IV SIMTEC
Simpósio de Tecnologia da Fatec Taquaritinga

Certificação Digital: Conceitos e aplicações

Digital Certification: Conceptions and applications

Isabella Pegorete Mandetta de Souza – isabellapmdesouza@gmail.com
Brazelino Bertolete Neto – brazelino.neto@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (FATEC) – Taquaritinga – SP – Brasil

RESUMO

A certificação digital é uma tecnologia que permite que transações no meio digital sejam efetuadas com segurança, garantindo a integridade, confidencialidade, autenticidade e o não repúdio das informações. Os objetivos deste artigo foram: apresentar a definição de certificação digital e certificados digitais, explicar a classificação dos tipos de certificados digitais existentes quanto a aplicabilidade e requisitos de segurança, evidenciar o papel e a hierarquia da Infraestrutura de Chaves Pública Brasileira, fazer uma análise dos conceitos relacionados às tecnologias utilizadas no funcionamento dos certificados, tais como, assinatura digital, criptografia de chave pública e função resumo e mostrar algumas de suas possíveis aplicações com vantagens de uso. A metodologia foi baseada em pesquisas bibliográficas em livros com autores especialistas no assunto e sites oficiais, como o do próprio Instituto Nacional de Tecnologia da Informação. Os resultados finais obtidos demonstraram que devido ao seu funcionamento, a certificação digital consegue proporcionar transações eletrônicas mais seguras e numerosos benefícios para quem a utiliza.

Palavras-chave: Certificação Digital. Certificado Digital. Identidade Digital

ABSTRACT

Digital certification is a technology that allows transactions in the digital environment to be carried out safely, guaranteeing the integrity, confidentiality, authenticity and non-repudiation of information. The objectives of this article were: present the definition of digital certification and digital certificates, explain the classification of the types of digital certificates that exist in terms of applicability and safety requirements, highlight the role and hierarchy of the Brazilian Public Key Infrastructure, analyze the technologies used in the operation of the certificates, such as digital signature, public key cryptography and abstract function and show some of its possible applications with advantages of use. The methodology was based on bibliographical researches in books by specialized authors and official websites, such as the National Institute of Information Technology. The final results obtained demonstrated that due to its operation, digital certification can provide safer electronic transactions and numerous benefits for those who use it.

Keywords: Digital Certification. Digital Certificate. Digital Identity

1 INTRODUÇÃO

De acordo com Moreira (2009), uma das grandes dificuldades encontradas no meio digital, além dos diversos tipos de ataques digitais existentes, é comprovar que as partes envolvidas em uma transação eletrônica, negociação ou troca de mensagens, são realmente quem dizem ser e esses obstáculos se transformam em vulnerabilidades que possibilitam ataques, nos quais uma entidade se passa por outra confiável a fim de obter informações, privilégios ou bens de maneira ilícita. Assim, devido à necessidade de proteção contra as fraquezas existentes, foi desenvolvida a certificação digital.

A primeira seção deste artigo faz referência a base teórica relacionada à certificação digital, bem como a estrutura de um certificado digital, a definição e papel da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) e a classificação dos tipos de certificados existentes.

A segunda seção refere-se aos conceitos das tecnologias utilizadas no funcionamento de um certificado digital, como a criptografia assimétrica, função *hash* e assinatura digital. O terceiro capítulo diz sobre as vantagens do uso da certificação digital e alguns exemplos de sua aplicação, tratando sobre aqueles mais utilizados no cotidiano da população brasileira, isto é, os certificados e-CPF e e-CNPJ, e a NF-e (Nota Fiscal Eletrônica).

2 FUNDAMENTAÇÃO TEÓRICA

De acordo com Alecrim (2016), a certificação digital é uma tecnologia de identificação que permite que transações eletrônicas sejam realizadas considerando os aspectos da integridade, autenticidade e confidencialidade, de forma a evitar que adulterações, interceptações de informações privadas ou outros tipos de ações indevidas ocorram.

