ASSINATURA DE DOCUMENTOS ELETRÔNICOS UTILIZANDO CERTIFICADOS DIGITAIS: Estudo de caso de assinaturas digitais aplicadas em atas de reuniões.[1]

VIEIRA, Renato Melo *
ARAÚJO, Wagner Junqueira de**

Resumo:
A necessidade de se manter as informações em segurança é tão antiga quanto a própria informação. No passado, imperadores colocavam guardas para proteger documentos oficiais e as igrejas mantinham seus documentos guardados a sete chaves. Com a explosão no uso dos computadores, os documentos ganharam o formato digital, e a internet passou a ser um grande veículo disseminador desse novo formato. Quanto maior o número de pessoas com acesso a determinada informação, maior sua vulnerabilidade. Com tanta informação circulando a velocidades de um clique, não demorou muito para que houvesse a necessidade de se ter ferramentas capazes de autenticar, dar integridade, confidencialidade, disponibilidade e para certos tipos de documentos o não repúdio ou irretratabilidade da ação ou autoria de um ato nos documentos digitais. O presente trabalho objetiva investigar assinaturas em documentos eletrônicos com chaves criptográficas assimétricas, utilizando certificados digitais gerados e gerenciados por em softwares livres ou gratuitos, que possibilitem garantir sua autenticidade. Utilizou-se uma abordagem experimental em conjunto com o método "multicritério de análise de decisão" (MMAD) para avaliação das ferramentas estudadas. O estudo constatou que todas as ferramentas analisadas possuem a funcionalidade de assinar documentos eletrônicos. No entanto, possuem diferenças quanto ao tipo de extensão usada, o idioma, tipo de licença, se usa de múltiplas assinaturas e na solicitação de senha ao assinar.

Palavras- chave: Assinatura Digital. Certificado Digital. Documento Eletrônico.

[1]Comunicação Oral apresentada ao GT 06 – Tema Livre.

* Universidade Federal da Paraíba. Graduando do Curso de Biblioteconomia. rmvrenato@hotmail.com
**Universidade Federal da Paraíba. Profº Dr. do Departamento de Ciência da Informação – DCI wagnerjunqueira.araujo@gmail.com

1 INTRODUÇÃO

Segundo a *Organisation for Economic Co-operation and Development* - OECD (1996), as economias são baseadas cada vez mais no conhecimento e na informação. O conhecimento é reconhecido como um agente da produtividade e do crescimento econômico, conduzindo a um novo foco no papel da informação, da tecnologia e do aprendizado no desempenho econômico. O termo "*knowledge-based economy*" é definido pela OECD como uma economia na qual a criação e o uso do conhecimento está no centro das decisões e do crescimento econômico. Essa nova sociedade contempla a evolução da sociedade industrial, com uma característica marcante: o acesso à informação, considerada a matéria-prima fundamental para o desenvolvimento. Para autores como: Masuda (1982), Dertouzos (1997) e Castells (1999), a sociedade da informação seria a próxima fase da evolução econômica da sociedade pós-industrial.

Moore (1997) apresenta três características principais da sociedade da informação. Primeiramente, a informação é usada como um recurso econômico. As organizações usam da informação para aumentar sua eficiência, estimular a inovação e aumentar sua eficácia e sua competitividade, freqüentemente com melhorias na qualidade dos bens e serviços que produzem. Há também uma tendência para o desenvolvimento das organizações de informação - o uso da informação agrega maior valor e beneficia assim a economia de um país. Segundo, é possível identificar maior uso da informação entre o público geral. As pessoas utilizam a informação de forma mais intensiva em suas atividades como consumidores: para suas escolhas entre produtos diferentes, para explorar seus direitos e deveres junto aos serviços públicos, e com maior controle em suas próprias vidas, além disso, os sistemas de informação estão sendo desenvolvidos de forma a estender o acesso à educação e à cultura. A terceira característica da sociedade da informação é o desenvolvimento do setor da informação dentro da economia, com a função de satisfazer à demanda geral por serviços de informação. Uma parte significativa é centrada na infra-estrutura tecnológica: as redes das telecomunicações e de computadores, com isso a informação passa a ser produzida e distribuída em formato eletrônico.

Para ilustrar o volume da informação distribuída em formato eletrônico que está disponível na internet em abril de 2010, ao realizar uma rápida pesquisa em páginas Web, buscando identificar o número de páginas indexadas por um motor de busca que estão publicadas em sites hospedados no Brasil, neste caso, o Google. O motor de busca Google permite que se realize buscas de páginas sua base, pela sua identificação dos sites *URL*1, ou por parte desta, usando para isso o comando "site: nomedosite". Em uma busca aplicando como parâmetro de entrada (site:*.*.br), sendo que, a extensão ".br" nas *URL* dos sites indicam o pais (nesta exemplo o Brasil) onde este foi registrado e supostamente onde site está hospedado. Como resultado o motor de busca retornou mais de 2 milhões e 310 mil páginas indexadas. É sabido que esse volume cresce de forma vertiginosa, impulsionado por diferentes fatores, como: o acesso cada vez maior à internet, a familiarização das pessoas com as tecnologias, redução dos preços de equipamentos e serviços entre outros.

