CERTIFICAÇÃO DIGITAL: assinatura digital, certificados digitais e sua utilização no mercado nacional

Digital certification: digital signature, digital certificates and its use in the national market

José Diego Zunino[1]

Resumo: O presente artigo aborda assuntos relacionados à Certificação digital, voltados para área de assinatura e documentos digitais, tratando aspectos legais e jurídicos referente a assinaturas com a arquitetura de certificados estipuladas pela ICP-Brasil. Contempla suas características, seu padrão de hierarquia utilizado, diferença entre uma assinatura digital e a assinatura formal, aquela efetuada em cartórios. Também é apresentada a atual situação da utilização no mercado nacional brasileiro, apresentando indicadores de crescimento retirados de um portal de assinatura, a utilização de certificados digitais na área da saúde, que cada vez mais vem abrindo espaço no mercado brasileiro. O artigo também aborda a evolução, quais os rumos que ainda devem ser tomados em relação a todo esse mercado que ainda tem muito a crescer, tanto em nível nacional quanto em nível mundial, voltados cada vez mais para dispositivos móveis.

Palavras-chave: Certificação digital. Assinatura digital. Certificados digitais. Portal de coleta de assinaturas.

Abstract: The article deals with issues related to Digital Certification, aimed at the area of signature and digital documents. Addressing legal and legal aspects regarding signatures with the architecture of certificates stipulated by ICP-Brazil. Contemplating what its characteristics, hierarchy standard used, difference between a digital signature and the formal signature, that done in notaries. It will also be presented the current situation of use in the Brazilian national market, presenting growth indicators taken from a subscription portal, the use of digital certificates in the health area, which is increasingly opening space in the Brazilian market. And what is the evolution, what are the directions that still have to be taken in relation to this whole market that still has and much to grow, both nationally and globally, increasingly turned to mobile devices.

Keywords: Digital certification. Digital signature. Digital certificates. Sign collection portal.

O objetivo deste artigo é apresentar o uso de documentos digitais, verificar a utilidade desta nova tecnologia do ponto de vista técnico, analisando os aspectos de garantia de autenticidade, sigilo, reconhecimento, integridade e confiabilidade em documentos digitais e assinaturas coletadas digitalmente. Será abordado também o ponto de vista jurídico, acerca da validade, o não repúdio de documentos e a segurança jurídica, e apontar as estruturas hierárquicas dos certificados digitais. Serão apresentadas e esclarecidas informações sobre a certificação digital, englobando a parte de assinatura digital e carimbo do tempo. Apresentando as estruturas hierárquicas que compõem um certificado, avaliando os aspectos que fazem com que o certificado se torne íntegro, autêntico, sigiloso e reconhecido em operações de assinaturas de documentos digitais/digitalizados. Tipos de certificados digitais existentes atualmente no mercado nacional. Além disso, serão apresentados números e indicadores de assinaturas digitais de nível nacional brasileiro, apresentando o crescimentos nos últimos tempos em relação à utilização de certificados digitais.

A inclusão digital está cada vez mais forte no nosso dia a dia, afetando inclusive o meio de assinatura. O método atual é burocrático, é necessário ir até o cartório, com documentos impressos e reconhecer firma (para confirmar que a pessoa que está assinando é ela mesma), isso torna esse método de assinatura caro também.

[1] Centro Universitário Leonardo Da Vinci – UNIASSELVI –. Rodovia BR 470 – KM 71 – nº 1.040 – Bairro Benedito – Caixa Postal 191 – 89130-000 – Indaial/SC Fone (47) 3281-9000 – Fax (47) 3281-9090 – E-mail: josediegozunino@gmail.com

Partindo desse ponto, a assinatura digital faz com que todo o processo seja simplificado, em que a pessoa possui um certificado digital (muitas vezes, um e-cpf) e o documento digital, este documento pode estar em um *site*/portal de assinatura, e pronto, é só fazer a assinatura. Este novo modo economiza tempo, visto que a assinatura leva em média 3 segundos e todo o processo (entrar no *site*, selecionar o documento e assinar) leva no máximo 2 minutos. Enquanto em um modelo tradicional, contando com transporte e enfrentamento de fila em um cartório, esse tempo pode ser bem estendido. O gasto com papel e impressão também se torna zero, visto que não se faz necessário imprimir, pois todos os documentos finais (documento assinado) são digitais.

Será apresentada a atual situação da certificação e indicadores de nível nacional, da utilização de certificados digitais e documentos digitais, indicadores retirados de um portal de assinatura nacional, a utilização de assinaturas digitais em hospitais e empresas do ramo da saúde também podem desfrutar, e muito, dessa tecnologia. O futuro da certificação, voltado para a área de dispositivos móveis, também tem muito para crescer, visto que a utilização dessa plataforma tem crescido muito nos últimos anos e tende a crescer cada vez mais.

Todas as pesquisas apresentadas nesse artigo serão com fundamentos em trabalhos já publicados, em *sites* do ramo de assinatura e documentos digitais. Este artigo será dividido em tópicos, para melhor apresentação do conteúdo. Os dados utilizados para a geração de gráficos não trazem informações de empresas/clientes ao *site* que disponibilizou as informações, para garantir a integridade das mesmas.

O que é certificação digital?

> A certificação digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos. Na certificação digital é utilizada, como base, a tecnologia de criptografia de chaves pública. Eles são emitidos por uma autoridade certificadora credenciada à ICP-Brasil. A certificação digital identifica pessoas e empresas no mundo digital, comprovando sua identidade, permite acessar serviços eletrônicos e assinar documentos eletrônicos com a possibilidade de autenticidade e integridade dos dados. Além destas vantagens, a certificação pode ser usada também como: garantia de sigilo e privacidade de *sites*, controle de acesso a aplicativos, assinatura de formulários, identificação de remetentes, assinatura de mensagens e impossibilidade de repúdio (MONTEIRO; MIGNONI 2007, p. 80).

