ASSINATURA DE DOCUMENTOS ELETRÔNICOS UTILIZANDO CERTIFICADOS DIGITAIS

SIGNATURE OF ELECTRONIC DOCUMENTS USING DIGITAL CERTIFICATES

Wagner Junqueira de Araújo*

Renato Melo Vieira**

RESUMO

A necessidade de 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 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. Contudo, 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 executado nos documentos digitais. O objetivo do trabalho foi assinar documentos eletrônicos com chaves criptográficas assimétricas, utilizando certificados digitais gerados e gerenciados por software com licença livre 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 de software estudadas. Foram analisadas 12 ferramentas indicadas na literatura específica. Constatou-se que todas as ferramentas possuem a funcionalidade para assinar documentos eletrônicos, no entanto, possuem diferenças entre si quanto ao tipo de extensão de arquivo usado, idioma, tipo de licença, possibilidade de múltiplas assinaturas e solicitação de senha ao assinar. Após a análise, as ferramentas **ARISP** e **Okey** obtiveram a maior classificação, ambas com 57 pontos. As ferramentas com maior pontuação 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. Apesar de possuírem as mesmas pontuação, a ferramenta Okey apresenta um interface mais amigável.

Palavras-chave**:** Gestão da segurança da informação. Assinatura Digital. Certificado Digital. Documento Eletrônico. Tecnologia da informação e comunicação.

ABSTRACT

The need to keep information secures is as old as information itself. In the passed, emperors put custodians to defend the churches and official documents kept their documents under lock and key. With the explosion in the use of computers, digital documents have accessed, additionally the Internet has become a great vehicle disseminator. However, the greater the number of people with access to certain information, the greater its vulnerability. With so much information flowing at speeds of a click, not long before there was the need to have tools able to authenticate, to integrity, confidentiality, availability, and certain types of documents or non-repudiation Irreversible action or authorship of an act performed in the digital documents. The objective of this study was to sign electronic documents with asymmetric cryptographic keys, using digital identities generated and managed by software with free license or freeware, enabling guarantee its authenticity. We used an experimental approach with the method "multi criteria decision analysis" (MMAD) for evaluation of software tools studied. We analyzed 12 tools pointed in the literature. It was found that all tools have the functionality to sign electronic documents, however, have differences to the type of file extension used, language, license type, signatures and the possibility of multiple signing. After the analysis, tools Okey and Arispe had the highest rating, both with 57 points. Tools with higher scores have the following features: multiple signatures, signing files in. PDF, have free license type, available in Portuguese and password request to sign a document.

KEYWORDS: Information security management. Digital Signature. Digital identities. Electronic Document. Information technology and communication.

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.

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 do projeto de pesquisa relatado neste artigo tratou esta questão, por meio da avaliação e 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. O objetivo geral foi 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: a) Identificar na literatura ferramentas de software de geração, gerenciamento e assinatura de documentos eletrônicos, com as características necessárias para implementação do projeto; b) avaliar por meio de metodologia específica as ferramentas de software necessárias para implementação do projeto.

Para atingir tais objetivos o primeiro passou foi desenvolver uma revisão de literatura que aborda os tópicos sobre segurança da informação, segurança em documentos, certificação digital e assinatura em documentos digitais.

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 pelas redes aos seus usuários com uma maior rapidez e praticidade. Sendo a informação um recurso estratégico para as organizações essas mudanças necessitam de mecanismos que garantam a segurança destas informações, logo, surgiu a necessidade de se criar procedimentos e ferramentas que garantam a proteção da informação, por meio da integridade, confidencialidade e disponibilidade para estes novos suportes.

De acordo com Ferreira; Araújo (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.

> Esteja esta informação na forma impressa, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, apresentada sob a forma de filmes ou falada em conversas, ou seja qual for a forma, meio, ou mídia que a informação é apresentada, compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente (ARAÚJO, 2009, p. 39).

Contudo nem toda informação deve ser protegida, implementar os procedimentos para gestão da segurança da informação demanda recursos e isso gera custos. Portanto é necessário classificar e identificar qual a informação dever ser protegida. No ambiente organizacional, parte da informação está registrada em documentos internos, como ofícios, contratos, relatórios etc. É que essencial antes de proteger, 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 nº 20, de 16 de julho de 2004 do CONARQ faz considerações aos dois tipos de documentos citados.

> 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, 2004b §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, 2004b §2º)

> Portanto, 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.

Com o uso do computador como uma ferramenta e intermediador, e esse instrumento quem possibilitou novas descobertas em todas as áreas do conhecimento, provocou a criação e popularização do "documento eletrônico". Segundo Scheibelhofer (2001) "um documento eletrônico é composto por uma seqüência de bits cujo conteúdo só pode ser revelado com o auxílio de uma plataforma computacional". Apesar de ser reconhecido e tratado com um documento, este tem características diferentes de um documento impresso.

> 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, p. 10).

Seja pelos avançados editores de textos, que aposentaram de vez a velha máquina de escrever, ou mesmo assumindo funções desempenhadas apenas por seres humanos, a exemplos dos caixas eletrônicos nos bancos, é inegável a importância desses equipamentos em nossas vidas.