Dados do *Internet World Stats2*, contabilizam 360,985,492 de usuário da Web em todo mundo, com uma taxa de crescimento de mais de 399% no período de 2000 à dezembro de 2009, que indica o crescimento e utilização destas tecnologias. Todavia, devemos considerar que estes usuários, não são apenas consumidores de informação, mas potenciais criadores e disseminadores. Tal crescimento da utilização destas tecnologias vem criando uma dependência social da informação digital, para o CONARQ (2004) "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".

Contudo, a utilização de novas tecnologias, traz novos riscos. A OECD (2006, p.9) adverte que com o desenvolvimento das tecnologias da informação e comunicação, das redes, em particular a Internet, criou-se um conjunto emergente de novos tipos de ações maliciosas chamadas *cybercrimes*. De acordo com o Centro de Tratamento de Incidentes – Cert.br (BRASIL, 2006, p.13), existem diversos riscos envolvidos no uso da Internet, associados aos programas leitores de *e-mails*, navegadores *(browsers*), programas de troca de mensagens, de distribuição de arquivos e recursos para compartilhamento de arquivos. Saber se um documento eletrônico é original ou não, se sofreu alterações, se foi acessado por pessoas de forma indevida, passam a fazer parte das discussões. O que nos leva ao seguinte **problema**: como garantir a autenticidade em documento eletrônico? A proposta deste projeto tratou esta questão, por meio da aplicação de tecnologias de informação e segurança da informação, que podem possibilitar a autenticidade em documentos eletrônicos.

A autenticidade em documentos eletrônicos pode ser obtida através da utilização de tecnologias de certificados digitais, oriundos de uma infra-estrutura de chaves públicas – ICP, que no Brasil possui legislação específica que trata deste assunto definida por meio da MP 2200-2 de 2001. Os procedimentos que permitem garantir a autenticidade de documentos eletrônicos por meio de assinatura digital poderão ser aplicados a um caso de uso prático, nesta proposta, para assinatura das atas de reuniões realizadas pelo colegiado do Departamento de Ciência da Informação – DCI do Centro de Ciências Sociais Aplicadas – CCSA da Universidade Federal da Paraíba – UFPB.

1.1 OBJETIVO GERAL E ESPECÍFICOS

Assinar documentos eletrônicos com chaves criptográficas assimétricas, utilizando certificados digitais gerados e gerenciados por softwares livres ou gratuitos, que possibilitem garantir sua autenticidade.

Para atingir nosso objetivo geral, estabelecemos os seguintes objetivos específicos:

- Promover o treinamento de pesquisador-aprendiz nas tecnologias de certificação e assinatura digital.
- Identificar na literatura ferramentas de software de geração, gerenciamento e assinatura de documentos eletrônicos, com as características necessárias para implementação do projeto.
- Selecionar por meio de metodologia específica as ferramentas de software necessárias para implementação do projeto.
- Produzir documentação de instalação e manuais com os procedimentos para assinatura digital em documentos eletrônicos.
- Divulgação dos documentos e procedimentos elaborados, em seminário e pela Internet no portal do Laboratório de Tecnologias Intelectuais - LabT*i3.*

2 SEGURANÇA DA INFORMAÇÃO

Antes da explosão na utilização dos computadores os documentos tinham como principal suporte o papel, mas com a crescente demanda e uso dos recursos computacionais, é cada vez mais utilizado o formato digital. O registro das informações neste novo formato faz com que tais

informações possam estar disponíveis aos seus usuários com uma maior rapidez e praticidade. contudo essas mudanças necessitam de mecanismos que garantam a segurança destas informações, logo, por isso surgiu a necessidade de se criar procedimentos e ferramentas que garantam a proteção da informação, por meio da integridade, confidencialidade e disponibilidade nestes novos suportes.

De acordo com Ferreira (2008) A Segurança da Informação tornou-se um dos temas importante dentro das organizações, devido às fortes necessidades de proteção das informações e grande dependência de Tecnologia da Informação.

> [...] O Entendimento daquilo que precisa ser protegido está além do simples hardware e software que compõem os sistemas, abrangendo, também, as pessoas e os processos de negócio. Deve-se considerar o hardware, software, dados e documentação, identificando de quem esses elementos necessitam ser protegidos. Nesta análise, aspectos sobre a segurança dos dados, backup, propriedade intelectual e respostas a incidentes devem ser levados em consideração. (FERREIRA 2008)

2.1 DOCUMENTO ELETRÔNICO

É essencialmente necessário antes de assinar ou validar um documento entender a tipologia do mesmo, ou seja, se é um documento físico também chamado documento de arquivo, ou se é um documento eletrônico, (suporte digital). A Resolução CONARQ nº 20, de 16 de julho de 2004 faz considerações aos dois tipos de documentos citados.

