

APLICATIVO DE ASSINATURAS EM DOCUMENTOS DIGITAIS NOS DISPOSITIVOS MÓVEIS: ANÁLISE COMPARATIVA PELO MÉTODO MULTICRITÉRIO DE ANÁLISE DE DECISÃO (MMAD)

Lucas Carneiro Guedes Santiago¹

RESUMO

Há centenas de anos, já havia a preocupação no sigilo da informação, de modo que o imperador romano trocava o alfabeto de sua língua local para as letras gregas, numa tentativa de impedir que o inimigo compreendesse a mensagem. Aparentemente, isso parece simples, mas, na época, não era. Com o surgimento e o aperfeiçoamento da informática, os documentos passaram a ter um novo suporte, o digital, passando, então, a ser comum a utilização da assinatura digitalizada. Neste trabalho, aborda-se a fragilidade deste processo, como também reforça a importância da assinatura criptografada como segurança ao documento. Os documentos digitais fazem parte do nosso dia-a-dia e através da tecnologia dos dispositivos móveis, podemos armazenar contatos, enviar e receber mensagens, acessar os e-mails, navegar na web e até mesmo assinar documentos digitais em qualquer lugar. O objetivo deste trabalho foi realizar uma análise comparativa em programas para assinatura digital em dispositivos móveis, nos sistemas operacionais Android e iOS. A amostra foi composta de 18 aplicativos analisados através do método de análise por multicritérios. Foram estabelecidas seis variáveis para análise com suas respectivas pontuações. Verificou-se que os aplicativos estão voltados à segurança dos documentos assinados, utilizando da assinatura digital criptografada como recurso de integridade. Foi verificado que três softwares são compatíveis com a legislação vigente no Brasil. Todos os programas possuem formato padrão de leitura dos documentos o PDF e também layouts interativos. Constatou-se que o idioma predominante é o inglês, seguido do português. O aplicativo que teve a maior pontuação foi o ESIGNA WRITE LITE, que oferece licença grátis, idioma em português, assinatura na tela do dispositivo móvel, certificado digital e interatividade.

Palavras-chave: Assinatura Digital. Segurança da Informação. Dispositivo Móvel. Documento Eletrônico.

ABSTRACT

Hundreds of years ago, there was already concern on the confidentiality of information so that the Roman Emperor changed the alphabet of their local language to the Greek letters in an attempt to prevent the enemy understands the message. Apparently, this seems simple, but at the time it wasn't. With the emergence and the development of information technology, the documents have been given a new, digital support, passing then to be common to use digitized signature. This paper discusses the fragility of this process, but also reinforces the importance of the encrypted signature as security to the document. The digital documents are part of our daily lives and through the technology of mobile devices, we can store contacts,

¹ Graduando do Curso de Arquivologia – Universidade Federal da Paraíba - lucassantiago18@gmail.com.

send and receive messages, access your emails, surf the web and even sign digital documents anywhere. The aim of this study was to conduct a comparative analysis in programs for digital signature on mobile devices, Android and iOS operating systems. The sample was composed of 18 applications analyzed by the method of multi-criteria analysis. Were established six variables for analysis with their respective scores. It was found that the applications are geared towards the safety of signed documents, using the encrypted digital signature as health resource. It was verified that three softwares are compatible with current legislation in Brazil. All programs feature reading standard format of documents PDF and interactive layouts too. It was noted that the predominant language is English, followed by the Portuguese. The application that had the highest score was the ESIGNA WRITE LITE, which offers free license, in Portuguese language, signature, on the screen of the mobile device, digital certificate and interactivity.

Keywords: Digital Signature. Information Security. Mobile Device. Electronic Document.

1 INTRODUÇÃO

Vive-se em uma constante evolução tecnológica, inserida num dia-a-dia informatizado por meio de dispositivos móveis como smartphones, tablets, relógios Gear, etc. Atualmente, milhares de pessoas estão conectadas ao “mundo digital” através da internet, que é utilizada com canal de comunicação para diversos fins. No campo da Ciência da Informação, percebe-se que os estudos sobre os documentos tem crescido nestas últimas décadas. Devido a suas vantagens o suporte digital ganha espaço em relação aos documentos tradicionais/impressos. “O grande volume de informações com que se lida atualmente é um dos fatores que tem determinado a migração destas para o documento digital, em face à agilidade dos recursos digitais e à necessidade frenética de maior acesso à informação” (REIS, 2008, p. 1). No artigo 4º, da Lei n.º 12.527² diz que “documento é a unidade de registro de informações, qualquer que seja o suporte ou formato”. Independente do suporte o documento precisa de elementos para ser considerado como prova verídica, como exemplo cita-se a assinatura, carimbos, entre outros.

Há centenas de anos, a assinatura escrita está presente no nosso cotidiano, porém, com a evolução dos suportes informacionais e o aumento do gerenciamento de documentos digitais, as assinaturas digitais surgiram diante das necessidades. Por trazer praticidade,

² Lei n.º 12.527 de 18 de novembro de 2011. “Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

segurança e economia, órgãos públicos e privados vêm aderindo a este recurso, a exemplos de tribunais, receita federal, banco central, bancos e advogados.