A certificação tem como principal foco garantir a segurança entre as transações, visto que somente o próprio portador do certificado poderá fazer uso de tal ferramenta, não podendo ser transferível, a menos que esse portador autorize, por meio de uma procuração, que outras pessoas utilizem seu próprio certificado. Uma vez comprovada a identidade da pessoa no mundo digital, com seu próprio certificado ela poderá fazer uso de portais de assinaturas, fazer as devidas assinaturas, ou acompanhamento com base em *log* de rastreamentos. "O certificado digital é um documento eletrônico que identifica pessoas e empresas no mundo digital, comprovando sua identidade. Permite acessar serviços *on-line* e assinar documentos eletrônicos com possibilidade de certificação da autenticidade e da integridade" (CORDEIRO, 2008, p. 7).

Também conhecido como identidade digital, o certificado é um arquivo que identifica os dados de determinada pessoa ou empresa, em que ela possui suas chaves para fazer a certificação. Para a segurança e total funcionamento do serviço, os certificados utilizam criptografia para cifrar e decifrar as assinaturas, sendo utilizado dois tipos de chaves no seu processo: chave pública e privada.

Chave pública e privada

A chave pública pode ser acessada e conhecida por todos, são dados do proprietário do próprio certificado. São esses dados que as aplicações utilizaram para gerar logs de eventos, autenticar a pessoa no sistema e validar os dados antes de executar alguma ação. "As principais informações que constam em um certificado digital são: chave pública do titular; nome e endereço de *e-mail*; período de validade do certificado; nome da Autoridade Certificadora – AC que emitiu o certificado; número de série do certificado digital; assinatura digital da AC" (ITI, 2016a).

Quanto à chave privada, apenas o próprio proprietário do certificado deve conhecer a chave privada, ela seria, literalmente, a senha de acesso ao certificado digital.

> A verificação de Assinatura Digital determina se ela foi criada pela Chave Privada correspondente à 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; MIGNONI 2007, p. 90).

ICP-Brasil

> A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos (ITI, 2016a).

Em todo o território nacional, o controle sobre a certificação digital é feito pelo ITI – Instituto Nacional de Tecnologia da Informação, totalmente voltado aos cuidados e inovações em tecnologia de ampliação da cidadania digital.

> O Instituto Nacional de Tecnologia da Informação (ITI) é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, sendo a primeira autoridade da cadeia de certificação – AC Raiz.
> A Medida Provisória 2.200-2 de 24 de agosto de 2001 deu início à implantação do sistema nacional de certificação digital da ICP-Brasil. Isso significa que o Brasil possui uma infraestrutura pública, mantida e auditada por um órgão público, no caso, o ITI, que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil, cujos membros, representantes dos poderes públicos, sociedade civil organizada e pesquisa acadêmica, são

> nomeados pela Presidenta da República.
> Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Sua principal linha de ação é a popularização da certificação digital ICP-Brasil e a inclusão digital, atuando sobre questões como sistemas criptográficos, *hardware* compatíveis com padrões abertos e universais, convergência digital de mídias, desmaterialização de processos, entre outras (ITI, 2016b).

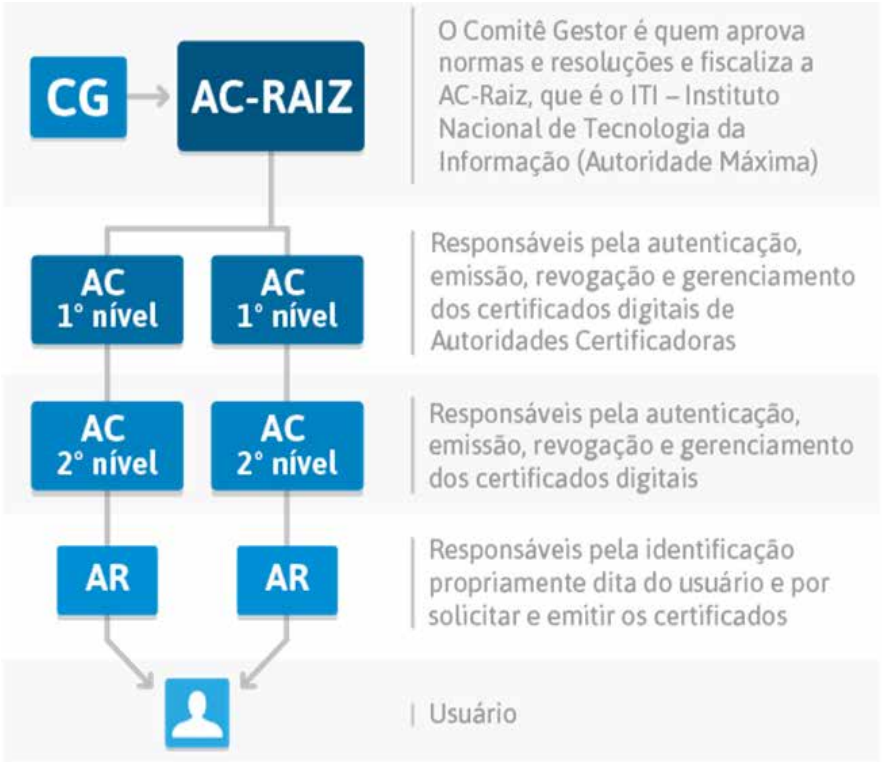
A ICP é que define as diretrizes e normas que devem ser seguidas, seu padrão é atualmente seguido por todas as certificadoras e empresas que dispõem desse serviço. É importante ressaltar que é ela quem define as políticas de certificados e normas técnicas e operacionais, todas aprovadas por um comitê gestor organizado pela própria ICP-Brasil.

Hierarquias da certificação

Para garantir a qualidade e confiança na certificação digital, foi implantado no dia primeiro de janeiro de 2012 a segunda versão do certificado digital ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira).

> A cadeia de confiança de certificação digital é a hierarquia existente entre os componentes da ICP-Brasil. Estes componentes são a AC Raiz (Autoridade Certificadora Raiz), as ACs (Autoridades Certificadoras) de primeiro nível e segundo nível, as ARs (Autoridades de Registros), e, finalmente, o usuário final (BENEFÍCIOS E APLICAÇÕES DA CERTIFICAÇÃO DIGITAL, 2013).

