem como objetivo ser uma cópia fiel do que foi criado no meio digital.

5 - Legislação concernente:

SEFAZ – PE: A legislação vigente que institui o processo da NFe tanto Nacionalmente,protocolo ICMS 10/07 Introduz alterações na Consolidação da Legislação Tributária do Estado de Pernambuco, relativamente à Nota Fiscal Eletrônica - NF-e e ao Documento Auxiliar da Nota Fiscal Eletrônica – DANFE, e suas alterações, como localmente em nosso estado, Decreto nº 31.612, de 03 de abril de 2008 que Introduz alterações na Consolidação da Legislação Tributária do Estado de Pernambuco, relativamente à Nota Fiscal Eletrônica - NF-e e ao Documento Auxiliar da Nota Fiscal Eletrônica - DANFE. e suas alterações.

ATI: Além da MP 2200-2 que regulamenta a certificação digital, a utilização do sistema esta respaldada no Provimento estadual nº 38/2008 e o 11/2010 da Corregedoria Geral de Justiça e o Decreto Estadual 32.876/2008.

6 - Segurança da informação:

SEFAZ – PE: No âmbito da SEFAZ todo o processo de comunicação do contribuinte com o aplicativo autorizador de NFe , é feito sob o protocolo HTTPS, com autenticação mútua, ou seja , certificados de servidor e de cliente, para garantir todo o processo.

ATI: São empregadas as normas de politicas de segurança da ATI e dentro do DataCenter da própria ATI.

7 – Preservação digital:

SEFAZ – PE: A SEFAZ-PE possui um plano de preservação digital de seus documentos, de caráter confidencial, porém que utiliza ferramentas para viabilização da guarda, indexação, preservação dos originais, garantindo sua autenticidade, entre outras.

ATI: São empregadas as normas e políticas da ATI.

8 – Resultados dos projetos:

SEFAZ – PE: Com o advento da NFe, diariamente autorizamos apenas em Pernambuco, uma média de 150.000 Notas Eletrônicas, evitando assim a emissão de 750.000 folhas de nota fiscal modelo 1 e 1^A (em 5 vias). Esses números nacionalmente na data de hoje 25/02/2011, montam 2.198.183.374 notas autorizadas, perfazendo um valor total em reais de R$ 68.795.929.234.084,57.

Com isso houve um aumento na arrecadação de todos os Estados, uma melhoria na qualidade da informação e especialmente um aperfeiçoamento nas atividades de auditoria, com o cruzamento de informações, através de ferramentas de Data Warehouse [35] / Business Intelligence [36](DW/BI).

[35] Um data warehouse (ou armazém de dados) é um sistema de computação utilizado para armazenar informação relativa às atividades de uma organização em banco de dados, de forma consolidada. O desenho da base de dados favorece os relatórios e análise de grandes volumes de

Com a totalidade das operações totalmente eletrônicas já é possível ter uma melhor qualidade e acompanhamento de tudo que circula no país, possibilitando entre muitas coisas, o rastreamento de produtos desde sua fabricação até a entrega ao consumidor final, evitando desvios e fraudes.

ATI: O projeto está implantado em 8 maternidades e 19 cartórios dez mil registros.

---

dados e obtenção de informações estratégicas que podem facilitar a tomada de decisão (PETUCO, 2006)

[36] O termo BI (Business Intelligence) é associado à inteligência nos negócios, ou seja, o uso de informações de maneira diferenciada para obter vantagem competitiva diante dos concorrentes. Estas informações são disponibilizadas pelos chamados Sistemas de Apoio à Decisão (SAD), cujo termo vem do inglês Executive Support Systems (TERRIBILI, 2009).