MEMÓRIA DIGITAL: APLICAÇÕES DE CERTIFICAÇÃO DIGITAL

Sânderson Lopes Dorneles[*]

Resumo:
A presente comunicação tem por finalidade identificar aplicações e políticas públicas de certificação digital desenvolvidas na cidade do Recife, a fim de compreender os novos suportes da informação que conservarão a memória da atual sociedade. Para tanto, são abordados conceitos, tecnologias da informação e requisitos sobre certificação digital, as políticas públicas a respeito do assunto, a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, bem como a descrição de duas aplicações de certificação digital em desenvolvimento no Recife. No final são tecidas algumas considerações sobre o panorama da certificação digital no Recife e sugestões do que deve ser feito para preservar a memória digital.

Palavras-chave: Certificação digital. Memória digital. Tecnologia da informação. Políticas públicas. Autenticidade da informação digital.

INTRODUÇÃO

As tecnologias da informação revolucionaram os processos de criação de documentos, bem como a Internet agilizou a forma de transmitir esses documentos, porém um problema a ser estudado é a questão da legalidade e autenticidade das informações contidas nos documentos gerados na forma digital, bem como discutir as formas de preservação dessa memória certificada digitalmente.

A presente comunicação tem como tema a certificação digital, uma tecnologia da informação que é campo de estudo da Ciência da Informação, haja vista que o imperativo tecnológico está impondo a transformação da sociedade moderna em sociedade da informação, era da informação ou sociedade pós-industrial, conforme afirmação de Saracevic (1996).

Reconhecida a instabilidade da informação arquivística digital, 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 integridade, o acesso contínuo e o uso pleno da informação a todos os segmentos

[*] Arquivista (Reg. DRT/POA nº 1.500/2005), pós-graduando em Arquivos e Patrimônio Histórico, Artístico e Cultural Integrado pela Universidade Salgado de Oliveira (UNIVERSO), pesquisador em Ciência da Informação da Universidade Federal de Pernambuco (UFPE).

da sociedade brasileira. 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.

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. 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.

Neste sentido, busca-se identificar 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 os novos suportes da informação que conservarão a memória da atual sociedade. Para tanto, e à luz da Ciência da Informação e da interdisciplinaridade da Arquivologia e Tecnologia da Informação, serão abordados conceitos relevantes do tema, comentados dois projetos já em andamento, como também ressaltada a importância da preservação da memória digital. Neste sentido, o presente estudo valeu-se da pesquisa exploratória, fazendo uso de levantamento bibliográfico sobre os principais conceitos da certificação digital, a fim de abordar as aplicações de certificação digital no Recife como objetos de estudo. Assim como da coleta de dados sobre o projeto Minha Certidão do governo do Estado de Pernambuco e o projeto Nota Fiscal Eletrônica, também do Estado de Pernambuco e desenvolvido em parceria com a Receita Federal do Brasil.

A CERTIFICAÇÃO DIGITAL

Os computadores e a Internet são largamente utilizados para o processamento de dados e para a troca de mensagens e documentos entre cidadãos, governo e empresas. No entanto, estas transações eletrônicas necessitam da adoção de mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas. A certificação digital é a tecnologia que provê estes mecanismos. No cerne da certificação digital está o certificado digital, um documento eletrônico que contém o nome, um número público exclusivo denominado chave pública e muitos outros dados que mostram quem somos para as pessoas e para os sistemas de informação. A chave pública serve para validar uma assinatura realizada em documentos eletrônicos. A certificação digital tem trazido inúmeros benefícios para os cidadãos e para as instituições que a adotam. Com a certificação digital é possível utilizar a Internet como meio de

comunicação alternativo para a disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e substancial redução de custos.