Ou seja, essa tecnologia funciona como uma espécie de “documento de identidade eletrônico” com validade jurídica e que garante a identificação e a proteção das partes envolvidas nas transações no meio eletrônico.

Azevedo e Mariano (2009 apud MOREIRA, 2009, p.17), explicam que Certificação Digital pode ser definida como “[...] a tecnologia que provê os mecanismos de segurança capazes de garantir autenticidade, confidencialidade e integridade às informações eletrônicas das mensagens e documentos trocados na Internet”.

2.1 Conceito de Certificado Digital

> Um Certificado Digital ou identidade digital é um arquivo digital de computador que, como os demais documentos tradicionais de identificação, além dos dados do indivíduo ou entidade, possuem também uma Chave Pública do assinante. Esses documentos eletrônicos são chancelados digitalmente pela entidade emissora, conhecida como Autoridade Certificadora, com o objetivo de interligar a Chave Pública a uma pessoa ou entidade, possuindo o mesmo valor de um documento físico, como carteira de identidade, passaporte, cartões de créditos e utilizados da mesma forma na identificação de indivíduos ou entidades na rede que, ao serem apresentados, servem como prova de identificação. (MONTEIRO e MIGNONI, 2007, p.15)

O certificado digital age 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, segundo o ITI (Instituto Nacional de Tecnologia da Informação) (2017).

Certificados digitais são arquivos digitais que estabelecem um elo entre um sujeito, que pode ser uma pessoa física ou empresa, e uma autoridade que tem o poder de certificação. O padrão mais difundido desta certificação é o X.509, atualmente na sua versão 3. (MARTINI, 2008)

Os campos que compõem um certificado digital na sua versão X.509 são descritos na Tabela 1 abaixo.

Tabela 1 – Descrição dos campos de um certificado no formato X.509 v3.

Campos	Descrição
Versão	Número da versão X.509 do certificado.
Número de série	Identificador único do certificado e representado por um inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma AC.
Algoritmo de Assinatura da AC	Identificador do algoritmo usado para assinatura do certificado pela AC.
Nome do Emissor	Nome da AC que produziu e assinou o certificado.
Período de Validade	Intervalo de tempo que determina até quando um certificado deve ser considerado válido
Nome do sujeito	Identifica o dono do Certificado
Chave Pública do	Contém o valor da chave pública do certificado junto com informações

Sujeito	de algoritmos com o qual a chave deve ser usada.
ID único do Emissor	Campo para permitir o reuso de um emissor com o tempo.
ID único do Sujeito	Campo para permitir o reuso de um sujeito com o tempo.
Extensões	Campos complementares para personalizar um Certificado

Fonte: Silva et al. (apud Moreira, 2009, p. 20-21)

2.2 ICP – Brasil

Segundo o ITI (2017), "a ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão".

A ICP-Brasil foi instituída pela Medida Provisória 2.200-2 de 24 de agosto de 2001. O modelo brasileiro adotado é o de certificação com raiz única, sendo que a ICP-Brasil, além de desempenhar o papel de AC-Raiz (Autoridade Certificadora Raiz), também tem o papel de credenciar e descredenciar os demais participantes, supervisionar e fazer auditoria dos processos, emitir, expedir, distribuir, revogar e gerenciar os certificados das ACs (Autoridades Certificadoras). (ITI, 2017)

Para a AC de 1º nível Certisign, a ICP-Brasil é "um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais".