Para acompanhar esses avanços, a legislação também evolui, 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, 1998).

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

3 SEGURANÇA EM DOCUMENTOS ELETRÔNICOS

Junto com o suporte eletrônico, apareceram novas vulnerabilidades e o aumento dos riscos de fraudes. O que impulsionou os estudos em busca de tecnologias que pudessem garantir a validade de um documento eletrônico. Em 1976, Diffie e Hellman desenvolveram uma tecnologia

capaz de minimizar alguns problemas de segurança nas redes de computadores, foi criado um método de criptografia baseada na troca de pares de chaves. Este tipo de criptografia possibilita recursos necessários que garantam autenticar documentos e pessoas, bem como assinar transações online.

A primeira forma de criptografia foi a Simétrica, desempenhava o papel de cifrar ou ocultar dados sigilosos. Posteriormente surgiu a criptografia assimétrica, também conhecida pelos seus pares de chaves, **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.

Esta tecnologia emprega o uso de certificados digitais. A certificação digital começou a ser desenvolvida na década de 80

4 CERTIFICAÇÃO DIGITAL

Os certificados digitais, também chamados de identidade digital, é um 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 pode ser assinada utilizando-se a Chave Privada do assinante, porém esta assinatura só será validada pela com a chave pública correspondente.

Os pares de chaves são gerados pelas autoridades certificadoras.

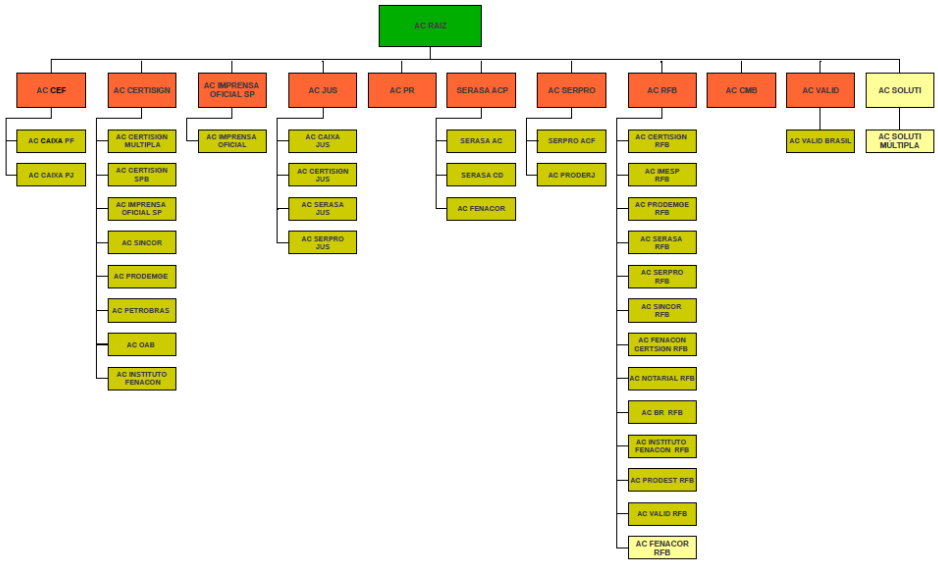
Denominam-se autoridades certificadoras entidades ou empresas com alto nível de confiança e reputação. Elas emitem certificados digitais para outras entidades, empresas e indivíduos, que precisam se identificar e garantir as suas operações no mundo digital. As autoridades certificadoras trabalham junto com uma autoridade de registro, que é uma empresa ou uma entidade responsável pela verificação das informações fornecidas pelos requisitantes dos certificados.

No ano de 2001, o governo brasileiro apresentou 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. Em alguns casos, somente as transações realizadas com certificados emitidos por autoridades credenciadas na ICP-Brasil têm validade reconhecida, como exemplo as transações com a Secretaria da Receita Federal. A figura 1 apresenta a de

autoridades certificadoras e autoridades de registro credenciadas na ICP-BR.

Estrutura ICP-Brasil em 04 de outubro de 2012



Fonte: iti.gov.br

5 ASSINATURAS DIGITAIS EM DOCUMENTOS ELETRÔNICOS

Nos documentos de arquivo são as assinaturas manuscritas e os carimbos que validam sua autoria, autenticidade e integridade. Já para os documentos eletrônicos 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, Dias e Rolt (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.

> Uma assinatura digital é um algoritmo de autenticação, que possibilita ao criador de um objeto unir ao objeto criado, um código que irá agir como. Esta assinatura confirma que o objeto não foi alterado, desde o ato de sua assinatura e permite identificar o assinante (MONTEIRO, 2007, p.10).

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

> A verificação de Assinatura Digital determinar 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, p. 90).

As atas que antes eram feitas em documentos de arquivos e são lavradas normalmente ao término de cada reunião, avançaram com 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 estar em outras cidades, estados ou até mesmo outros países, necessitando de ferramentas eletrônicas que possibilitem as assinaturas dos integrantes que participam a distância.