Porém a facilidade de criar e transmitir documentos traz como consequência a informalidade na linguagem, nos procedimentos administrativos, bem como o esvaziamento das posições hierárquicas. A facilidade de acesso pode acarretar intervenções não autorizadas que podem resultar na adulteração ou perda dos documentos. A rápida obsolescência tecnológica (*software*, *hardware* e formatos) e a degradação das mídias digitais dificultam a preservação de longo prazo dos documentos e sua acessibilidade contínua. Os problemas em questão tornam necessária a adoção de medidas preventivas para minimizá-los. Dessa forma, o Conselho Nacional de Arquivos (CONARQ), criado pela Lei nº 8.159, de 1991, que tem por finalidade definir a política nacional de arquivos públicos e privados e exercer orientação normativa, visando à gestão documental e à proteção especial aos documentos de arquivo. Através da Câmara Técnica de Documentos Eletrônicos – CTDE que redigiu e elaborou o "Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil (2006)". Dentre os quais recomenda que um sistema informatizado no tocante da assinatura digital, a fim de garantir a confiabilidade e autenticidade das informações registradas em documentos eletrônicos, deve:

> a) ser capaz de garantir a origem e a integridade dos documentos com assinatura digital;
> b) somente administradores autorizados têm que ser capazes de incluir, remover, ou atualizar no sistema os certificados digitais de computadores ou de usuários;
> c) ser capaz de verificar a validade da assinatura digital no momento da captura do documento;
> d) no processo de verificação da assinatura digital, tem de ser capaz de registrar nos metadados do documento o seguinte: validade da assinatura verificada, a autoridade certificadora do certificado digital, data e hora em que a verificação ocorreu;
> e) ser capaz de armazenar juntamente com o documento as seguintes informações de certificação: assinatura digital, certificado digital (cadeia de certificação) usado na verificação da assinatura, Lista de Certificados Revogados – LCR;
> f) deve ser capaz de receber atualizações tecnológicas quanto à plataforma criptográfica de assinatura digital;
> g) deve destruir, ou tornar indisponíveis, as chaves de criptografia quando estas estiverem contidas em listas de certificados revogados (LCR);
> h) deve ter acesso a relógios e carimbador de tempo confiáveis para o seu próprio uso. O relógio gerador do selo de tempo deve ser sincronizado com o Observatório Nacional.

Por outro lado, a criptografia é um método de codificação de objetos digitais segundo um código secreto (chave), de modo que estes não possam ser apresentados por uma aplicação de

forma legível ou inteligível e somente usuários autorizados podem restabelecer sua forma original. Esta seção trata dos serviços de segurança apoiados em criptografia a fim de assegurar o sigilo das informações. É importante salientar que no uso de criptografia em documentos que apresentam longa temporalidade devem ser tomadas medidas administrativas para garantir a manutenção do sigilo e do acesso a esses documentos. Esses documentos não devem ser armazenados criptografados. Alguns fatores que comprometem a criptografia no longo prazo são: comprometimento ou obsolescência da chave, indisponibilidade do portador da chave e evoluções tecnológicas.

A palavra criptografia tem origem grega e significa a arte de escrever em códigos de forma a esconder a informação na forma de um texto incompreensível. A informação codificada é chamada de texto cifrado. O processo de codificação ou ocultação é chamado de cifragem, e o processo inverso, ou seja, obter a informação original a partir do texto cifrado, chama-se decifragem.

A cifragem e a decifragem são realizadas por programas de computador chamados de cifradores e decifradores. Um programa cifrador ou decifrador, além de receber a informação a ser cifrada ou decifrada, recebe um número chave que é utilizado para definir como o programa irá se comportar. Os cifradores e decifradores se comportam de maneira diferente para cada valor da chave. Sem o conhecimento da chave correta não é possível decifrar um dado texto cifrado. Assim, para manter uma informação secreta, basta cifrar a informação e manter em sigilo a chave.

Atualmente existem dois tipos de criptografia: a simétrica e a de chave pública. 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 e na decifragem, 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 cifrada.

Os algoritmos de chave pública 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.

Ainda em relação à criptografia, o CONARQ por meio do e-ARQ Brasil (2006) faz as seguintes recomendações ao que deve ter um sistema informatizado:

> a) Usar a criptografia no armazenamento, na transmissão e na apresentação de documentos arquivísticos digitais ao implementar a política de sigilo.
> b) Limitar o acesso aos documentos cifrados somente àqueles usuários portadores da chave de decifração.
> c) Registrar os seguintes metadados sobre um documento cifrado:
> _ indicação se está cifrado ou não;
> _ algoritmos usados na cifração;
> _ identificação do remetente;
> _ identificação do destinatário;
> _ Indicação da robustez ou grau de segurança da criptografia.
> d) Deve poder assegurar a captura de documentos cifrados, diretamente de uma aplicação de software que disponha da funcionalidade de cifração.
> e) Somente os usuários autorizados têm que ser capazes de realizar as seguintes operações:
> _ Incluir, remover ou alterar parâmetros dos algoritmos criptográficos instalados no sistema;
> _ Incluir, remover ou substituir chaves criptográficas de programas ou de usuários do sistema;
> _ Cifrar e alterar criptografia de documentos;
> _ Remover a criptografia de um documento. A remoção da cifração pode ocorrer quando a sua manutenção resultar em indisponibilidade do documento. Por exemplo, quando a chave de cifração/decifração estiver embarcada em hardware inviolável cuja vida útil está prestes a se esgotar ou quando o documento for desclassificado.
> f) No caso de remoção da cifração do documento, os seguintes metadados adicionais tem que ser registrados na trilha de auditoria:
> _ Data e hora da remoção da cifração;
> _ Identificação do executor da operação;
> _ Motivo da remoção da cifração.
> g) Deve possuir uma arquitetura capaz de receber atualizações tecnológicas quanto à plataforma criptográfica.

Em suma, o certificado digital é um documento eletrônico assinado digitalmente e cumpre a função de associar uma pessoa ou entidade a uma chave pública. As informações públicas contidas num certificado digital são o que possibilita colocá-lo em repositórios públicos. Um Certificado Digital normalmente apresenta as seguintes informações:

- nome da pessoa ou entidade a ser associada à chave pública
- período de validade do certificado
- chave pública
- nome e assinatura da entidade que assinou o certificado
- número de série.

Essas informações são os metadados, ou seja, são dados sobre dados, uma descrição informativa que identifica determinado documento. A parte descritiva do documento deve combinar com a indexação que é a atribuição de termos à descrição do documento, utilizando vocabulário controlado e/ou lista de descritores, tesauro e o plano de classificação dos documentos. O CONARQ (2006) argumenta que:

> A indexação dos documentos pode ser limitada à terminologia estabelecida no plano de classificação ou a outros controles adequados à complexidade dos documentos do órgão ou entidade, como tesauro ou vocabulário controlado. Vocabulário controlado é um conjunto normalizado de termos que serve à indexação e a recuperação da informação. Permite controlar a terminologia utilizada na indexação, estabelecendo os termos aceitos pelo órgão ou entidade e controlando o uso de sinônimos, homônimos, abreviaturas e acrônimos. O significado dos termos não é definido, mas apenas algumas relações entre eles, como, por exemplo, relação entre sinônimos. Um tesauro é uma lista controlada de termos ligados por meio de relações semânticas, hierárquicas, associativas ou de equivalência, que cobre uma área específica do conhecimento. Em um tesauro o significado do termo e as relações hierárquicas com outros termos são explicitados.

Portanto, foram abordados os conceitos, as tecnologias e os requisitos que fazem da certificação digital uma tecnologia que atribui autenticidade, integridade e confiabilidade aos documentos eletrônicos, proporcionando respaldo jurídico aos documentos digitais e que os mantém sob a forma digital.

AS POLÍTICAS PÚBLICAS DE CERTIFICAÇÃO DIGITAL

No Brasil, a legislação sobre documentos eletrônicos ainda é pouco abordada. Porém, segundo Santos (2005), em alguns momentos a citação sobre documentos eletrônicos na legislação brasileira é explícita, em outros não, mas a referência é constante. Um exemplo disso é a Lei 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados, onde define a necessidade de se preservar a acessibilidade dos documentos eletrônicos, em virtude da grande massa documental gerada sob a forma eletrônica. Assim sendo, o Art. 4º da referida lei explicita: Todos têm o direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos que serão prestadas no prazo da lei, sob pena de responsabilidade [...].

Ainda sobre a Lei 8.159/1991, o Art. 1º estabelece: É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação. É neste sentido, e buscando aferir validade jurídica aos documentos eletrônicos, que a Medida

Provisória Nº 2.200-2, de 24 de agosto de 2001, institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. A Medida Provisória (MP) 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.

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;
- Gabinete de Segurança Institucional da Presidência da República.

O Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG ICP-Brasil, instituído pela MP 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 Infra-Estrutura, vinculado à Casa Civil da Presidência da República. Ele tem por finalidade atuar na formulação e controle da execução das políticas públicas relacionadas à Infra-Estrutura 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 subsequente ao seu.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as Autoridades Certificadoras (ACs)

estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor.

Já às 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 a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às ACs 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.