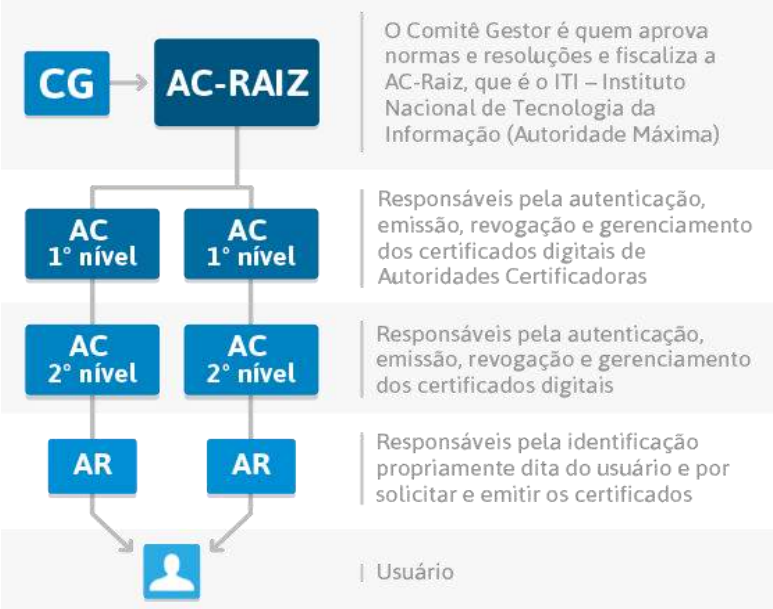
"A ICP-Brasil assume certos critérios objetivos: tem como base modelos de auditoria, baseia-se em padrões abertos e estabelece regra públicas mantidas por Comitês. Trata-se, como foi assinalado, de um sistema de confiança [...]". (MARTINI, 2008, p.37)

Segundo Silva et al. (2008 apud Moreira, 2009, p. 25):

> A adoção da tecnologia de chaves públicas requer uma infraestrutura de chaves públicas (ICP) que define o conjunto de padrões utilizados, autoridades certificadoras, estrutura entre autoridades certificadoras, métodos para validar certificados, protocolos de operação, protocolos de gerenciamento, ferramentas de interoperabilidade e suporte legislativo.

A seguir, a Figura 1 especifica e traz as funções dos níveis de autoridade que compõem a ICP-Brasil.

Figura 1 – Hierarquia da ICP-Brasil



Fonte: Benefícios da Certificação Digital (2013)

2.3 Tipos de Certificado Digital

Segundo a ICP-Brasil, existem três tipos de certificados digitais, que são classificados quanto a sua aplicabilidade e requisitos de segurança à Chave Privada. Quanto à aplicação os certificados ICP-Brasil são classificados como:

- **Certificados Tipo A – Assinatura Digital:** Conforme explica Brocardo (2016), este é o tipo de certificado mais utilizado. Serve para realizar assinaturas digitais em todos os tipos de documentos, transações eletrônicas, entre outras aplicações. Tem como funções identificar o assinante, atestar a autenticidade da operação e confirmar a integridade do documento assinado. Os certificados tipo A mais utilizados são o A1 e o A3.
- **Certificados Tipo S – Sigilo:** Este tipo de certificado digital é utilizado exclusivamente para proporcionar sigilo à transação. Possibilita criptografar os dados de um documento, que passa a ser acessível somente com a utilização de um certificado digital autorizado para abrir o arquivo. É usado para o envio de informações de forma segura, mantendo em sigilo o seu conteúdo. (BROCARDO, 2016)

- **Certificados Tipo T – Tempo:** Segundo Brocardo (2016), os certificados do tipo T são definidos da seguinte maneira:

> O certificado digital do tipo T é mais conhecido como carimbo do tempo, ou *timestamp*. O carimbo de tempo é um documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado. O carimbo do tempo busca a informação de data e hora de uma terceira parte segura, que é uma fonte confiável para atestar corretamente estas informações. É utilizado em conjunto com os outros tipos de certificados digitais e é essencial para garantir a temporalidade e a tempestividade de documentos importantes.

De acordo com a ICP-Brasil, quanto aos requisitos de segurança, os certificados digitais são classificados de acordo com a Tabela 2 abaixo.