Os Procedimentos a serem analisados antes do processo de assinatura são: conceitos, características, diferenças e semelhanças.

> Considera-se documento arquivístico como a informação registrada, independente da forma ou do suporte, produzida e recebida no decorrer das atividades de um órgão, entidade ou pessoa, dotada de organicidade e que possui elementos constitutivos suficientes para servir de prova dessas atividades. (CONARQ 2004 §1º)

> Considera-se documento arquivístico digital o documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional. São exemplos de documentos arquivísticos digitais: planilhas eletrônicas, mensagens de correio eletrônico, sítios na internet, bases de dados e também textos, imagens fixas, imagens em movimento e gravações sonoras, dentre outras possibilidades, em formato digital. (CONARQ 2004 §2º)

Um documento de arquivo é gerado no curso de uma atividade prática e serve como fonte de prova da ação que o gerou, sendo que o valor desta fonte depende da fidedignidade e autenticidade do documento. O texto publicado pelo CONAR(2004b)

> Um Documento Eletrônico é composto por uma seqüência de bits cujo conteúdo só pode ser revelado com o auxílio de uma plataforma computacional. (Scheibelhofer, 2001).

> O Documento eletrônico apresenta características específicas que não estão presentes no documento tradicional em papel. No Documento em papel tem-se

> acesso direto ao conteúdo sem auxílio de equipamentos. Os eletrônicos por sua vez, estão armazenados na forma de um conjunto de bits formatada segundo algum padrão de representação para um formato mais apropriado a compreensão humana. O Documento visualizado deve ser único independente da plataforma de software utilizados nesta transformação e expressar fielmente seu conteúdo de acordo com a vontade do assinante. (CUSTÓDIO 2003, pag.10)

2.2 ASPECTOS JURÍDICOS DO DOCUMENTO

Nossa sociedade vive desde a metade do século passado uma mudança na forma de criar, armazenar, circular e validar os documentos produzidos. Seria uma espécie de revolução silenciosa, mas que acontece de forma rápida e gigantesca. Para acompanhar essa nova realidade, é preciso que os meios jurídicos possam repensar os velhos dogmas para poder encarar essa nova realidade.

É preciso entender que o computador desempenha um papel de intermediador nesse avanço, e esse instrumento quem possibilitou novas descobertas em todas as áreas do conhecimento.

Seja pelos avançados editores de textos, onde aposentaram de vez a velha máquina de escrever, ou mesmo assumindo papéis antes desempenhados apenas por seres humanos, a exemplos dos caixas eletrônicos nos bancos, é inegável a importância desses equipamentos em nossas vidas. Para coroar essa importância, não poderíamos deixar de falar também da internet, pois quase tudo que é produzido localmente nos computadores, cabe a ela intermediar essa comunicação, desempenhado um papel singular para nossa sociedade. A internet é sem dúvida um dos meios de comunicação mais completos já vistos pelo homem.

Tamanha importância do computador nas nossas vidas, a legislação atual não pode jamais enxergar esse equipamento como uma máquina qualquer, onde apenas é composta por hardwares e softwares. Nesse sentido, aqui no Brasil já foram feitas algumas alterações na legislação e outras estão em tramitação no congresso visando regulamentar e respaldar o uso dessas novas tecnologias.

> [...] o direito não pode ser alheio a tal realidade, e nem se isolar dos meios eletrônicos. Assim como tem em mente os documentos escritos manualmente, a expressão “documento eletrônico” deve ser entendida como válida e como algo representativo de um fato, mesmo que esse venha ser imortalizado em um novo suporte. (LIMA NETO)

Na verdade, as mudanças ainda em análise e as mudanças que já ocorreram na lei, refletem uma tendência mundial já vivemos em um mundo globalizado e tais mudanças visam harmonizar e ou equiparar as nossas leis com as já existentes em outros países, onde o uso e a validade dos meios eletrônicos estão legitimados a vários anos.

2.3 SEGURANÇA EM DOCUMENTOS

Junto com a vulnerabilidade do novo suporte, veio a preocupação com riscos de fraudes. Estudiosos foram em busca tecnologias que pudessem garantir a validade de um documento eletrônico, e em 1976, Diffie e Hellman desenvolveram uma tecnologia capaz de resolver com êxito os problemas de segurança nas redes de computadores, foi criada assim a criptografia.

A criptografia possibilita os recursos necessários que garantam os seguintes serviços: Autenticidade, Integridade, Confidencialidade e a Irretratabilidade.

A primeira forma de criptografia foi a Simétrica, desempenhava o papel de cifrar ou ocultar dados sigilosos. Posteriormente surgiu a criptografia assimétrica, também conhecida como **chave pública** e **chave privada.**

A criptografia provê recursos para garantir os seguintes serviços:

- **Autenticação:** Garante a origem da informação, permitindo sua comprovação;
- **Integridade:** Assegura a veracidade e a integridade da informação recebida;
- **Confidencialidade:** Garante o acesso às informações somente pelas pessoas autorizadas;
- **Irretratabilidade:** Assegura que a origem (o emissor) da mensagem não poderá negar que foi o autor de determinada mensagem.