Com os dispositivos móveis, surgiu a possibilidade de se executarem diversas tarefas através de um aparelho eletrônico portátil, por meio de aplicativos inseridos diretamente na rede digital, pelos quais podemos, por exemplo, visualizar ou mesmo assinar um documento digital.

De acordo com a previsão (2010-2015) de índice de rede Visual da Cisco³ (*Visual Networking Index (VNI) Global Mobile Data Traffic Forecast*), a quantidade de dispositivos móveis irá ultrapassar os 15 bilhões em 2015, ou seja, ultrapassará a quantidade de habitantes no planeta terra.

Neste contexto, o estudo apresentado neste artigo avaliou softwares que realizam a assinatura digital através dos dispositivos móveis, disponibilizados para os sistemas operacionais Android e iOS.

2 DOCUMENTOS DIGITAIS

Para entender sobre a assinatura digital, precisa-se compreender o conceito de documentos digitais. O Conselho Nacional De Arquivo (2006, p. 10) define documento como “informação registrada, qualquer que seja o formato ou suporte”.

É comum confundir os significados de documentos eletrônicos com documentos digitais, porém existem diferenças. De acordo com o Dicionário Brasileiro de Terminologia Arquivística (2005, p. 75), documento digital é o “documento codificado em dígitos binários, acessível por meio de sistema computacional”, como texto em PDF, planilha de cálculo em Microsoft Excel, áudio em MP3 e filme em AVI, e o documento eletrônico é conceituado como “gênero documental integrado por documentos em meio eletrônicos ou somente acessíveis por equipamentos eletrônicos, como cartões perfurados, disquetes e documentos digitais”. Então, nem todo documento eletrônico é digital, mas entende-se que todo documento digital é eletrônico (CTDE, 2013).

Percebe-se que não podemos associar documentos apenas para o suporte de papel, pois, de acordo com os conceitos expostos, fica claro que não existe diferença do documento tradicional para o documento eletrônico, ambos têm o mesmo objetivo, a diferença está no

³ CISCO. Disponível em: <<http://www.itforum365.com.br/noticias/detalhe/43857/em-2015-serao-15-bilhoes-de-dispositivos-moveis>>. Acesso em: 09 ago. 2014.

suporte no qual a informação está contida (OTTONI, 2003). O que reforça o pensamento de Marcacini (1999, p. 20) quando indica que “[...] é perfeitamente possível enquadrar o documento eletrônico na teoria e disposições legais relativas à prova documental”.

Desde a introdução dos computadores nas atividades rotineiras das organizações há documentos que já nascem de modo digital, e este suporte informacional permite-nos disseminar a informação em segundos, uma vez que o conteúdo digital não tem barreiras, não cria limites para o conhecimento. Devido às necessidades de uma rotatividade ágil da informação, os documentos tradicionais vêm sendo substituídos pelos digitais, porém adverte-se que estes documentos físicos não serão abolidos por completo. É importante ressaltar que os documentos digitais, tal qual os impressos necessitam ter autenticidade e integridade para ser considerados como prova, como ocorrem com os documentos impressos/tradicional.

2.1 Validade Jurídica dos Documentos Digitais e Assinatura Digital

Diante do crescimento do meio eletrônico, existe a preocupação que toda esta documentação seja regulamentada diante do âmbito jurídico.

No ano de 2001 o governo determina através da Medida provisória nº 2.200-2 que qualquer documento digital tem validade legal se for certificado pela ICP-Brasil (Infraestruturas de Chaves Públicas). A medida provisória também prevê a utilização de certificados emitidos por outras infraestruturas de chaves públicas, desde que as partes que assinam reconheçam previamente a validade destes (BRASIL, 2001).

A lei nº 11.419 de 2006 dispõe sobre a informatização no processo judicial, que regulamenta o uso de meio eletrônico na tramitação de processos judiciais – um avanço, buscando otimizar o tempo e atender às demandas solicitadas. Importante destacar que diversos funcionários da justiça podem assinar eletronicamente (utilizando as chaves públicas criptografadas), desde que haja obediência na forma da lei (BRASIL, 2006).

No ano de 2012, foi sancionada a lei nº 12.682 pela Presidente da República, regulamentando a validade jurídica dos documentos digitalizados e o arquivamento pelo meio eletrônico, esta lei expõe a necessidade da recuperação da informação de forma rápida e precisa, afirmando a obrigatoriedade da existência de software e possibilitando a busca deste documento, através do processo adequado de indexação (BRASIL, 2012), porém ressalta-se que existem, dentro da norma, alguns parâmetros a ser seguidos, que são eles: a integridade, autenticidade e, se preciso, a confidencialidade do documento digital. Na lei n.º 12.527 no artigo 4, inciso VII conceitua autenticidade como “qualidade da informação que tenha sido

produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema”. Para a NBR 17799⁴ (2001, p. 2) entende confidencialidade como “garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso e integridade como salvaguarda da exatidão e completeza da informação e dos métodos de processamento.” Devendo todo este processo estar regulamentado pelo certificado digital, fornecido pela Infraestrutura de Chaves Públicas Brasileira.