Tabela 2 – Classificação dos certificados Digitais quanto à segurança

Tipo	Tamanho da Chave	Geração do Par de Chaves	Validade máxima do certificado
A1/S1	2048	Software	**1 ano**
A3/S3	2048	Hardware	**Até 5 anos**
A4/S4	4096	Hardware	**Até 6 anos**

Fonte: Benefícios e Aplicações da Certificação Digital (2013)

Segundo Alecrim (2016), o armazenamento do par de chaves por hardware é feito em cartão inteligente (*smart card*) com chip ou *token* USB (dispositivo semelhante a um *pendrive*) protegidos por senha, como ilustra a Figura 2. "O sistema ICP-Brasil tem um protagonista essencial, a saber, *smart card*, o cartão com chip ISO-7816. Nele a chave privada é gerada e nele é armazenada, sem nunca usar a memória volátil do sistema, o que, por fim, lhe ajuda a garantir mais segurança". (MARTINI, 2008, p.39)

Figura 2 – Cartão inteligente (*smart card*) e *token* USB



Fonte: Certisign (2017)

Para o caso de se utilizar o cartão inteligente, também é necessária a leitora de cartão, como a da Figura 3, que é conectada via USB.

Figura 3 – Leitora de cartão inteligente



Fonte: Certisign (2017)

3 PROCEDIMENTOS METODOLÓGICOS

A Certificação Digital utiliza a tecnologia de Chave Pública, que é armazenada no certificado, enquanto a Chave Privada é guardada em sigilo pelo assinante. Assim, qualquer mensagem pode ser assinada usando a Chave Privada do assinante, mas essa assinatura digital só pode ser validada ser for correspondente com a sua Chave Pública. (MONTEIRO e MIGNONI, 2007).

3.1 Criptografia de Chave Pública

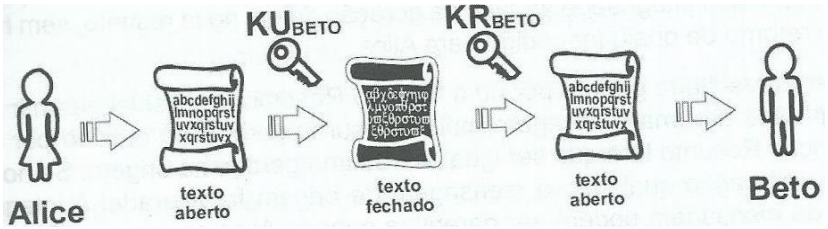
Os certificados digitais são de chave pública e garantem que uma determinada chave pública pertence a um sujeito. A AC possui sua própria chave privada correspondente que assinou e emitiu o certificado. Assim, ela pode autenticar que os proprietários dos certificados são quem realmente dizem ser e protegem os dados partilhados em rede de fraudes e roubos com o uso da encriptação. (MARTINI, 2008)

Segundo Stallings (2008, p.187), a criptografia de chave pública ou assimétrica pode ser caracterizada da seguinte forma:

> Os sistemas de chave pública são caracterizados pelo uso de um algoritmo criptográfico com duas chaves, uma mantida privada e uma disponível publicamente. Dependendo da aplicação, o emissor utiliza a chave privada do emissor ou a chave pública do receptor, ou ambas, para realizar algum tipo de função criptográfica.

A Figura 4 mostra o esquema de funcionamento da criptografia assimétrica.

Figura 4 – Criptografia Assimétrica



Fonte: Monteiro e Mignoni (2007, p.7)

Alice deseja enviar uma mensagem cifrada para Beto, usando a Chave Pública KUBeto dele para cifrar o texto. Após receber a mensagem cifrada, Beto deve decifrar a mensagem e, para isso, ele utiliza a sua Chave Privada KRBeto e torna o texto legível.

Para Alecrim (2016), o esquema de funcionamento das chaves na criptografia de chave pública considera dois aspectos importantes: confidencialidade e autenticidade. A confidencialidade consiste em tornar a informação acessível somente a pessoas ou organizações autorizadas e a autenticidade assegura ao receptor que a informação provém da origem e forma esperadas.