Nos países mais desenvolvidos, a certificação digital começou a ser usada na década de 80 e o Brasil precisava adequar sua legislação visando se adequar o que vinha sendo usado por outros países.

2.4 CERTIFICAÇÃO DIGITAL

Os certificados digitais, também chamados de identidade digital, é uma arquivo de computador capaz de identificar dados de um indivíduo ou entidade, possuindo chaves para fazer a certificação.

A certificação digital usa a criptografia para cifrar e decifrar as assinaturas, são usadas dois tipos de chaves no processo de assinaturas digitais, Uma Chave Pública que é armazenada no certificado e a outra chave é denominada Chave Privada que é guardada sigilosamente pelo assinante. Qualquer mensagem o código pode ser assinado utilizando-se a Chave Privada do assinante, porém esta assinatura só será validada pela com a chave pública correspondente

O processo de certificação digital sugere cincos aspectos básico a serem considerados fundamentais para confiança de uma assinatura digital.

- Confiança;
- Integridade;
- Confiabilidade;
- Não repúdio;
- Autorização.

2.5 AUTORIDADES CERTIFICADORAS

Denomina-se autoridades certificadoras entidades ou empresas com alto nível de confiança e reputação, elas emitem certificados digitais para outras entidades, empresas e indivíduos, que precisam se identificar e garantir as suas operações no mundo digital.

2.6 AUTORIDADES DE REGISTRO

Denomina-se autoridade de registro uma empresa ou uma entidade responsável pela verificação das informações fornecidas pelos requisitantes dos certificados.

2.7 A CERTIFICAÇÃO DIGITAL NO BRASIL

No ano de 2001, o governo brasileiro começou estudar formas de regulamentar o uso de certificados digitais no país com objetivo de usá-los nas transações online entre os vários órgãos públicos e seus fornecedores. A idéia era dar valor legal, permitindo maior agilidade no processo de compras e a diminuição de custos com uso, gerenciamento e armazenamento de documentos oficiais sigilosos ou não sigilosos.

A ICP-Gov teve origem a partir da Medida Provisória 2.200-2, de 24 de outubro de 2001, posteriormente se expandiu e transformou-se na ICP-Brasil. A ICP-Brasil é a atual estrutura hierárquica de autoridades certificadoras ligadas ao governo brasileiro. Somente as transações realizadas com certificados emitidos por autoridades credenciadas na ICP-Brasil têm validade jurídica reconhecida no país.

2.8 ASSINATURAS DIGITAIS EM DOCUMENTOS ELETRÔNICOS

Com o avanço no uso das tecnologias a informação passou também a ser produzida e disponibilizada em formato digital, essa nova forma de armazenamento teve um enorme crescimento nas últimas décadas.

Nos documentos de arquivo são as assinaturas manuscritas e os carimbos que validam sua autoria, autenticidade e integridade, já os documentos eletrônicos começavam a ser usados em larga escala e com o crescimento, surgiram os riscos eminentes de fraudes nesse novo suporte, essas assinaturas que antes eram feitas a mão, precisavam ganhar também sua forma ou um formato digital, para garantir que os mesmo não fossem violados.

Ao assinar um documento de papel firma-se que o mesmo é integro e autêntico. Para CUSTÓDIO 2003, o ato de assinar um documento estabelece um vinculo entre quem assina e o documento em si. Essa ligação acontece tanto na forma manuscrita como na forma digital, porém no caso da assinatura digital essa ligação entre o documento e o autor é feita por um algoritmo de autenticação. Tanto as assinaturas manuscritas quanto as assinaturas digitais estabelecem os mesmos objetivos e finalidades, a de possibilitar ao criador que o documento criado não seja alterado ou violado.

A assinatura digital é uma modalidade de assinatura eletrônica, é o resultado de uma operação matemática que utiliza algoritmos de criptografia assimétrica, denominadas chaves criptográficas e permite aferir, com a segurança, a autenticidade do documento.

> O ato de assinar um documento no papel está efetivando a ligação entre a assinatura propriamente dita e a informação impressa no papel. Na assinatura manuscrita existe uma ligação entre a pessoa que assina e o documento [...]. Uma assinatura digital é uma algoritmo de autenticação, que possibilita ao criador de um objeto unir ao objeto criado, um código que irá agir como assinatura [GUI 00]. Esta assinatura confirma que o objeto não foi alterado, desde o ato de sua assinatura e permite identificar o assinante [...]. (MONTEIRO, 2007, pag.10.)

A assinatura digital comprova que a pessoa é o autor o concorda com o documento assinado digitalmente, assim como assinar na forma manuscrita garante a autenticidade, do mesmo modo quando aplicada a um documento a assinatura eletrônica permite a verificação de sua integridade ao passo que estabelece uma imutabilidade lógica do conteúdo do documento subscrito.