Dessa forma, a Medida Provisória legitima as aplicações de certificação digital, o que gera consequências para a Arquivologia tanto no que cabe à Gestão Documental dos documentos não permanentes como à 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, conforme afirmação de Bodê (2006).

Assim sendo, o pensar arquivístico nacional não deve se restringir tão somente à gestão de documentos produzidos e acumulados da forma tradicional. Como também contemplar a gestão de documentos eletrônicos como realidade dos tempos atuais e, consequentemente, segundo Bodê (2006, p.17) "...as atividades relacionadas à classificação, descrição e preservação de documentos eletrônicos, levando-se em consideração as características próprias destes, como os metadados, devem ser levadas em consideração no fazer arquivístico", bem como a legislação sobre a política nacional de arquivos deve regulamentar leis concernentes à produção e acumulação de documentos eletrônicos, políticas de segurança de informações digitais e políticas para a preservação de documentos digitais.

OS PROJETOS DO RECIFE

O projeto Minha Certidão é uma realização da 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, que em 2008 lançou o Programa Minha Certidão. O objetivo do referido projeto 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. Os pais não precisam se deslocar até o cartório.

Os computadores instalados nas maternidades vão encaminhar os dados do declarante e a declaração de nascido vivo, que são escaneados e enviados pela internet para os cartórios. O registrador recebe o material, confere e gera a certidão de nascimento, assinada digitalmente com certificação digital da Autoridade Certificadora Certisign, que faz parte da ICP-Brasil, e reenvia para a maternidade. Dessa forma, a certidão é impressa e entregue aos responsáveis pelo recém-nascido. No que tange à conferência da assinatura digital, já vem um código impresso para ser conferido no sítio da internet do SERC, onde será possível verificar o certificado digital de qual oficial de cartório que aferiu fé pública ao documento.

No tocante à preservação e conservação digital das certidões, os analistas da ATI-PE informaram que as certidões são mantidas sob formato de arquivo de fácil manipulação, leve e perene. Assim como são realizadas diariamente cópias de segurança nos servidores onde as informações estão contidas.

Outro programa de destaque é o projeto Nota Fiscal Eletrônica (NF-e), que é coordenado pelo ENCAT (Encontro Nacional dos Administradores e Coordenadores Tributários Estaduais) e desenvolvido em parceria com a Receita Federal do Brasil e tem como finalidade a alteração da sistemática atual de emissão da nota fiscal em papel por nota fiscal eletrônica com validade jurídica para todos os fins.

Tem como objetivo a implantação de um modelo nacional de documento fiscal eletrônico que venha substituir a sistemática atual de emissão do documento fiscal em papel, com validade jurídica garantida pela assinatura digital do remetente, simplificando as obrigações acessórias dos contribuintes e permitindo, ao mesmo tempo, o acompanhamento em tempo real das operações comerciais pelo Fisco.

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).

Portanto, foram ilustradas duas aplicações de certificação digital no Recife e mudança na forma de produção e preservação de documentos. O que leva ao desenvolvimento de políticas de preservação de documentos sob a forma digital.

CONSIDERAÇÕES FINAIS

Como se pôde observar, a certificação digital é uma realidade que está revolucionando o aspecto jurídico dos documentos eletrônicos. O que antes não tinha nenhum valor legal, hoje as tecnologias da informação encontraram soluções para viabilizar a segurança das informações e atribuir confiabilidade, autenticidade e inalterabilidade aos documentos digitais.

Porém, o que desperta apreensão é como esses programas serão conduzidos para a perpetuação dessas informações registradas em suportes digitais e quais políticas serão estabelecidas para a preservação do patrimônio arquivístico digital. No futuro, os atuais Arquivos Históricos serão grandes Arquivos Tecnológicos, onde os pesquisadores ao invés de consultarem aqueles documentos amarelados e envelhecidos pelo tempo, nessa nova perspectiva irão realizar suas consultas em computadores, bem como poderão até salvarem essas informações digitais em mídias apropriadas. Mas, para isso, deve haver legislações que assegurem o estabelecimento de políticas sobre migrações digitais e infraestruturas com potentes formas de segurança digital.