O Brasil encontra-se em situação igualitária em relações a outros países quando se trata que legislação que regem a assinatura digital. Marcacini (1999, p. 20) afirma que:

[...] em quase todos os cinquenta estados norte-americanos há lei, ou em vigor, ou em estudo, tratando da utilização de assinaturas digitais. Ao redor do mundo, podemos mencionar a existência de recente legislação já aprovada a este respeito, em 1997, na Alemanha, Itália e Malásia e, aqui na América Latina, a Argentina recentemente adotou norma a permitir o uso de assinatura digital perante os órgãos públicos à semelhança da legislação californiana.

Percebe-se que, desde a década de 1990, em vários lugares do mundo, já se tinha a preocupação de regulamentar e introduzir a assinatura digital em seus ambientes. Hoje, este cenário nestes espaços se encontra ainda mais avançado. No Brasil, as transações das instituições financeiras com o banco central já utilizam documentos assinados digitalmente desde 2002, entidades com a Receita Federal do Brasil, diferentes tribunais, entre outros, também mantêm relações com seus usuários por meios de documentos assinados digitalmente. Apesar de recentes, acredita-se que a legislação brasileira marcou um início de uma nova geração de documentos informatizados.

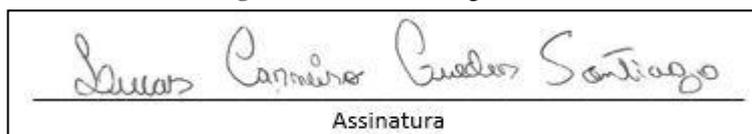
3 ASSINATURAS DIGITAIS

A assinatura digital é o conjunto de dados gerados a partir do processo de assinatura de arquivo. Através da assinatura digital, é possível verificar a integridade e a autoria de um documento eletrônico. (BRASIL, 2001).

Atualmente as assinaturas digitais mais comuns são a digitalizada, biométrica e a das chaves criptografadas assimétricas. A assinatura digitalizada, pode ser utilizada isoladamente ou em conjunto com certificados digitais. Quando isolada, esta forma de assinar digitalmente é constituída pela reprodução da assinatura no suporte físico através da tecnologia do scanner, permitindo a migração para o meio digital. Na figura 1 apresenta um exemplo.

⁴ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001. 56 p.

Figura 1: Assinatura digitalizada



Fonte: Elaborado pelo próprio autor

A fragilidade deste tipo de assinatura é nítida, pois não oferece segurança e autenticidade para o usuário, ou seja, pode ser reproduzida de qualquer documento assinado fisicamente e inserida em qualquer documento digital.

Seja pela íris do olho, pelo reconhecimento facial ou impressão digital, a assinatura biométrica está presente em bancos, nos processos eleitorais, complexos de segurança em geral, entre outros. A biometria surgiu como alternativa, e oferece proteção para usuários e empresas. Riha e Matyas explica que:

A verificação de identidade (autenticação) em sistemas de computador tem sido tradicionalmente baseada em chip-cartão ou PIN [...] com o surgimento da biometria esta assinatura passou a oferecer métodos de verificação de identidade ou de identificação sobre o princípio das mensuráveis características fisiológicas ou comportamentais, como uma impressão digital ou uma amostra de voz. (2000, p. 4, tradução nossa).

Como vantagem deste tipo de assinatura temos um aumento na segurança da informação, pois mesmo que outra pessoa tenha acesso a sua senha, o mesmo não conseguirá acessar seus dados. Em relação as desvantagens, pode-se citar o custo dos equipamentos, manutenção elevada e resistência por parte dos usuários.

Apesar de existirem processos diferentes, as assinaturas têm a mesma finalidade, mostrar nossa identificação pessoal. A assinatura digital mais utilizada é a de chaves criptográficas assimétricas, na qual:

[...] fornece meios para proteção da autenticidade e integridade de documentos eletrônicos [...] Possibilita a verificação de quem assinou o documento eletrônico e checar se o conteúdo do documento eletrônico assinado foi modificado. (NBR 17799, 2001, p. 41).

Para que o documento não seja aberto por pessoas não autorizadas, este tipo de assinatura utiliza meios de segurança para isto não ocorrer, neste processo usa a criptografia.

Acerca disso, Fiarresga (2010, p. 3) explica que:

Tão velha, mas com o mesmo objectivo primordial, ocultar a mensagem, – a criptografia – que também deriva de dois vocábulos gregos: *kryptos*, que significa oculto e *graphien* cujo significado já é conhecido, não esconde a existência da mensagem, apenas oculta o seu significado. De um modo geral, se a mensagem cair nas mãos de um intruso, este ao lê-la, não a compreenderá. Só o remetente e o destinatário, em princípio, através de um acordo pré-estabelecido, é que têm acesso ao significado da mensagem. O termo criptografia é usado muitas vezes como sinónimo de criptologia, abrangendo, desta forma, a criptanálise que tem por função descobrir os segredos, quebrar a confidencialidade entre emissor e receptor.