> A verificação de Assinatura Digital determina se ela Foi criada pela Chave Privada correspondente a Chave Pública listada no certificado do signatário e se a mensagem

> associada não foi alterada desde a criação da Assinatura Digital. A pessoa ou entidade que confiar em uma assinatura que não possa ser confirmada ou que venha a ocorrer falhas na verificação da assinatura, estará assumindo todas as responsabilidades de riscos e se isentando de qualquer direito em relação ao uso da assinatura. (MONTEIRO, 2007, pag. 90)

As atas que antes eram feitas em documentos de arquivos, são lavradas normalmente ao término de cada reunião, e com o avanço e à expansão dos computadores e das redes, elas começaram ganhar a forma digital. Hoje as reuniões podem ser feitas usando inclusive a teleconferência, onde os participantes podem participas podem estar em outras cidades, estados ou até mesmo outros países.

Pode-se perceber que o assunto estudado tem poucas pesquisas realizadas anteriormente, e as pesquisas já existentes sobre certificação e assinaturas digitais são voltadas em sua maioria para redes de computadores e caixas de e-mail.

Durante a pesquisa, foram testados 12 (doze) ferramentas assinadoras, onde foram separados, classificados e pontuados usando os seguintes critérios: Múltiplas assinaturas, Idioma, licença, Exigência de senha para validar uma assinatura.

3 PROCEDIMENTOS METODOLÓGICOS

Definir qual deve ser a abordagem, o método, as técnicas e as ferramentas que serão empregadas em uma investigação científica não é uma tarefa trivial. A escolha de determinada ferramenta ou técnica pode auxiliar ou inviabilizar a realização da pesquisa. Até a opção pelo tipo de pesquisa e sua caracterização é uma tarefa que deve ser considerada cuidadosamente pelo pesquisador.

O Trabalho aqui relatado constitui um estudo de caso sobre ferramentas que possibilitem assinar documentos eletrônicos usando chaves criptográficas assimétricas, disponíveis em certificados digitais gerados. A proposta deste trabalho foi estudar softwares livres ou gratuitos, que possibilitem emitir certificados digitais, gerenciá-los e assinar documentos digitais, seguindo os padrões sugeridos pela ICP-Brasil.

O “objetivo fundamental da pesquisa é descobrir respostas para problemas mediante o emprego de procedimentos científicos” (GIL, 1999, p. 42). Esses procedimentos compõem o método científico.

Segundo Godoy (2006) o estudo de caso deve estar centrado em uma situação ou evento particular cuja importância vem do que ele revela sobre o fenômeno objeto da investigação. Essa especificidade torna o estudo de caso um tipo de pesquisa especialmente adequada quando se quer focar problemas práticos, decorrentes das intrincadas situações individuais e sociais presentes nas atividades, nos procedimentos e nas interações cotidianas. (GODOY, 2006, p.121)

Esta pesquisa se enquadra neste cenário, pois visa estudar um evento em particular e foca um problema prático identificado na literatura e aplicado às organizações. Para Yin (2005), um estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos. (YIN, 2005, p.32)

Esta pesquisa estuda um fenômeno contemporâneo, que trata da segurança e autenticidade de documentos digitais.

Segundo Godoy (2006, p. 124), o estudo de caso pode ser: descritivo, interpretativo e avaliativo. Para o autor denomina-se estudo de caso avaliativo quando a preocupação é gerar dados e

informações obtidos de forma cuidadosa, empírica e sistemática, com o objetivo de apreciar o mérito e julgar os resultados e a efetividade de um programa. (GODOY, 2006, p.125)

Estaremos desenvolvendo neste projeto um estudo de caso, aplicado em atas de reuniões geradas no Departamento de Ciência da Informação - DCI da UFPB. Esta opção é referenciada por diferentes autores (RICHARDSON, 1999; RÉVILLION, 2001; SILVA E MENEZES, 2001).

3.1 MÉTODO MULTICRITÉRIOS DE ANÁLISE DE DECISÃO

Dentro das atividades propostas neste projeto, uma delas implica na seleção de determinadas ferramentas de software, para isso optamos por aplicar um método multicritério de análise de decisão. Segundo VILLAS BOAS (2010) “os métodos multicritérios de análise de decisão (MMAD) aparecem como uma opção para consecução desse propósito. Eles provêem um maior entendimento do contexto multidisciplinar do processo decisório”.

Os modelos de processos decisórios de problemas multicriteriais têm como finalidade apresentar uma lista ordenada das alternativas para solução de um problema, de acordo com as preferências dos decisores, ou selecionar, entre todas alternativas, a solução que melhor satisfaça os objetivos dos decisórios (VILLAS BOAS, 2006).