Figura 1. Componentes da ICP-Brasil



Fonte: Disponível em: <http://www.beneficioscd.com.br/cartilha_online/?pagina=oq06->. Acesso em: 3 abr. 2016.

AC – Raiz:

> A Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.
> A AC-Raiz também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil (ITI, 2016c).

AC – Autoridade Certificadora:

> Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).
> Cabe também à AC emitir lista de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (ARs) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada (ITI, 2016c).

AR – Autoridade de Registro:

> É responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de 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, 2016c).

ACT – Autoridade Certificadora do Tempo:

> Uma Autoridade Certificadora do Tempo – ACT – é uma entidade responsável por emitir Carimbos do Tempo. A AC-Raiz da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é a responsável pelo credenciamento das ACT's que desejam integrar a estrutura, com base em critérios estabelecidos nos documentos que regulamentam o assunto (ITI, 2016b).

O conteúdo de um documento, após ser assinado, é criptografado. Com uma autoridade certificadora do tempo, é garantido que o documento foi assinado naquele dia, mês, ano, hora, minuto e segundo. Todo seu conteúdo pode ser validado e garantido em relação a questões de tempo com a ACT.

Assinatura formal x assinatura digital

Para maior compreensão sobre o assunto, será abordado o que são assinatura formal e assinatura digital, destacando suas principais diferenças.

Assinatura formal

Em um modelo mais tradicional que conhecemos, os documentos são assinados e reconhecidos em cartório. "Os cartórios, mais corretamente denominados como Serviços Notariais e de Registral, são aqueles de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos" (CERTIFIXE, 2016, s.p.).

Para realizar essas assinaturas é necessário criar um cadastro em cartório, reconhecendo a própria "firma", após isso, pode ser realizada a assinatura de qualquer tipo de documento. Reconhecer "firma" é atestar que aquela assinatura é a sua. O reconhecimento de firma de próprio punho pode ser feito por dois modelos:

Por semelhança: sendo a mais comum, é garantida pela semelhança entre as assinaturas realizadas e a assinatura registrada no cartório. São verificados os traços da assinatura realizada.

Por autenticidade: utilizada quando se necessita de mais segurança, neste modelo é necessário que o signatário tenha que ir pessoalmente ao tabelionato e assinar o documento na presença do tabelião.

O reconhecimento por autenticidade é muito mais seguro que o de semelhança, pois força a responsabilidade do tabelião em garantir a sua veracidade.

Mesmo com toda essa garantia, ainda existem pessoas que tentam agir de má fé e burlar/falsificar assinaturas, ainda mais no modelo por semelhança, que é válida a caligrafia utilizada na assinatura.

Assinatura digital

> Quando você mandar uma mensagem pela estrada da informação, ela será "assinada" pelo seu computador, ou outro dispositivo de informação, com uma assinatura digital que só você será capaz de aplicar, e será codificada de forma que só seu destinatário real será capaz de decifrá-la. Você enviará uma mensagem, que pode ser informação de qualquer tipo, inclusive voz, vídeo ou dinheiro digital. O destinatário poderá ter certeza quase absoluta de que a mensagem é mesmo sua, que foi enviada exatamente na hora indicada, que não foi nem minimamente alterada e que outros não podem decifrá-la (GATES; MYHRVOLD; RINEARSON, 1995, p. 138).

Nesse cenário, ao invés do signatário se dirigir até um cartório, ele deve utilizar um portal/aplicativo voltado para este fim. E onde antes era utilizada uma caneta para assinar, nesse novo modelo é utilizado um certificado digital.

> A Assinatura Digital, como o próprio nome diz, serve para assinar qualquer documento eletrônico. Tem validade jurídica inquestionável e equivale a uma assinatura de próprio punho. É uma tecnologia que utiliza a criptografia e vincula o certificado digital ao documento eletrônico que está sendo assinado. Assim, dá garantias de integridade e autenticidade (QUALISIGN, 2005-2017).

> A assinatura digital é uma técnica capaz de agregar características de segurança semelhantes às obtidas ao assinarmos um documento utilizando papel e caneta, mas em meio eletrônico. Trata-se de uma forma de assinar arquivos digitais do tipo PDF, DOC, ou qualquer outro formato (BRY TECNOLOGIA, 2016).

Para realizar uma assinatura digital é necessária a utilização de um e-CPF, do tipo A-1 ou A-3. A diferença entre os dois modelos está na validade e segurança.

Certificado A-1

Esse modelo é armazenado na própria máquina e seu tempo de assinatura é mais rápido se comparado ao A-3, tem validade máxima de 1 ano.

> No certificado tipo A1 o par de chaves pública/privada é gerado em seu computador, no momento da solicitação de emissão do certificado. A chave pública será enviada para a Autoridade Certificadora (AC) com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada em seu computador, devendo, obrigatoriamente, ser protegida por senha de acesso. Este certificado for instalado no mesmo computador onde foi efetuada a solicitação do certificado e tem validade de 1 (um) ano (ASS TECNOLOGIA, 2012).

Certificado A-3

Sua validade pode ser de um, dois ou três anos, dependendo da necessidade do assinante, pode ser em formato de cartão ou *token* (parecido com um *pendrive*).

> O certificado tipo A3 oferece mais segurança, justamente porque o par de chaves é gerado em *hardware* específico, isto é, num cartão inteligente ou *token* que não permite a exportação ou qualquer outro tipo de reprodução ou cópia da chave privada. Também no certificado tipo A3 a chave pública será enviada para a AC junto com a solicitação de emissão do certificado, enquanto a chave privada ficará armazenada no cartão ou *token*, impedindo tentativas de acesso de terceiros. Com este método, você poderá transportar a sua chave privada e o seu certificado digital de maneira segura, podendo realizar transações eletrônicas onde desejar. O certificado tipo A3 tem validade de 3 (três) anos (ASS TECNOLOGIA, 2012).

> O Certificado Digital e-CPF é a versão eletrônica do CPF (Cadastro de Pessoa Física) e permite realizar operações na internet com a mesma validade jurídica que o documento físico. Também pode ser usado em instituições privadas, como já fazem alguns bancos para determinadas transações. Em instituições públicas como a Receita Federal e a Caixa, sua utilização é indispensável (SERASA EXPERIAN, 2014).