A criptografia de chaves assimétricas utiliza duas chaves relacionadas, uma é a assinatura digital (chave pública), a outra chave é a de identidade da assinatura (chave privada). Quando o emissor assina o documento, a mensagem passa a ficar criptografada, e através da chave privada que o receptor terá acesso a este conteúdo. Para cada documento assinado, produz uma nova assinatura, evitando que a mesma assinatura seja repetida, um processo complexo e seguro. Esta assinatura possui como suporte o *hash function*, que de acordo com Atreya (2002, p. 88 apud BODÊ, 2006, p. 65):

Funções hash são, às vezes, chamadas de funções unidirecionais, por sua característica única, que faz o processo inverso extremamente difícil ou impossível de se alcançar. Algumas pessoas referem-se ao resumo de mensagem (hash) como sendo uma impressão digital dos dados de entrada [...]. Dado o mesmo valor de entrada duas vezes, a função hash deve ser capaz de gerar o mesmo resumo em ambas às vezes. Uma mudança de 1 bit nos dados de entrada resultará num valor bastante diferente de resumo.

Este processo cria um único valor para todo o documento, como medida de segurança ao acesso a informação. Abordou-se sobre o uso das chaves públicas e privadas na assinatura de documentos, mas, para utilizá-las, o usuário necessita possuir os certificados digitais disponibilizados por uma ICP, no caso do Brasil a autoridade certificadora da ICP-Brasil.

3.1 Certificados digitais – Autoridade Certificadora

A certificação digital é um documento eletrônico assinado digitalmente, fator que oferece segurança a todo o processo e autenticidade, confidencialidade e integridade ao certificado (ITI, 2014). Ainda para o autor o certificado digital:

[...] funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.⁵

⁵ BRASIL. Instituto Nacional de Tecnologia da Informação. 2014. Disponível em: <<http://www.itl.gov.br/certificacao-digital/o-que-e>>. Acesso em 09 ago de 2014.

Esta autoridade certificadora (AC) citada trabalha como um cartório, na qual os usuários somente poderão utilizar as chaves públicas e privadas se a autoridade certificadora disponibilizá-las. Gandini et al., elucida que:

A autoridade certificadora tem a função de fornecer aos usuários os pares de chaves utilizados tanto para a assinatura digital como para a criptografia. É ela que fornece os certificados digitais, os quais podem ser definidos como um arquivo de computador que identifica quem você é para as outras pessoas, além de evitar o repúdio. (2002, p. 13).

Atualmente, existem treze autoridades certificadoras do Instituto de Chaves Públicas – Brasil, entre elas: Receita Federal, Caixa, Casa da Moeda, entre outras. Na intermediação entre o usuário e a AC está a Autoridade de Registro (AR), que tem como finalidade:

[...] receber, validar, encaminhar solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota. (ITI, 2014)

O certificado possui campos-chaves que são a identificação da assinatura do usuário, como: versão, número de série, assinatura, emissor, validade, assunto e extensões. Estas variáveis modificam, pois dependem da política de segurança da autoridade certificadora. Aumentando a segurança o certificado pode-se tornar inválido, seja pela validade do tempo ou por outra situação. HOUSLEY et al explica:

Quando um certificado é emitido, é esperado que ele seja usado por seu todo o período de validade. No entanto, várias circunstâncias pode causar um certificado para se tornar inválido antes do término da validade período. Tais circunstâncias incluem a mudança de nome. (2002, p. 10)

Percebe-se ao longo do tópico que existe um processo de validade do certificado digital seja válido, caso alguma etapa seja esquecida, poderá não funcionar adequadamente.

4 PROCEDIMENTOS METODOLÓGICOS E DESENVOLVIMENTO

Decidir a metodologia que vai ser abordada em trabalhos acadêmicos é um procedimento que requer atenção. É através dos métodos utilizados que a pesquisa utilizará as ferramentas adequadas para alcançar os objetivos traçados pelo autor.

Este artigo constitui um estudo de caso sobre os aplicativos que realizam assinaturas em documentos digitais nos dispositivos móveis. Para Severino (2007, p. 121), estudo de caso caracteriza-se por ser:

Pesquisa que se concentra no estudo de um caso particular, considerado representativo de um conjunto de casos análogos, por ele significativamente representativo. [...] os dados devem ser coletados e registrados com o necessário rigor [...] devem ser trabalhados, mediante análise rigorosa, e apresentados em relatório qualificados.

Por ser uma investigação qualitativa e exploratória, esta pesquisa tem características de um estudo de caso. Como o objetivo deste artigo foi realizar a análise comparativa entre os softwares, utilizou-se o método multicritério de análise de decisão.

As abordagens multicritérios se constituem em formas de modelar os processos de decisão, onde entram em jogo: uma decisão a ser tomada, os eventos desconhecidos que podem afetar os resultados, os possíveis cursos de ação e os próprios resultados. Estes modelos refletem, de maneira suficientemente estável, o juízo de valores dos decisores (VILA BOAS, 2014, p. 5).

Para avaliar os programas que realizam as assinaturas digitais, utilizou-se critérios de pontuação. Ainda para a autora:

[...] os resultados obtidos pela análise multicritérios dependem do conjunto de ações consideradas, da qualidade dos dados, da escolha e estruturação dos critérios, dos valores de ponderação atribuídos aos critérios, do método de agregação utilizado e da participação dos diferentes atores (SOARES, 2003 apud VILAS BOAS, 2014, p. 6).

A análise multicritérios define o problema, avalia e agrega os critérios utilizados e mostra qual a melhor decisão/opção a ser usada ou tomada (VILAS BOAS, 2014).