Estas técnicas podem, por conseguinte, “ser utilizadas para: (a) identificar a melhor opção, (b) ordenar as opções, (c) listar um número limitado de alternativas para uma subseqüente avaliação detalhada, ou (d) simplesmente distinguir as possibilidades aceitáveis das inaceitáveis” (VILLAS BOAS, 2006). Considerando os objetivos e definidos os critérios necessários para a solução do problema, é possível utilizar as técnicas de decisão multicritério para sua resolução. Os passos podem ser assim indicados: definição de pesos para os critérios, normalização e combinação dos critérios, onde são atribuídos pesos aos critérios identificados, que por sua vez podem ser tabulados por meio de software apropriado (GOMES, 1998; VILLAS BOAS, 2006).

Para visualizar a análise utilizada para pesquisa, abaixo um quadro com critérios estabelecidos.

Quadro 1 - Critérios utilizados na pesquisa

Critérios	**Descrição**	**Pontos**
Múltiplas assinaturas	Funcionalidade que permite ao usuário assinar um mesmo documento com diferentes certificados digitais, sem que ocorra a perda da assinatura anterior.	Sim = 10 Não = 03
Idioma	Esse critério visa eliminar ou diminuir as barreiras lingüísticas entre o usuário e o softwares.	Português = 10 Espanhol = 06 Inglês = 05 Outros = 00
Licença	Compreende o que é autorizado ou proibido, são os direitos de um autor sobre o software. É o tipo de	GNU/GPL(Livre) = 10

	licença que determina se o software é livre ou gratuito ou se a licença é paga.	Gratuita = 07 Trial (Teste) = 02
Restrição por Senha	Valida senha do certificado para efetuar a assinatura digital	Sim = 10 Não = 00
Formato	É o tipo de formato digital que o software é capaz de assinar.	.PDF = 10 .Doc,.Docx = 07 .ODT = 07 .RTF = 03 Outros = 01
Proteção de Conteúdo	Após assinado, o certificado bloqueia o documento de novas alterações.	Sim = 10 Não = 03

Fonte: Dados da pesquisa, 2011.

3.2 SOFTWARES ANALISADOS

Adobe Acrobat: Com oAdobe Acrobat 9 Pro é possível tanto criar um certificado digital quanto assinar um documento. O software é multilinguagem e pode ser baixado no site http://superdownloads.com.br , uma versão para teste (trial) com vaidade de 30 (trinta) dias. Nessa versão também é possível gerar múltiplas assinaturas.

Office 2007: O Word Officce 2007 traz como novidade a assinatura digital, nele é possível assinar um documento em formato .DOCX, sem que o mesmo possa ser alterado. O ponto fraco desse software como assinador é quando o documento precisa ser exportado, pois ao exportar um documento na extensão .PDF o Office 2007 não exporta junto os certificados, isso acontece até mesmo quando o documento é salvo na versão anterior do frabricante, ou seja, a versão .DOC não é possível manter os certificados, sendo inclusive possível alterar o documento. A versão Word Office 2007 pode ser baixado para teste por 30 (trinta) dias no site http://www.pcworld.com/downloads/file/fid,64414-order,1-page,1/description.html .

Open Office: Sob licença GNU/GPL, o Open Office é um software totalmente livre. Com ele é possível assinar documentos no formato .ODT, mas o software tem a fragilidade de não exportar o certificado quando o documento é gerado em .PDF e não solicita senha para assinar.

PDF Creator: O software tem licença gratuita, pode ser baixado em diversos sites entre eles o http://baixaki.com.br. Gera e assina PDF, pode ser encontrado no idioma português, mas não permite fazer múltiplas assinaturas.

Expert PDF7: A versão 7 do ExpertPDF tem licença para teste (Trial) por 30 (trinta) dias. Pode ser baixado no http://baixaki.com.br. Com ele é possível gerar certificados e fazer múltiplas assinaturas, após os trinta dias a licença gratuita expira e é necessário adquirir versão "Full" que é paga.

DigiSigner: Essa ferramenta solicita a senha somente ao carregar o certificado. Necessário instalar o certificado com nível alto de segurança inserindo a senha.

JSignPdf: É um software de licença GNU/GPL (livre) pode ser baixado no http://busca.superdownloads.com.br/busca/jsignpdf_3A.s1.html . Tem uma boa interface, mas está disponível apenas na língua inglesa.

DeskSigner: Gratuito para testar, o permite assinar arquivos eletrônicos, isoladamente ou em lotes. A co-assinatura é permitida em arquivos que foram previamente assinados, não havendo limites para a quantidade de assinaturas. Pode ser baixado para teste no site: http://www.baixaki.com.br/download/desksigner.html.

PDF Sign&Seal: É uma ferramenta de licença paga, podendo ser baixado no site http://www.ascertia.com/Downloads.aspx, uma versão para (Trial) para teste. É disponível na língua inglesa.