Um aspecto relevante das atuais políticas públicas que estabelecem a certificação digital no Brasil é que o documento em formato digital possui valor jurídico, uma vez que a autenticidade dele é posta em prova através dos *softwares* de navegação da Internet. Dessa forma, a confirmação da autenticidade e integridade do certificado digital é realizada instantaneamente pelas Autoridades Certificadoras digitais. No que tange aos programas de certificação digital em desenvolvimento no Recife e citados nesta comunicação, ressalta-se o programa Minha Certidão, que apresenta uma metodologia própria e que faz uso da infraestrutura de chaves públicas, e se configura como um exponencial programa de Certificação Digital no cenário nacional e contribui para a socialização do acesso ao primeiro documento da cidadania brasileira. Por outro lado, o programa de notas fiscais eletrônicas do Governo Estadual em parceria com a Receita Federal que está sob os moldes da infra-estrutura de chaves públicas brasileiras é outra iniciativa que otimiza o fisco nas auditorias fiscais e agiliza os negócios comerciais.

Dessa forma, a certificação digital no Brasil carece de políticas públicas mais específicas para o uso e consolidação de assinaturas digitais em documentos eletrônicos na atualidade. O que se observou nos programas de certificação digital do Recife são aplicações que auxiliam na agilização dos processos de produção de documentos, consultas e acesso às informações.

Portanto, os profissionais que labutam pela preservação da memória cultural da nossa sociedade devem acompanhar essas transformações das formas de produção e acumulação de informações, bem como pensar e participar da construção de políticas públicas para salvaguarda de documentos digitais. Uma vez que a certificação digital está mantendo as futuras fontes históricas em formatos digitais, e, portanto, devem-se estabelecer formas em que essas

informações sejam armazenadas, organizadas, recuperadas e disponibilizadas, garantindo assim o direito democrático e cultural de acesso às informações de cada cidadão brasileiro.

DIGITAL MEMORY: APPLICATIONS OF DIGITAL CERTIFICATION

Abstract:
The present communication has for purpose to identify to applications and developed public politics of digital certification in the city of Recife, in order to understand the new supports of the information that will conserve the memory of the current society. For in such a way, they are boarded concepts, technologies of the information and requirements on digital certification, the public politics regarding the subject, the Infrastructure of Public Keys Brazilian - ICP-Brazil, as well as the description of two applications of digital certification in development in Recife. In the end some proposals on the panorama of the digital certification in Recife and suggestions of what it must be made to preserve the digital memory.

Keywords: Digital certification. Digital memory. Public technology of the information. Public politics. Authenticity of the digital information.

REFERÊNCIAS

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: 09 dez. 2009.

CARTILHA certificação digital. São Paulo: Associação dos Registradores Imobiliários de São Paulo, [200-?]. Disponível em: <https://www.oficioeletronico.com.br/Downloads/Cartilha CertificacaoDigital.pdf > Acesso em: 02 jun. 2009.

CONSELHO NACIONAL DE ARQUIVOS. **Carta para a Preservação do Patrimônio Arquivístico Digital Preservar para garantir o acesso.** Rio de Janeiro: Conarq, 2004. Disponível em: <https://www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm.> Acesso em: 30 ago. 2009.

_____. Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil). Rio de Janeiro: Conarq, 2006. Disponível em: https:// www.conarq.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm. Acesso em: 30 ago. 2009.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Estrutura da ICP-Brasil**. Brasília: ITI, [200-?]. Disponível em: < http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp >. Acesso em: 25 ago. 2009.

PERNAMBUCO. SECRETARIA DA FAZENDA. **NFe – Nota Fiscal Eletrônica** Recife, 200-. Disponível em: <http://www.sefaz.pe.gov.br/sefaz2/asp2/mostra.asp?pai=1040> Acesso em: 02 jun. 2009.

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

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

SANTOS, Vanderlei Batista dos. **Gestão de documentos eletrônicos**: uma visão arquivística. 2. ed. rev. aum.. Brasília: ABARQ, 2005.

SARACEVIC, T. Ciência da Informação: origem, evolução, relações. Perspectivas em Ciência da Informação, Belo Horizonte, v.1, n.1, p. 41-62, 1996.

TRIBUNAL DE JUSTIÇA DE PERNAMBUCO. Minha Certidão: software pernambucano é modelo nacional. Recife: TJPE, 2009. Disponível em: <http://www.direito2.com.br/tjpe/2009/abr/15/minha-certidao---software-pernambucano-e-modelo-nacional> Acesso em: 02 jun. 2009.