O objeto de estudo foram os assinadores digitais nos dispositivos móveis, no qual foram analisados 18 (dezoito) aplicativos, individualmente. Selecionou-se estes aplicativos devido a quantidade de download de ordem decrescente. Realizou-se o download dos softwares em suas respectivas plataformas e testamos no período de 02 a 20 de julho.

A partir da revisão bibliográfica para levantamento dos conceitos relacionado ao tema foram definidas as justificativas das pontuações atribuída, conforme o quadro 1.

Quadro 1 - Justificativa dos pontos

Critério	Justificativa
Versão	Entendemos que o software gratuito permite que os usuários possam conhecer e utilizar o aplicativo da assinatura digital e suas ferramentas, sem ter a necessidade de pagar o download do programa, por isso atribuímos 10 pontos. Para a versão trial, atribuímos 05 pontos, pois ela oferece a opção de utilizar o programa durante um certo período e possibilita que o usuário escolha se irá comprar ou não. Atribuímos 03 pontos à versão paga, pois ela não permite que o usuário sequer manuseie o programa antes de comprar, diferente das outras versões. Além disso, lembramos que parte dos aplicativos cobra-se em dólar, mais que o dobro do preço do real, sendo um ponto negativo para atrair novos clientes.
Certificado Digital	Se o programa disponibilizar a opção de utilizar o certificado digital, então, tem 10 pontos, pois o aplicativo consegue fornecer segurança para o usuário. Caso não possua, tem 0 ponto, devido à falta de segurança do software.
Assinatura na Tela	Quando o aplicativo fornece a opção de assinar o documento, seja com o dedo e/ou caneta, entendemos que esta função é uma ferramenta interativa, diferencial. Caso possua, tem 03 pontos, se não, 0 ponto.
Linguagem	Como o idioma oficial do nosso país é o português, o software que disponibiliza a língua tem 10 pontos, até mesmo para atrair mais clientes no Brasil. A língua mundial mais falada, ainda, é o Inglês, por isso, atribuímos 08 pontos. Logo, em seguida, está o espanhol, com 06 pontos, um idioma cotado por muitos a substituir o Inglês. Por fim, demais idiomas com 03 pontos.
Interface Interativa	Caso o programa possua uma interface interativa, onde o usuário encontre os recursos oferecidos sem muitas dificuldades, atribuímos 05 pontos. Se o programa apresentar um layout que seja de difícil entendimento, atribuímos 03 pontos.
Formato	O PDF (Portable Document Format) apresenta mais segurança que os demais formatos, o software diminui o risco de fazer edições no documento. Além disso, é um software gratuito, utilizado com frequência, e o documento não perde qualidade, por isso, atribuímos 10 pontos. Para o DOC e DOCX, aplicamos 08 pontos, tem utilização massiva de usuários, porém tem segurança menor que a do PDF e também é um programa pago. 06 pontos atribuímos para o formato ODT (OpenOffice), semelhante às características dos formatos DOC e DOCX, software gratuito, mas não utilizado com frequência pelos usuários. Para o formato RTF (Rich Text Format), a pontuação é de 05 pontos, é um software gratuito, mas permite fazer edições simples e não é utilizado frequentemente por usuários. Para os demais formatos, atribuímos 03 pontos.

Fonte: Dados de pesquisa, 2014.

Conforme o quadro 2 observamos os critérios, descrição e pontos a serem considerados na avaliação.

Quadro 2 - Critérios, descrições e pontuações utilizadas no artigo

Critérios	Descrições	Pontuação
Licença	Se o programa é pago, gratuito ou trial (versão experimental)	Gratuito (10), Trial (05) e Pago (03)
Certificado Digital	Se é o programa é compatível com a ICP-Brasil ou com as normas mundiais de assinatura digital	Sim (10) e Não (0)
Assinatura na Tela	Se o software permite que o usuário assine com o dedo e/ou caneta no próprio aparelho touchscreen	Sim (3) e Não (0)
Linguagem	Qual idioma utilizado pelo aplicativo	Português (10), Inglês (08), Espanhol (06) e Outras (03)
Interface Interativa	Se o software possui um layout interativo	Sim (05) e Não (03)
Formato	Quais formatos suportados pelo programa	PDF (10), Doc e Docx (08), ODT (06), RTF (05) e Outros (03)

Fonte: Dados de pesquisa, 2014.

O uso dos dispositivos móveis está presente em nosso cotidiano, seja com a finalidade de verificar agendamento de compromissos profissionais, pessoais ou lazer. Devido a sua praticidade para realizar tarefas, estamos, cada vez mais, utilizando suas vantagens ofertadas.

De acordo com Silva (2011, p. 11):

Dispositivos móveis são pequenos computadores, geralmente de uso pessoal, que podem possuir tela sensível ao toque e/ou teclado em miniatura, podendo ser levados para todos os lugares. Além disso, estes dispositivos possuem um paradigma de interação humano-computador diferente do que estamos acostumados

Esta interação citada por Silva (2011) é o que nos impressiona e fascina, pois os aplicativos presentes nos dispositivos móveis trazem recursos de comodidade e bem-estar para o usuário. Os dispositivos permitem armazenar contatos, realizar chamadas, enviar e receber mensagens, acesso a e-mails e sites e possui diversos aplicativos (exemplo: leitores de livros, editores de textos, calculadoras, GPS, mapas, jogos e até assinadores digitais).