ARISP: Esse software permite a verificação de assinatura no padrão PKCS#7 e é gratuito (freeware). Foi desenvolvido baseado na legislação brasileira de certificação. A verificação dos arquivos assinados digitalmente se dá de forma natural, sendo o arquivo exibido juntamente com as assinaturas digitais e o chancelamento eletrônico. Basta efetuar um duplo-clique sobre um arquivo assinado (*.p7s, *.p7b, *.dca, *.sig) para que ele possa ser verificado e exibido. Pode ser baixado no site: http://www.arisp.com.br .

XSign Corporate: O XSign Corporate é um software de assinatura digital. Pode ser baixado a versão para teste no site http://www.superdownloads.com.br/download/71/xsign-corporate .

Quadro 2 - ferramentas de software para assinatura digital analisadas

Software	Mult. Assin.	Idioma	Licença	Usa senha	Protege	Formato	Pontos
Open Office	03	10	10	0	03	7	33
Office 2007	10	10	2	0	10	7	39
DigiSigner	10	5	7	0	10	10	42
Expert PDF	10	5	2	10	10	10	47
PDF Sign&Seal	10	5	2	10	10	10	49
PDFCreator	03	10	7	10	10	10	50
Adobe Acrobat	10	10	2	10	10	10	52
DeskSigner	10	10	2	10	10	10	52
XSign Corporate	10	10	2	10	10	10	52
JSignPdf	10	5	10	10	10	10	55
ARISP	10	10	7	10	10	10	57
OKey	10	10	7	10	10	10	57

Fonte: Dados da pesquisa, 2011.

4 CONSIDERAÇÕES FINAIS

Os certificados foram criados no Adobe Reader, seguindo o formato PKCS#12 que gera um arquivo com extensão.pfx. Este formato e equivalente ao tipo A1 da ICP-Brasil, estes certificados tipo A1 são gerados em seu computador, e dispensa o uso de cartões inteligentes ou tokens. Aconselha-se para como procedimentos de segurança, que no momento de sua criação optar protegê-lo com uma senha de acesso e que se faça uma cópia de segurança. Pela ICP-Brasil este tipo de certificado possui validade de 12 meses em virtude de sua fragilidade, contudo verificou-se que as ferramentas utilizadas para gerar os certificados de teste, que estes podem ser criados com validade de até cinco anos.

Para validar, os certificados devem ser importados como certificados raízes. Para isso é necessário usar o gerenciador de certificados no IE.

Verificou-se nas ferramentas de software analisadas que 100% possuem a funcionalidade de assinar documentos eletrônicos. No entanto, as ferramentas possuem interfaces diferentes, umas mais simples, outras mais complexas, dependendo da experiência do usuário com o tema, e algumas ferramentas não pedem senha para assinar, há também ferramentas que permitem alteração no documento após assinado.

A ferramenta ARISP, após assinar um documento apresenta o brasão da ICP-Brasil, sugerindo que o documento foi assinado com um certificado emitido peal ICP-Brasil, contudo nos teste desenvolvidos sempre foram utilizados certificados emitidos fora da ICP.

Após a análise as ferramentas **ARISP** e **Okey** obtiveram a maior classificação, ambas com 57 pontos. Essas duas ferramentas possuem as seguintes funcionalidades: múltiplas assinaturas, assina arquivos no formato .PDF, possuem licença tipo gratuita, estão disponíveis na língua portuguesa e solicitam senha para assinar um documento. Mas apesar de iguais na pontuação, a ferramenta **Okey** leva uma pequena vantagem frente a ferramenta **ARISP** em dois aspectos: Interface mais simples ou limpa e a possibilidade de se escolher as extensões do arquivo após assinado entre: .PDF, PKCS#7 e XMLDSig. O ARISP dispõe apenas a extensão .P7s

A medida que for avançando o uso dos certificados, certamente irá aumentar a necessidade de estudos sobre os componentes que envolvem este tema, sejam componentes de hardware, software, ou processos.

REFERÊNCIAS:

MONTEIRO, Emiliano S., MIGNONI, Maria Eloisa. **Certificados Digitais** : Conceitos e Práticas / Emiliano S. Monteiro, Maria Eloisa Mignoni. – Rio de Janeiro : Brasport, 2007.

CUSTÓDIO, F. Ricardo., DIAS, Júlio S., ROLT, Carlos R. de. **Revista: BRy Tecnologia S.A**, Laboratório de Tecnologia de Gestão – Labges – UDESC, [s.d.].

FERREIRA, Fernando Nicolau Freitas. ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação** : Guia prático para elaboração e implementação / Fernando Nicolau Freitas Ferreira, Márcio Tadeu de Araújo. - Rio de Janeiro : Editora Ciência Moderna, 2008.

DAWEL, George. **A segurança da Informação nas Empresas**. Rio de Janeiro : Editora Ciência Moderna, 2005.

ARAÚJO, Wagner Junqueira de. **A segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento**. 2009. Tese (Doutorado em Ciência da Informação) Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 17799**: Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 27001**: Tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, requisitos. Rio de Janeiro, 2006.