Em termos de garantia de autenticidade e integridade de documentos, as assinaturas de próprio punho e assinaturas digitais têm a mesma validade, de acordo com a lei MP nº 2.200/02 e estando de acordo com as normas exigidas pela ICP-Brasil (BRASIL, 2001).

Portal de assinatura digital

Um portal de assinatura digital é um ambiente disponibilizado para coleta de assinaturas.

> Desde 2002, a Assinatura Digital passou a ter a mesma validade jurídica que uma assinatura manuscrita. Ela é gerada por meio do uso do Certificado Digital ICP-Brasil e facilita a rotina de pessoas físicas e jurídicas, já que assinando no meio eletrônico, economiza-se tempo e dinheiro. Afinal, você cria, assina e transmite o documento no meio digital, sem precisar utilizar papel, imprimir vias, se deslocar para autenticar o documento e ainda transportá-lo a outra parte interessada (CERTISGN EXPLICA, 2014).

Esses portais geralmente abrem espaço para disponibilização dos documentos para coleta de assinatura, a coleta de assinatura em si, com todos os signatários parametrizados previamente antes de começar o processo de recolhimento de assinatura, e em sua maior parte, disponibilizam a guarda dos documentos assinados, em que dispõem uma grande infraestrutura, com controle de acesso aos documentos (de acordo com o documento e necessidade do cliente, somente algumas pessoas têm acesso ao documento). Dentre todas as vantagens da utilização de portais de assinaturas digitais, podemos citar:

Economia de tempo: todo o processo de transporte de documentos é anulado em um portal de assinaturas, visto que em muitas vezes esses portais são disponibilizados na internet. A locomoção do signatário também é anulada, pois de qualquer lugar pode ser acessado e realizada as assinaturas.

Economia de dinheiro: para todo o processo de assinatura não se faz necessária a impressão dos documentos que serão assinados, sendo assim, a economia de papéis e impressão é zero. Em um modo geral, as assinaturas digitais são mais baratas que as assinaturas de próprio punho. "É possível obter uma redução superior a 50% nos trâmites que envolvem assinatura, armazenamento e envio de documentos. Só para se ter uma ideia, o retorno médio sobre o investimento, um mês após a implementação das soluções de DTM, é de mais de 300%" (BLOG DOCUSIGN, 2015).

Notificações: a cada assinatura, todos os signatários podem ser notificados. A cada nova solicitação, todos podem ser notificados. Isso gera mais facilidade, pois os usuários só acessam o portal quando necessário.

Facilidade no uso: em um modo geral, esses portais de assinatura são bem práticos e de fácil utilização para o usuário final. De acordo com a Explicação da empresa Certsign Explica (2014), "[...] basta acessar o Portal de Assinaturas, uma plataforma de serviços em nuvem, onde você faz o *upload* do documento, cria o fluxo de assinaturas, assina com validade jurídica e ainda transmite o documento [...]".

Sustentabilidade: com todos seus documentos digitais, você evita o desperdício de papel e energia, afetando e contribuindo para a preservação do meio ambiente.

> A ideia de desmaterializar processos (transformar o físico em digital) através do Certificado Digital permite que os usuários não desperdicem mais milhares de papéis na emissão de documentos, impactando indiretamente na redução do desmatamento. O Certificado Digital permite a ausência de impressão, sem autenticação adicional e com validade jurídica, tudo de forma simples e totalmente digital (CERTISGN EXPLICA, 2014).

Mobilidade: com a grande expansão da tecnologia móvel pelo mundo, a certificação digital vem acompanhando também, e é possível hoje, de qualquer lugar do mundo, realizar uma assinatura digital. Conforme explicado por Maurício Coelho, diretor de infraestrutura de Chaves Públicas, no ITI – Instituto Nacional de Tecnologia da Informação, a possibilidade do uso do certificado ICP-Brasil em meios móveis, leva a certificação digital para um ambiente mais agradável e torna o sistema mais flexível para o usuário final (SERASA EXPERIAN, 2014).

Confiança: com a utilização de um certificado, a assinatura fica muito mais restrita. Somente quem possui o certificado pode realizar a assinatura. Com a assinatura registrada, ficam todos os dados do signatário, garantindo que tal pessoa em tal horário realizou a assinatura em um determinado documento.

> Uma das formas de proteger os usuários é o Certificado Digital, que é uma assinatura digital com validade jurídica, garantindo agilidade e segurança às transações eletrônicas e outros serviços via internet. Esse documento eletrônico segue os padrões determinados pela Infraestrutura de Chaves Públicas Brasileira, que busca sempre a proteção no âmbito digital. À ICP-Brasil, coube também, a função de determinar uma Autoridade Certificadora Raiz, responsável por conceder, supervisionar outras Autoridades Certificadoras e fazer a auditoria dos certificados emitidos por elas. Esta AC-Raiz é a ITI – Instituto Nacional de Tecnologia da Informação (SERASA EXPERIAN, 2014).

Validade: atualmente, perante a lei, documentos com assinaturas digitais já são válidos, podendo ser utilizados como meio comprobatórios.

> A lei nº 12.682/2012 define que, após a digitalização de um documento, e mesmo que ele possua assinatura digital, o original assinado deve ser preservado. Entretanto, a medida provisória nº 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), regulamenta a validade jurídica de documentos que nascem digitais e são assinados com uso de certificado digital. Diante desse cenário, a solução criada pelo Serpro ajuda a sanar os entraves ocasionados na digitalização de documentos (SERPRO, 2016).
>
> De acordo com o art. 10, da MP n° 2.200-2, os documentos eletrônicos assinados digitalmente com o uso de certificados emitidos no âmbito da ICP-Brasil têm a mesma validade jurídica que os documentos em papel com assinaturas manuscritas. Importante frisar que os documentos eletrônicos, assinados digitalmente por meio de certificados emitidos fora do âmbito da ICP-Brasil, também têm validade jurídica, mas esta dependerá da aceitação de ambas as partes, emitente e destinatário, conforme determina a redação do § 2º do art. 10 da MP n° 2.200-2 (ITI, 2016b).