Optou-se por trabalhar com as plataformas iOS e Android, pois são os sistemas operacionais mais consolidados no mercado, abrangendo a maior parte da população mundial.

Lista-se no quadro 3 os aparelhos e marcas que suportam os dois sistemas operacionais estudados na pesquisa.

Quadro3 – Aparelhos, marcas e sistemas operacionais

Android	iOS
Tablets - Samsung	iPad - Apple
Tablets - Motorola	iPad mini - Apple
Tablets - Asus	iPhone - Apple
Smartphone - LG	iPod - Apple
Smartphone - Samsung	
Smartphone - Sony	

Fonte: Dados de pesquisa, 2014.

Segundo a empresa Google, no ano de 2013, existiam 900 milhões de aparelhos com sistema Android no mundo, tendo se tornado o mais utilizado, devido aos seus preços mais acessíveis.

Pereira e Lourenço (2009, p. 3) dizem que o Android sempre está em evolução:

[...] sistema operacional foi construído com a intenção de permitir aos desenvolvedores criar aplicações móveis que possam tirar total proveito do que um aparelho portátil possa oferecer. Foi construído para ser verdadeiramente aberto.

O Android tem um layout de fácil visualização e manuseio, permitindo o usuário a operar com o sistema tranquilamente. Para podermos utilizar os aplicativos (app) ofertados pelo Android, inclusive os softwares de assinaturas digitais de documentos, utilizou-se a loja virtual do Android, Google Play Store.

Já quanto à Apple, segundo dados da própria empresa, no ano 2012, existiam 400 milhões de dispositivos ativos com o sistema iOS ativo. Sendo o maior concorrente do Android, o iOS está, cada dia mais, aumentando seu número de clientes, apesar do custo alto de seus produtos. O sistema, atualmente, encontra-se na versão 7.1.1.

Pinto; Gomes (2012, p. 7) dizem que “O sistema operacional iOS, que roda nos dispositivos iPhone, iPod touch e iPad [...] é responsável por controlar o hardware do aparelho e prover recursos para as aplicações desenvolvidas para o mesmo”.

Tomaz (2011, p. 12) complementa, afirmando que “O iOS é um dos mais populares e robustos, possuindo sistema de interface com o usuário, simples e intuitivo, com capacidade de reconhecimento de gestos”. Assim como o Android, o iOS possui uma loja de aplicativos, chamada Apple Store, um dos pontos diferenciais da plataforma, oferecendo mais aplicativos que sua concorrente.

As descrições foram retiradas e/ou adaptadas das páginas dos fabricantes e testadas nos dispositivos móveis. Para utilizar os aplicativos que oferecem o certificado digital, é necessário realizar o procedimento semelhante ao dos desktops, então, os dispositivos móveis que utilizam os sistemas operacionais Android e iOS requerem que o usuário realize um cadastro, seja direto do aplicativo, no site do fabricante ou importando sua assinatura para o programa, de modo que o usuário assine o documento.

Lista-se os dezoito aplicativos trabalhados na pesquisa: Adobe EchoSign, DocuSign, eSigna Writer Lite iOS, ITTRU, Certisigner, Signnow, Certillion, Signwasy, HelloSign, Adobe Reader, Esigna Writer Lite Android, SignNow, Sign & Fill Documents, SigningHub, SIGNificant Signature, eSigna Mobile, Signdoc, Imobigin e Signply.

Através do quadro 4, pode-se visualizar o resultado da análise dos softwares.

Quadro 4 - Aplicativos analisados na pesquisa

Software	Plataforma	Licença	Certificado Digital	Assina na tela	Linguagem	Interface Interativa	Formato	Pontos
ESIGNA WRITE LITE	Android	10	10	3	10	5	10	48
ESIGNA WRITER LITE	iOS	10	10	3	10	5	10	48
DOCUSIGN	iOS	10	10	3	8	5	10	46
SIGNIFICANT SIGNATURE	Android	10	10	3	8	5	10	46

SIGNINGHUB	Android	10	10	3	8	5	10	46
CERTILLION	iOS	10	10	0	10	5	10	45
ITTRU	iOS	10	10	0	10	5	10	45
ESIGNA MOBILE	Android	10	10	0	8	5	10	43
SIGNNOW	iOS	5	10	3	8	5	10	41
SIGNNOW SIGN & FILL DOCUMENTS	Android	5	10	3	8	5	10	41
ADOBE ECHOSIGN	iOS	3	10	3	8	5	10	39
ADOBE READER	Android	10	0	3	10	5	10	38
CERTISIGNER	iOS	3	10	0	10	5	10	38
IMOBISIGN	Android	10	0	3	8	5	10	36
SIGNDOC	Android	10	0	3	8	5	10	36
SIGNPLY	Android	10	0	3	6	5	10	34
SIGNEASY	iOS	5	0	3	10	5	10	33
HELLO SIGN	iOS	5	0	3	8	5	10	31

Fonte: Dados de pesquisa, 2014.