BASTOS, Alberto. Os novos rumos da gestão de segurança com as normas ISO 17799 e BS 7799. **Módulo Security Magazine**, ago. 2002. Disponível em: <http:// www.modulo.com.br>. Acesso em: 12 jan. 2003.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 jun. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em 20 mar. 2008.

BRASIL. MP 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 ago. 2001. Disponível em: < http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em 16 de abr. 2010.

BRASIL. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 28 dez. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2002/ D4553.htm>. Acesso em 20 de mar. 2008.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília: TCU, Secretaria Adjunta de Fiscalização, 2003.

BRASIL. CERT.BR. **Cartilha de Segurança para Internet**: versão 3.1. São Paulo: Comitê Gestor da Internet no Brasil, 2006.

CASTELLS, Manuel. **A sociedade em rede**. 10. ed. São Paulo: Paz e Terra, 1999. v.1.

CONARQ(a). **Carta para a Preservação do Patrimônio Arquivístico Digital**: Preservar para garantir o acesso. 2004. Disponível em <http://www.conarq.arquivonacional.gov.br/Media/publicacoes/cartapreservpatrimarqdigitalconarq2004.pdf >. Acesso em: 16 de abr. 2010.

CONARQ(b). **Gestão Arquivística de Documentos Eletrônicos**. 2004. Disponível em <http://www.documentoseletronicos.arquivonacional.gov.br/Media/publicacoes/gt_gestao_arquivistica__pagina_web_corrigido3.pdf>. Acesso em: 16 de abr. 2010.

DERTOUZOS, Michel. **O que será**: como o novo mundo da informação transformará nossas vidas. São Paulo: Companhia das Letras, 1997. 12

DIAS, Claudia. **Segurança e auditoria da tecnologia da informação**: Rio de Janeiro: Axcel Books do Brasil, 2000.

ITI. **Glossário ICP-Brasil**. 2009. Disponível em : < http://www.iti.gov.br/twiki/pub/Certificacao/Legislacao/Glossario_ICP-Brasil-_Versao_1.3.pdf>. Acesso em 16 de abr. de 2010.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Editora Atlas, 1999.

GODOY, Arilda Schimidt. Estudo de caso . In: SILVA, Aneilson Barbosa da; GODOI, Christiane Kleinubing; MELO, Rodrigo Bandeira de. **Pesquisa qualitativa em estudos organizacionais, paradigmas, estratégias e métodos**. São Paulo: Saraiva, 2006.

GOMES, Luiz Flavio Autran Monteiro. Da Informação à Tomada de Decisão: Agregando Valor Através dos Métodos Multicritério. Recitec – **Revista de ciência e tecnologia**, Recife, v.2, n.2, p.117-139, 1998.

MASUDA, Yoneji. **A sociedade da informação como sociedade pós-industrial**. Rio de Janeiro: Editora Rio, 1982.

MATIAS-PEREIRA, José. **Manual de metodologia de pesquisa científica**. São Paulo: Atlas, 2007.

MOORE, Nick. **The information society, in World information report 1997/98**. Paris: UNESCO Publishin, 1997.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **The knowledge-based economy**. Paris, 1996. Disponível em: <http://www.oecd.org/ dataoecd/51/8/1913021.pdf>. Acesso em: 29 nov. 2007.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Studies in risk management norway:** information security. Paris: [s.n.], 2006.

RÉVILLION, Anya Sartori Piatnicki. **A Utilização de Pesquisas Exploratórias na Área de Marketing.** Apresentação. In: ENANPAD 2001, Campinas, set. 2001. (CD-ROM)

RICHARDSON, Roberto Jarry. **Pesquisa social, métodos e técnicas**. São Paulo: Atlas, 1999.

SILVA, Edna Lúcia da Silva; MENEZES, Estela Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. Florianópolis: UFSC, 2001.

SINGH, Simon. **O livro dos códigos**: a ciência do sigilo o do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

VILLAS BOAS, Cíntia de Lima. **Método multicritérios de análise de decisão (MMAD) para as decisões relacionadas ao uso múltiplo de reservatórios: Analytic Hierarchy Process (AHP)**. Disponível em < http://www.cprm.gov.br/rehi/simposio/go/METODO%20MULTICRITERIOS%20DE%20ANALISE%20DE%20DECISAO%20(MMAD)%20PARA%20AS%20DECISOES%20RELACIONADAS%20AO%20USO%20MULTIPLO%20.pdf>. Acesso em 17 de abr. 2010.

VILAS BOAS, Cíntia de Lima. **Modelo multicritérios de apoio à decisão aplicado ao uso múltiplo de reservatórios**: estudo da barragem do Ribeirão João Leite. 2006. 158 f. il., tab. Dissertação (Mestrado em Economia-Gestão Econômica do Meio Ambiente)-Departamento de Economia, Universidade de Brasília, Brasília, 2006

YIN, Roberto K. **Estudo de caso, planejamento e métodos**. Porto Alegre: Bookman, 2005.