Integridade: a integridade de um documento assinado digitalmente vai garantir a validade deste documento e que o mesmo não sofreu alterações em seu conteúdo, e suas assinaturas contêm todos os requisitos que permitem ser íntegros.

> A assinatura digital garante ao destinatário que o documento não foi alterado ao ser enviado (integridade) e ainda comprova a autoria do emitente (autenticidade), enfim, confere maior grau de segurança, pois os documentos eletrônicos não assinados digitalmente têm as características de alterabilidade e fácil falsificação (TRT4, s.d.).
>
> [...] a integridade visa assegurar que um documento não teve seu conteúdo alterado após ter sido assinado. Para isso, o sistema é capaz de detectar alterações não autorizadas no conteúdo. O objetivo é que o destinatário verifique que os dados não foram modificados indevidamente (E-SAJ, 2016).

Utilização no mercado nacional brasileiro

> A certificação digital existe no país desde 2001, mas seu uso cresceu de forma significativa a partir de 2006, com a aprovação de uma lei que tornava legalmente válida a autenticação de documentos por certificados digitais. No país, existem pouco mais de 5 milhões de companhias e pessoas físicas com certificados digitais e a perspectiva de representantes do setor é que o mercado cresça com a adoção dessa ferramenta em novas áreas. (SINDIFISCO NACIONAL, 2014).

O crescimento é inevitável, as adaptações às novas tecnologias também são precisas para pessoas físicas ou jurídicas, isso tanto no nosso mercado nacional brasileiro, como num cenário mundial, quem não se adaptar às novas tecnologias, por exemplo, à adoção da certificação digital, está sujeita a perder negócios, em alguns casos de negociação já é indispensável a utilização da assinatura digital. Um exemplo é a utilização de certificado digital para acessar o serviço "Conectividade Social ICP", adotado em junho de 2012.

> A Certificação Digital já faz parte do dia a dia nas empresas. Só em 2011 foram emitidos no Brasil, cerca de 1 milhão de certificados. Hoje existem mais de 5 milhões de certificados digitais emitidos, sendo que 70% são de pessoas jurídicas. O volume mensal de novos certificados emitidos já ultrapassa a casa dos 100.000/mês (QUALISIGN, 2005-2017).

Nos últimos anos, o mercado tem cada vez mais voltado sua atenção para questões de cuidados com o meio ambiente, e a certificação digital não foge dessa evolução. Com a utilização de documentos digitais é possível conseguir uma economia significativa em impressão de papel. Vendo por outro ponto de vista, com as pessoas cada vez mais atarefadas e com pouco tempo para executar suas tarefas, a assinatura digital se torna uma grande aliada, pois em pouco tempo o signatário faz todas assinaturas pendentes com apenas alguns cliques.

> Tudo isso aliado à certeza da segurança e eficiência em transações eletrônicas para uma sociedade sustentável nos empreendimentos, nas relações sociais e ambientais. Além disso, queremos fortalecer nosso papel e termos reconhecimento ainda maior junto aos Poderes Executivo, Legislativo e Judiciário, nas associações de classe, sindicatos, instituições de pesquisa científica e de ensino, instituições da sociedade civil e demais entidades e organismos nacionais e internacionais (CANGIANO, 2015).

> O número de emissões de certificados digitais no Brasil, ao longo de 2015, apresentou crescimento de mais de 28% em comparação com o ano anterior. De acordo com a Associação Nacional de Certificação Digital (ANCD), a assimilação, principalmente entre as empresas, desta tecnologia é tão grande que a estimativa é que este ano o setor cresça em torno de 20% (ANCD, 2016).

Indicadores

Os índices apresentados foram retirados de um portal de assinaturas digitais, Portal Q'Certifica, que vem se destacando no mercado nacional e sendo utilizado por 90 por cento dos fundos de investimentos e securitizadoras. Foi desenvolvido pela empresa QuickSoft Tecnologia da informação, que tem sua sede em Blumenau, Santa Catarina.

Figura 2. QuickSoft

Fonte: Disponível em: <http://www.quicksoft.com.br/img/a.jpg>. Acesso em: 4 jun. 2016.

Todos os dados apresentados aqui não apresentaram nenhuma informação de cliente da empesa QuickSoft, nem clientes que utilizem o produto do portal Q'Certifica. Tudo isso para manter o sigilo das informações dos clientes citados.

Figura 3. Portal Q'Certifica

Fonte: Disponível em: <http://www.qcertifica.com.br/img/logo.png>. Acesso em: 4 jun. 2016.

Abaixo, números e indicadores retirados do portal acima citado.

Assinaturas realizadas por mês

Indicador apresentando os números de assinaturas realizadas de outubro de 2014 até maio de 2016, demonstrando a quantidade de assinaturas realizadas e o crescimento ao longo do tempo.

Figura 4. Assinaturas realizadas por mês

Fonte: Disponível em: <https://portal.qcertifica.com.br>. Acesso em: 4 jun. 2016.

Documentos por mês

Indicador apresentando a quantidade de documentos assinados digitalmente de outubro de 2014 até maio de 2016.