Nos critérios idioma e formato, alguns programas fornecem mais de uma característica. Diante disso, considerou-se apenas a maior pontuação, para não haver desequilíbrio com as demais variáveis.

Verificou-se que 100% dos aplicativos possui interface interativa que auxilia no manuseio do sistema. Independente do sistema operacional as empresas buscam aprimorar este critério. Todos os programas apresentam como padrão o formato PDF, o mais utilizado nas assinaturas digitais, seja em dispositivos móveis ou não. Os softwares HELLO SIGN e SIGNEASY trazem o diferencial de suportar 06 tipos de arquivo (PDF, RTF, imagens, HTML e ODT).

No critério idioma, o inglês está mais presente. A língua portuguesa aparece em segundo lugar, com 38%, tendo 7 aplicativos com esta linguagem. O ESIGNA WRITE LITE para Android oferece mais de três idiomas (inglês, português, espanhol, outros), sendo este o mais completo neste quesito.

Acredita-se que a assinatura na tela consiste numa ferramenta com objetivo de atrair mais usuários para o aplicativo, pois deixa registrado realmente sua assinatura tradicional “manuscrita”, possibilitando, com isso, a interatividade de modo criativo e simples, por isso, este critério está presente em 77% dos programas.

Constatou-se que 12 fabricantes oferecem gratuitamente seus softwares, sendo a maioria da plataforma Android. Lembra-se que o fato de a licença ser livre não implica dizer que o usuário pode utilizar a opção de certificado digital. Mas, se o mesmo possuir um

certificado válido, poderá utilizar este serviço ofertado pelo programa. Apesar de serem programas não pagos, nenhum dos aplicativos apresentou propagandas.

Percebe-se que o certificado digital é uma prioridade das empresas após a análise dos programas. Sendo uma ferramenta fundamental para a segurança e o sigilo do documento digital, o certificado está presente em 66% dos programas analisados. Este critério encontra-se mais presente no sistema operacional iOS. Examinou-se que o CERTILLION, CERTISIGNER e ITTRU utiliza certificados compatíveis com a ICP-Brasil.

O programa que obteve a maior pontuação foi o ESIGNA WRITE LITE (Android e iOS) com 48 pontos, tendo todas as pontuações máximas, ou seja, o mais completo dentro dos critérios avaliados. O ESIGNA é interativo, seguro (utiliza-se smartcard ou certificado), em português e gratuito. Na última posição, ficou o HELLO SIGN, com 31 pontos, apresentando um programa básico, que permite fazer upload de documentos pela própria câmara do dispositivo e assinar documentos na tela.

6 CONSIDERAÇÕES FINAIS

Percebe-se que existe preocupação dos fabricantes dos softwares em utilizar os certificados digitais como ferramenta de segurança nas assinaturas digitais e verificamos que já possui aplicativos de acordo com as normas jurídicas do Brasil (ICP – Brasil). Ainda é comum utilizar a assinatura digitalizada nos documentos, porém como vimos na pesquisa este tipo de assinatura não tem garantia de integridade e autenticidade da informação, diferente das assinaturas criptografadas que atendem estes requisitos.

Espera-se que aumentem as atualizações e criações de novos softwares de assinaturas digitais em dispositivos móveis, que estes aplicativos possam chegar ao conhecimento e uso de mais usuários no mundo. Os benefícios oferecidos pela assinatura digital são diversos, e sabemos que ela traz novos caminhos, por isso, precisamos de mais estudos acerca do tema para trazer novas e diferentes ideias.

Acredita-se que esta é uma importante ferramenta para os dias de hoje, e deve acompanhar a evolução desta era da informação digital, quando os processos estão surgindo e migrando para o eletrônico, e, enquanto usuários, precisamos da garantia de que praticidade e segurança marchem juntas.

REFERÊNCIAS

BODÊ, Ernesto Carlos. **Assinaturas digitais e arquivologia**. Arquivística.net. v. 2, n. 1, p. 52-69, 2006. Disponível em: <www.arquivistica.net>. Acesso em: 06 ago. 2013.

BRASIL, Angela Bittencourt. **O documento físico e o documento eletrônico**. Jus Navigandi: Teresina, ano 5, n. 42, 1 jun. 2000. Disponível em: <<http://jus.com.br/artigos/1781>>. Acesso em: 27 jul. 2013.

BRASIL. **Instituto Nacional de Tecnologia da Informação**. 2014. Disponível em: <<http://www.iti.gov.br/certificacao-digital/o-que-e>>. Acesso em 09 ago de 2014.

BRASIL. Lei nº 12.682, de 09 de julho de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12682.htm>. Acesso em: 05 ago. 2013.

BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/111419.htm>. Acesso em: 05 ago. 2013.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Disponível em: <<http://brasil.isigmaglobal.com/legislacion/>>. Acesso em: 29 abr. 2014.

BRASIL. **Perguntas e Respostas sobre criptografia, assinatura digital, certificado digital, entre outras questões**. 2013. Disponível em: <<http://www.iti.gov.br/images/publicacoes/cartilhas/cartilhaentenda.pdf>>. Acesso em: 16 dez. 2013.