6 PROCEDIMENTOS METODOLÓGICOS E DESENVOLVIMENTO

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. A proposta deste trabalho foi avaliar ferramentas de softwares livres ou gratuitos, que possibilitem emitir certificados digitais, gerenciá-los e assinar documentos digitais, seguindo os padrões sugeridos pela ICP-Brasil.

> Um 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).

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).

Dentro das atividades propostas, a principal trata da avaliação de determinadas ferramentas de software, para isso optamos por aplicar um modelo simplificado do método multicritério de análise de decisão. Segundo Villas Boas

(2005) “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”.

Este método se mostrou adequado a proposta da pesquisa, pois,

> 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, 2005). 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).

Durante a pesquisa, foram testados 12 (doze) ferramentas assinadoras, que foram separadas, classificadas e pontuadas usando alguns dos seguintes critérios:

- Funcionalidade que permita múltiplas assinaturas, ou seja, um documento digital ser assinado por mais de uma pessoa;
- Idioma foi dado preferência aos softwares com suporte a língua portuguesa;
- Tipo da licença, foi verificado se a licença era livre, gratuita ou paga;
- Exigência de senha para validar uma assinatura.

O quadro 1 indica a pontuação aplicada na análise com a pontuação para cada critério estabelecido.

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 licença que determina se o software é livre ou gratuito ou se a licença é paga.	GNU/GPL(Livre) = 10; 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	Após assinado, o certificado bloqueia o	Sim = 10; Não = 03

Conteúdo	documento de novas alterações.	

Fonte: Elaborado pelo autores.

Com base nos critérios determinados, foram analisados as seguintes ferramentas de software:

1. **Adobe Acrobat Pro:** 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.
2. **Office 2007:** O Word Officce 2007 permite 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 para outros formatos. 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 fabricante, ou seja, a versão .DOC não é possível manter os certificados. Sendo 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
3. **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.
4. **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.
5. **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.
6. **DigiSigner**: Essa ferramenta solicita a senha somente ao carregar o certificado. Necessário instalar o certificado com nível alto de segurança inserindo a senha. Em suas versões mais novas ele é disponibilizado somente para teste por 30 dias.
7. **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.
8. **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.
9. **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.
10. **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 .
11. **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 .

12. **Okey:** Pode ser baixado direto do site do fabricante o http://www.pandorgatecnologia.com.br/Site/produtos-okey_free.aspx, e é uma ferramenta de licença gratuita. Após a instalação, para ativar a erramenta é necessário solicitar junto ao desenvolvedor um número de série. Esse procedimento é feito via e-mail.

Os certificados utilizados durante os testes 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. Os certificados tipo A1 são gerados no 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.

Os resultados apurados durante a pesquisa podem ser verificados no quadro 2.

Quadro 2 - ferramentas de software para assinatura digital analisadas

Software	Mult. Assin.	Idioma	Licença	Usa senha	Protege	Formato	Pontos
Open Office	3	10	10	0	3	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	3	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.

Para validar os documentos assinados os certificados gerados foram instalados como certificados raízes, o que permite a validação das assinaturas. Para implementação deste procedimento foi utilizado o gerenciador de certificados no Internet Explorer.

7 CONSIDERAÇÕES FINAIS

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. Contatou-se que algumas ferramentas não solicitam senha para assinar, fato grave, pois assinatura digital se trata de um procedimento de segurança. 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 pontuação, 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 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. Como durante os procedimentos que determinaram os critérios de avaliação e suas pontuações, as características sobre tipos dos arquivos gerados após o procedimento de assinatura e interface não forma incluídas, ocorreu o empate entre as ferramentas. Fica como uma sugestão para uma próxima pesquisa incluir estes dois itens como critérios de análise.

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

REFERÊNCIAS:

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.

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

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. 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. 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

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

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

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Carta para a Preservação do**

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

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

CUSTÓDIO, F. Ricardo, DIAS, Júlio S., ROLT, Carlos R. Assinatura Confiável de Documentos Eletrônicos. In CONFIANÇA no uso de documentos eletrônicos. BRy Tecnologia S.A. Laboratório de S3gurança em Computação – LABSEC – UFSC. Laboratório de Tecnologia de Gestão – LABGES – UDESC de. Florianópolis. Agosto de 2003.

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

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.

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

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

GODOY, Arilda Schimidt. Estudo de caso . In: SILVA, Aneilson Barbosa et al. **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.

INSTITUNO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (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.

LIMA NETO, José Henrique Barbosa Moreira. Aspectos jurídicos do documento eletrônico**. Jus Navigandi**, Teresina, ano 2, n. 25, jun. 1998. Disponível em <http://jus2.uol.com.br/doutrina/texto.asp?id=1780>. Acesso em: 08 jul. 2009.

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.

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

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

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

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

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.
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.

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

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)**. Brasília, 2005 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.

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

_____

Dados sobre autoria

*Doutor em Ciência da Informação/UnB, docente do Departamento de Ciência da Informação/UFPB.
E-mail: wagnerjunqueira.araujo@gmail.com

**Graduando em Biblioteconomia/UFPB.

Artigo enviado em setembro de 2012 para edição comemorativa da revista.