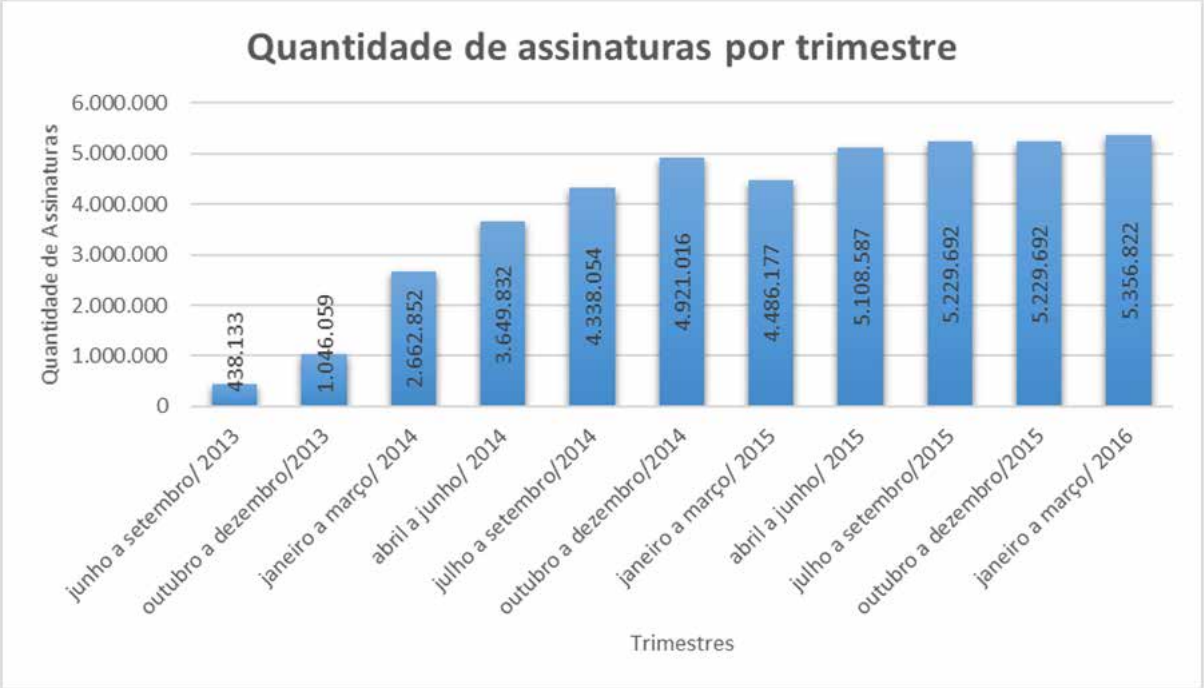
Figura 5. Quantidade de documentos por mês.

Fonte: Disponível em: <https://portal.qcertifica.com.br>. Acesso em: 4 jun. 2016.

Quantidade de assinaturas por trimestre

A figura abaixo demonstra o crescimento da utilização da assinatura digital desde junho de 2013 até março de 2016, agrupando por trimestres para melhor vizualização.

Figura 6. Quantidade de assinaturas por trimentre

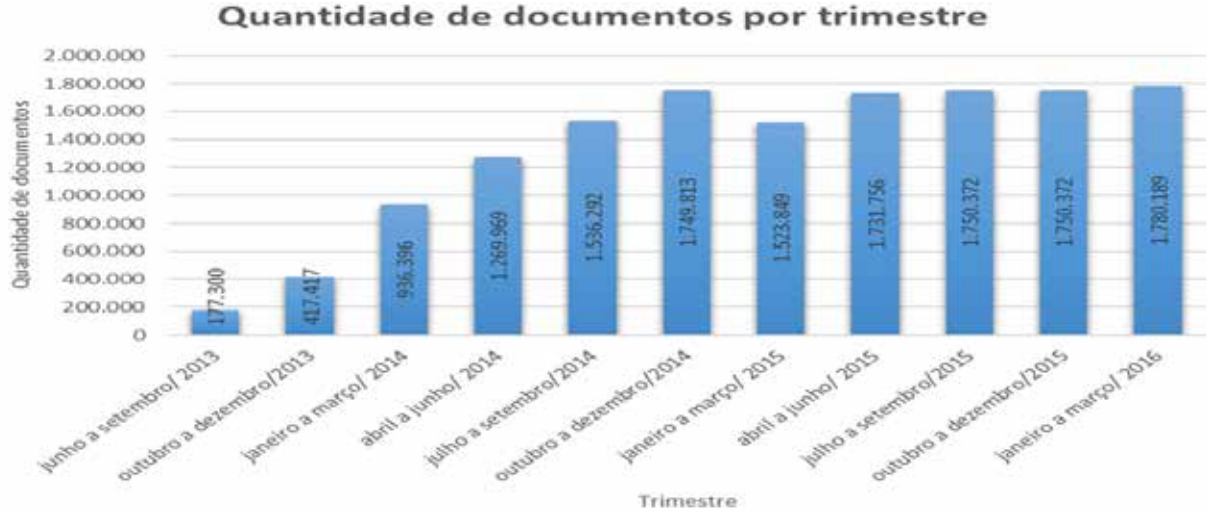


Fonte: Disponível em: <https://portal.qcertifica.com.br>. Acesso em: 4 jun. 2016.

Quantidade de documentos por trimestre

Abaixo é apresentada uma figura com o grande crescimento dos documentos digitais de junho de 2013 até março de 2016, agrupando, conforme a figura acima, por trimestres, para melhor vizualização.

Figura 7. Quantidade de documentos por trimentre



Fonte: Disponível em: <https://portal.qcertifica.com.br>. Acesso em: 4 jun. 2016.

Utilização da certificação digital na área hospitalar

Uma grande evolução da certificação digital pode ser citada na área da saúde, utilizada para assinar prontuários e atestados médicos, em que o médico que executa o serviço pode registrar sua assinatura digital, tendo validade e procedência necessárias para comprovações futuras.

> O Certificado Digital no uso médico daria validade jurídica e segurança a todos que utilizam a fonte médica em suas atividades diárias, como laboratórios, análises clínicas etc. O Prontuário Eletrônico do Paciente com certificado digital garantiria ministrar corretamente medicamentos, acompanhar a recuperação dos mesmos, a visualização da evolução de doenças crônicas. Sem contar que reduziria erros médicos, erros interpretativos e seria de fácil visualização em atendimentos remotos em qualquer parte do mundo (CANGIANO, 2015).

No caso de atestados médicos, isso evitaria o forjamento de documentos, visto que a assinatura poderia ser validada e comprovada junto a um visualizador de arquivos com assinatura digital ou até mesmo no próprio portal que foi expedido.

Futuro: certificados e assinaturas digitais em *smartphones*

Segundo Sodré (2015), a aplicação possibilita que o *smartphone* funcione como um token ou cartão, guardando o certificado digital. Dessa forma, o usuário tem mais facilidade para utilização do documento e dificilmente emprestará o certificado a terceiros. Atualmente, não é possível utilizar certificados digitas em *smartphones* ou dispositivos móveis do gênero, consequentemente não sendo possível realizar assinaturas. Com o grande crescimento da utilização dessa plataforma, é indispensável a realização de assinaturas nesses dispositivos.