CTDE (Câmara Técnica de Documentos Eletrônicos). Disponível em: <<http://www.documentoseletronicos.arquivonacional.gov.br/cgi/cgilua.exe/sys/start.htm?sid=10>>. Acesso em: 27 jul. 2013.

DICIONÁRIO BRASILEIRO DE TERMINOLOGIA ARQUIVÍSTICA. Rio de Janeiro: Arquivo Nacional, 2005.

FIARRESGA, Victor Manuel Calhabrês. **Criptografia e matemática**. 2010. 144 f. Dissertação (Mestre) - Universidade de Lisboa, Lisboa, 2010. Disponível em: <http://repositorio.ul.pt/bitstream/10451/3647/1/ulfc055857_tm_Victor_Fiarresga.pdf>. Acesso em: 06 ago. 2013.

FOLHA DE SÃO PAULO. **Aparelhos Android**. 2013. Disponível em: <<http://www1.folha.uol.com.br/tec/2013/05/1279008-existem-900-milhoes-de-aparelhos-com-sistema-android-no-mundo-diz-google.shtml>>. Acesso em: 27 abr. 2014.

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. **A segurança dos documentos digitais**. Jus Navigandi: Teresina, ano 7, n. 54, 1 fev. 2002. Disponível em: <<http://jus.com.br/artigos/2677>>. Acesso em: 25 ago. 2013.

HOUSLEY, Russell; FORD, Warwick; POLK, Tim; Solo, David. **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Internet RFC 3280**. Virginia: Internet Society. 2002. Disponível em: <<http://www.ietf.org/rfc/rfc3280.txt>>. Acesso em 09 ago de 2014.

MARCACINI, Augusto Tavares Rosa. **O documento eletrônico como meio de prova**. São Paulo, 1999.

OTTONI, Márcia Benedicto. **I Fórum sobre Segurança, Privacidade e Certificação Digital: Validade Jurídica dos Documentos Digitais**. São Paulo. 2003. Disponível em: <<http://www.docstoc.com/docs/107584278/%ef%bf%bdvalidade-jur%ef%bf%bddica%ef%bf%bd-dos-documentos-eletr%ef%bf%bdnicos-e-a-mp-220001>>. Acesso em: 27 jul. 2013.

PEREIRA, Lúcio Camilo Oliva; SILVA, Michel Lourenço da. **Android para desenvolvedores**. Rio de Janeiro: Brasport, 2009. Disponível em: <http://books.google.com.br/books?id=8u9wjowxfduc&pg=pr4&lpg=pr4&dq=pereira,+lucio+camilo+oliva;+da+silva,+michel+louren%20o.android+para+desenvolvedores.+brasport,+2009.&source=bl&ots=lslo12wlq4&sig=ipubmnc7vgoikmb3pxkdyyx_kni&hl=pt-br&sa=x&ei=zfvvcu-s8euvlsqtbwohybq&ved=0cduq6ae waq#v=onepage&q=pereira%20lucio%20camilo%20oliva%3b%20da%20silva%20michel%20louren%20o.android%20para%20desenvolvedores.%20brasport%202009.&f=false>. Acesso em: 27 abr. 2014.

PINTO, Pedro Micael Theosa Lucas Nogueira; GOMES, Antônio Ricardo Leocádio. **Segurança na conectividade wifi em dispositivos móveis: estudo de caso do iPhone**. e-Xacta, v. 4, n. 3, 2012.

REIS, Carolina Cunha dos. **Do Papel Ao Meio Eletrônico: A Validade Jurídica dos Documentos Eletrônicos e a Assinatura Digital**. 2008. Disponível em: <<http://www.webartigos.com/artigos/do-papel-ao-meio-eletronico-a-validade-juridica-dos-documentos-eletronicos-e-a-assinatura-digital/4272/>>. Acesso em: 21 jul. 2013.

RIHA, Zdenek; MARYAS, Vaclav. **Biometric authentication systems**. FI MU Report Series, RS-2000-08, November 2000. Disponível em: <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.3840&rep=rep1&type=pdf>>. Acesso em 10 de agosto de 2014.

RONDINELLI, Rosely Curi et al. **Conselho Nacional de Arquivos CONARQ**. 2006. Disponível em: <<http://www.documentoseletronicos.arquivonacional.gov.br/Media/publicacoes/ctdeglossariov22006.pdf>>. Acesso em: 27 jul. 2013.

SILVA, Tomaz Rocha da. **Um estudo de interação com displays grandes usando dispositivos iOS**. Porto Alegre. 2011.

SINGH, Simon. **O livro dos códigos**. Editora: Record, 2008.

SEVERINO, Antônio Joaquim. **Metodologia do trabalho científico**. 23. São Paulo: Cortez, 2007.

VILAS BOAS, Cíntia de Lima. **Análise da aplicação de métodos multicritérios de apoio à decisão (mmad) na gestão de recursos hídricos**. Universidade Nacional de Brasília: Goiânia. 2014. Disponível em: <<http://www.cprm.gov.br/rehi/simposio/go/Analise%20da%20Aplicacao%20de%20Metodos%20Multicriterios%20de%20Apoio%20a%20Decisao%20na%20Gestao%20de%20Recursos%20Hidricos.pdf>>. Acesso em: 04 jul. 2014.