Já existem várias empresas que atuam nas áreas de venda de certificados, voltando sua atenção para dispositivos móveis. A própria ICP-Brasil está com várias frentes de estudo para garantir que essa implementação seja feita da maneira mais correta possível.

Conforme explicado pelo diretor de tecnologia, Maurício Balassiano (CERTSIGN EXPLICA, 2014), "[...] com a aplicação esperamos retirar a complexidade do uso para o usuário final e excluir a necessidade de utilização de *hardwares*. O certificado deixará de ser um periférico e passará a fazer parte de um dispositivo pessoal [...]".

Com sua utilização em dispositivos móveis, cria para os usuários um ambiente mais agradável, onde ele tenha praticidade e ao mesmo tempo segurança de estar em seu próprio dispositivo. O diretor de Infraestrutura de Chaves Públicas, Maurício Coelho (ITI, 2016), diz que "[...] a possibilidade do uso do certificado ICP-Brasil em meios móveis leva a certificação digital para um ambiente mais agradável e torna o sistema mais flexível para o usuário final [...]".

Não existe nenhum meio físico, leitor de cartão ou token voltado para essa plataforma, e seria quase inviável ter que portar um leitor para tal finalidade, a ideia seria dentro de cada dispositivo possuir um arquivo de certificado digital instalado para tal finalidade, nesse ponto entrarão várias medidas que devem ser tomadas, tanto para a instalação no dispositivo quanto em questão de segurança, pois este certificado pode ser reconhecido como um documento pessoal, e pessoas que tendem a agir de má-fé podem invadir esses dispositivos móveis com essa informação e roubá-las ou até mesmo o próprio usuário fazer a troca do dispositivo móvel. Isso tudo deve ser pensado antes de implantar a assinatura digital em dispositivos móveis.

Resultados

Com a inclusão da certificação digital e, consequentemente, assinaturas digitais, criamos um novo cenário no mercado atual, tanto na parte de sustentabilidade, com o corte da utilização de papel e gastos com impressão, quanto na cultura de assinar documentos, em que antes era feito com a assinatura de próprio punho, tendo que se dirigir até um cartório. Hoje em dia vemos um cenário totalmente diferente, assinaturas que podem ser realizadas com apenas alguns cliques de *mouse* e em pouco tempo, com ambientes que alienam eficiência e segurança.

Todo esse novo modelo de assinatura traz para o usuário muito mais praticidade, uma vez que ele pode assinar qualquer documento digital, armazenar esse documento já assinado em um local que mais agradar, disponibilizar a qualquer momento para qualquer pessoa e o mais importante, acessar o documento de qualquer local, podendo estar no computador pessoal e ao mesmo tempo em seu *smartphone*.

Conforme apresentado nas figuras anteriores, os índices apontam o grande crescimento da certificação digital no Brasil. E esse mercado tende a crescer cada vez mais.

Um grande empecilho na implementação da certificação digital é a necessidade de um certificado digital, que ainda não é gratuito, e para alguns usuários esse custo se torna desnecessário. Outro ponto a ser visto é a falta de livros e documentos voltados para essa área, o material encontrado nessa área é, em grande parte, encontrado em *sites* de empresas que disponibilizam esses serviços, empresas que definem regras e diretrizes, inclusive, para a realização desse trabalho, a maior parte das referências foram encontradas nesses *sites* de empresas voltadas a essa área.

> A Autoridade de Registro Biométrica – AR Biométrica é um projeto conduzido pelo ITI que visa dar mais segurança ao processo de emissão de certificados digitais ICP-Brasil. Um princípio fundamental desse projeto é que os Institutos de Identificação dos Estados tenham suas bases, os registros dos cidadãos, digitalizados, ou informatizados, para que se realize uma consulta por sistemas, automatizada (ITI, 2016b).

Todo esse novo mercado ainda é muito novo e recente, e tem muito para crescer e evoluir, tanto em nível nacional quanto em nível mundial. Muitas ideias ainda podem ser evoluídas. Muitas empresas têm se dedicado para o crescimento, apresentando novas ideias, como é o caso da implementação da biometria, sendo especificada pelo ITI.

Considerações finais

Com tudo que foi apresentado neste documento, podemos observar cada vez mais o crescimento da certificação digital, consequentemente a utilização de certificados digitais, com a utilização cada vez mais frequente na coleta de assinaturas, tornando simples a sua utilização antes de realizar e após, para comprovação judicial ou a simples guarda desses documentos.

Com esses atributos, um certificado digital pode ser utilizado como um documento de identidade, pois contém todos os dados do proprietário, é sigiloso e intransferível. Sua utilização ainda pode ser muito expandida, por exemplo, podemos armazenar dentro de um certificado a nossa carteira de habilitação, que para validar o documento, um guarda de trânsito que inserisse o certificado em uma leitora, já saberia se a habilitação para dirigir está ativa ou não.

Por enquanto existem muitas empresas que estão se privando da utilização de certificados digitais, ainda mantêm a forma tradicional de ir até o cartório, registrar a firma para realizar a assinatura. Em sua maior parte, é pelo fato de muitos assinantes não terem acesso à internet ou

não saberem manusear um computador, geralmente pessoas mais antigas, que acreditam que a internet não é um lugar seguro e que seus dados podem ser roubados. A transferência de um proprietário de veículo automotor é um exemplo, a qual não é possível utilizar a certificação digital, que tornaria o processo menos burocrático, e consequentemente, mais rápido.

À medida que os certificados digitais forem avançando, certamente irá aumentar a necessidade de estudos em relação aos componentes de *hardware*, *software* ou nos próprios processos que envolvem a segurança e praticidade de sua utilização. A ICP-Brasil: Infraestrutura de chaves públicas Brasileira tem contribuído muito para esta evolução, atuando como uma entidade padronizadora e que rege diretrizes como normas técnicas para sua utilização e melhor funcionamento possível, fazendo com que toda a fiscalização e auditoria tenha concordância, visto que todas as assinaturas e documentos digitais utilizam um único padrão de comunicação.

Referências

ANCD. **Associação Nacional de Certificação Digital**. 2016. Disponível em: <http://jcrs.uol.com.br/_conteudo/2016/02/cadernos/jc_contabilidade/483654-certificacao-digital-deve-crescer-20-em-2016.html>. Acesso em: 3 jun. 2016.

ASS TECNOLOGIA. **Certificado Digital**. 2012. Disponível em: <http://www.asstecnologia.com.br/blog/?p=2232>. Acesso em: 9 maio 2016.

BENEFÍCIOS E APLICAÇÕES DA CERTIFICAÇÃO DIGITAL. **O que é certificação digital?** 2013. Disponível em: <http://www.beneficioscd.com.br/cartilha_online/>. Acesso em: 2 abr. 2016.

BLOG DOCUSIGN. **Como a assinatura digital traz economia para sua empresa?** 2015. Disponível em: <https://www.docusign.com.br/blog/como-a-assinatura-digital-traz-economia-para-sua-empresa/>. Acesso em: 20 maio 2016.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 11 maio 2016.

BRY TECNOLOGIA. O que é uma assinatura digital? 2016. Disponível em: <https://blog.bry.com.br/o-que-e-uma-assinatura-digital/>. Acesso em: 9 maio 2016.

CANGIANO, Antonio Sérgio. **Nova entidade pretende difundir benefício do certificado digital**. 2015. Disponível em: <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=39793&post%2525255Fdata=&sid=18>. Acesso em: 18 maio 2016.

CERTIFIXE. **O que são cartórios?** 2016. Disponível em: <https://www.certidao.com.br/portal/cartorios/oquesao.php>. Acesso em: 19 jul. 2017.

CERTSIGN EXPLICA. **Portal de assinaturas**: uma forma fácil e rápida de assinar documentos on-line. 2014. Disponível em: <http://www.certisignexplica.com.br/portal-de-assinaturas-uma-forma-facil-e-rapida-de-assinar-documentos-on-line/>. Acesso em: 24 abr. 2016.

CORDEIRO, Luiz Gustavo. **Certificação digital**: conceitos e aplicações; modelo brasileiro e australiano. Rio de Janeiro: Ciência Moderna, 2008.

CORREIOS. Certificado digital. 2017. Disponível em: <http://www.correios.com.br/para-voce/correios-de-a-a-z/certificado-digital>. Acesso em: 20 mar. 2016.

E-SAJ. Portal de serviços. Poder judiciário do estado do acre – Tribunal de justiça. 2016. Disponível em: <http://esaj.tjce.jus.br/WebHelp/id_seguranca_da_informacao.htm>. Acesso em: 12 maio 2016.

GATES, Bill; MYHRVOLD, Nathan; RINEARSON, Peter. **A estrada do futuro**. Companhia das Letras, 1995.

ITI. Instituto Nacional de Tecnologia da Informação. **O que é?** 2016a. Disponível em: <http://www.iti.gov.br/icp-brasil/o-que-e >. Acesso em: 19 mar. 2016.

_____. Instituto nacional de tecnologia da informação. **Como funciona?** 2016b. Disponível em: <http://www.iti.gov.br/index.php/icp-brasil/como-funciona>. Acesso em: 20 mar. 2016.

_____. Instituto Nacional de Tecnologia da Informação. **ICP-Brasil**. 2016c. Disponível em: <http://www.iti.gov.br/icp-brasil>. Acesso em: 20 mar. 2016.

MONTEIRO, Emiliano S.; MIGNONI, Maria E. **Certificados digitais**: conceitos e práticas. Brasport, 2007.

PORTAL Q'CERTIFICA. Disponível em: <portal.qcertifica.com.br>. 2016. Acesso em: 4 jun. 2016.

QUALISIGN. **Conceito de assinatura digital**. 2005-2017. Disponível em: <www.documentoeletronico.com.br/assinatura-digital.asp>. Acesso em: 9 maio 2016.

SERASA EXPERIAN. **Certificado Digital**: Receita Federal inicia em junho o pagamento das restituições. 2014. Disponível em: <http://noticias.serasaexperian.com.br/blog/2014/05/15/receita-federal-inicia-em-junho-pagamentos-das-restituicoes-acompanhe-o-processamento-da-sua-declaracao-com-o-e-cpf-da-serasa-experian/>. Acesso em: 8 maio 2016.

SERPRO. **Serviço Federal de Processamento de Dados**. 2016. Disponível em: <http://portal.ouvidoria.fazenda.gov.br/mnoticias/serpro-lanca-assinador-digital>. Acesso em: 11 maio 2016.

SINDIFISCO NACIONAL. Sindicato Nacional dos Auditores Fiscais da Receita Federal do Brasil. **Certificação digital ganha novo fôlego no Brasil**. 2014. Disponível em: <www.sindifisconacional.org.br/index.php?option=com_content&view=article&id=24225:certificacao-digital-ganha-novo-folego-no-brasil&catid=45&Itemid=73>. Acesso em: 3 jun. 2016.

SODRÉ, Rodrigo. **Certificados Digitais ICP-Brasil em dispositivos móveis**. 2015. Disponível em: <https://cryptoid.com.br/certificacao-digital/certificados-digitais-icp-brasil-em-dispositivos-moveis/>. Acesso em: 3 jun. 2016.

SOFTPLAN. **Assinatura Digital de Documentos Eletrônicos no Brasil**: Conceitos Básicos e Infraestrutura. Disponível em: <http://www3.softplan.com.br/saj/downloads/cartilha_eletronica.pdf>. Acesso em: 27 mar. 2016.

TRT4. **Tribunal Regional do Trabalho Quarta Região**: Rio Grande do Sul. [s.d.]. Disponível em: <http://www.trt4.jus.br/content-portlet/download/68/certificado_digital_ins.pdf>. Acesso em: 12 maio 2016.

Artigo recebido em 30/05/17. Aceito em 10/07/17.