O uso da criptografia assimétrica garante um maior sigilo e segurança das informações transmitidas entre emissor e destinatário, conforme explica Moreira:

> Com o uso da chave pública de uma pessoa garantimos a confidencialidade e integridade da mensagem, ou seja, apenas a possuidora da chave privada será capaz de decifrar a mensagem original. Ao usar a chave privada para cifrar uma mensagem constata-se a funcionalidade da assinatura digital, ou seja, é garantido a autoria e o não-repúdio da mesma. MOREIRA (2009, p. 13-14)

3.2 Função *Hash*

A Função Resumo (ou simplesmente *HASH*, em inglês) é um algoritmo que recebe de entrada uma mensagem de tamanho qualquer e gera um resumo de tamanho fixo, que representa o conteúdo da mensagem. Ela tem como objetivo produzir uma "impressão digital" da mensagem, conforme explicam Monteiro e Mignoni (2007).

> O código de *hash* também é conhecido como síntese de mensagem ou valor de *hash*. O código de *hash* é uma função de todos os bits da mensagem e oferece uma capacidade de detecção de erros: uma mudança em qualquer bit ou bits na mensagem resulta em uma mudança no código de *hash*. (STALLINGS, 2008, p.234)

Segundo a Cartilha de Segurança para Internet (2016), para verificar a integridade de um arquivo o valor de *hash* pode ser calculado, e quando julgar necessário, deve-se calcular novamente esse valor. Se os dois valores gerados forem iguais então, conclui-se que o arquivo não foi alterado. Caso contrário, há um forte indício de que o arquivo foi corrompido ou modificado.

3.3 Assinatura Digital

Monteiro e Mignoni (2007, p.10) definem Assinatura Digital como "Um algoritmo de autenticação, que possibilita ao criador de um objeto unir ao objeto criado um código que irá agir como uma assinatura". Isso confirmaria que o objeto não foi alterado e permitiria identificar o seu assinante, garantindo a autenticação da assinatura.

> Uma assinatura digital é um mecanismo de autenticação que permite ao criador de uma mensagem anexar um código que atue como uma assinatura. A assinatura é formada tomando o *hash* da mensagem e criptografando-a com a chave privada do criador. A assinatura garante a origem e a integridade da mensagem. (STALLINGS, 2008. p. 272)

Para que a assinatura escrita possa ser substituída pela assinatura digital, Tanenbaum (2003 apud MOREIRA, 2009, p. 15) explica que a técnica precisa atender aos seguintes requisitos:

- O Receptor possa verificar a identidade alegada pelo transmissor;
- O transmissor não possa repudiar o conteúdo da mensagem enviada;
- O receptor não possa ser capaz de adulterar a mensagem recebida.

O processo de assinatura digital está ilustrado na Figura 5 abaixo.

Figura 5 – Processo de Assinatura Digital



Fonte: Monteiro e Mignoni (2007, p.10)

Para criar uma Assinatura Digital, Alice faz uma função *hash* e cifra o resultado dela com a sua Chave Privada. Ela então envia o texto e seu resumo cifrado para Beto. Ele decifra o resumo com a Chave Pública de Alice, executa novamente a função *hash* do documento e compara os dois resultados originados. Se forem iguais, a assinatura digital é válida.

4 RESULTADOS E DISCUSSÃO

Para Moreira (2009, p.42), a utilização da certificação digital garante às pessoas, empresas, softwares ou computadores uma maior segurança nas suas atividades no meio digital. Assegurando a integridade, autenticidade, confidencialidade, disponibilidade e não-repúdio das informações disponibilizadas.

Segundo o ITI (2017), a certificação digital permite que aplicações como comércio eletrônico, assinatura de contratos digitais, operações bancárias virtuais, iniciativas de governo eletrônico, entre outras, sejam realizadas. Com o certificado digital é possível realizar uma série de procedimentos, virtualmente, sem a necessidade de se deslocar presencialmente à sede de órgãos governamentais e de empresas ou imprimir documentos, tais como:

- **Assinatura de documentos e contratos digitais:** os documentos assinados digitalmente com certificado digital têm a mesma validade que os documentos assinados em papel. Além de proporcionar economia de insumos, os documentos assinados digitalmente agilizam processos, pois podem ser enviados por *e-mail* e assinados de qualquer lugar facilmente;
- **Autenticação em sistemas:** há muitos sistemas com informações confidenciais, que só podem ser acessados presencialmente, através da confirmação de identidade. Como o certificado digital garante autenticidade, ele proporciona o acesso a esses sistemas e informações através da internet, não havendo necessidade de comparecimento presencial;
- **Atualização de informações em sistemas:** Além de garantir acesso seguro aos sistemas, o certificado também permite a alteração rápida de informações, evitando longos processos burocráticos;
- **Categorias profissionais:** diversas categorias profissionais (médicos, advogados, contadores, militares, entre outros) já utilizam o certificado digital em suas rotinas. Com o certificado, as classes profissionais têm a possibilidade

de trabalhar com sistemas virtuais unificados e seguros, proporcionando integração e desburocratização de processos relativos ao setor.

4.1 NF-e

Segundo Alecrim (2016), a NF-e é um tipo de documento fiscal em formato digital que serve para registrar a transferência de propriedade de um bem ou serviço comercial prestado a empresas e pessoas físicas. O autor ainda explica que desde 2007, a NF-e é parte do chamado SPED (Sistema Público de Escrituração Digital) e é de uso obrigatório no Brasil. Por conta disso, a NF-e tem validade fiscal e jurídica. Essa validade é garantida por assinatura digital.

Para a Valid Certificadora Digital, que é uma AC de 1º nível, o certificado NF-e é destinado à pessoa jurídica e permite a emissão de notas fiscais eletrônicas e, além de garantir que os dados emitidos são verdadeiros, esse certificado digital permite o acompanhamento das notas fiscais emitidas em tempo real.

> A NF-e nada mais é que um documento eletrônico no sentido próprio da palavra, e que receberá uma assinatura digital a partir de um certificado digital ICP-Brasil, com o fito de lhe dar validade jurídica [...] O projeto da NF-e tem como objetivo a implantação de um modelo nacional de documento fiscal eletrônico que venha substituir a sistemática atual da emissão do documento fiscal em papel, com validade jurídica garantida pela assinatura digital do remetente [...] (MARTINI, 2008, p. 67)

4.2 e-CPF e e-CNPJ

Os tipos de certificados mais conhecidos e utilizados no Brasil são o e-CPF e o e-CNPJ, ambos certificados de assinatura digital. O e-CPF é destinado a pessoas físicas e é um tipo de extensão do CPF (Cadastro de Pessoa Física). (ALECRIM, 2016)

Para a Valid Certificadora Digital, o e-CPF, “é um documento digital que garante a autenticidade e assegura que as informações e dados dos remetentes e destinatários possam trafegar pela Internet com segurança”. Além disso, o e-CPF também pode ser utilizado como assinatura digital, ou seja, permite a verificação da identidade do signatário com a garantia de que o documento não foi alterado após a assinatura.

De acordo com a Valid Certificadora Digital, o e-CPF permite:

- Assinar contratos;

- Fazer procurações eletrônicas;
- Acessar o site da Receita Federal e resolver questões pendentes diretamente no sistema;
- Ter acesso a serviços exclusivos oferecidos por empresas que trabalham com o certificado digital;
- Ter acesso a áreas exclusivas de sites que exigem a certificação digital.

Já o e-CNPJ é um certificado digital para pessoas jurídicas, a empresas e instituições, de igual forma, sendo um tipo de extensão do CNPJ (Cadastro Nacional da Pessoa Jurídica), e ele permite validar transações jurídicas, conforme explica Alecrim (2016).

Conforme ainda explica a Valid Certificadora Digital, o e-CNPJ é garante a autenticidade e integridade das transações da pessoa jurídica. Com ele é possível:

- Fazer procurações em ambiente digital;
- Acessar o site da Receita Federal e resolver questões pendentes diretamente no sistema;
- Ter acesso a serviços exclusivos oferecidos por empresas que trabalham com o certificado digital.

Alecrim (2016) ainda ressalta: “É importante destacar que o e-CPF e o e-CNPJ não são gratuitos. Sua aquisição deve ser feita em entidades conveniadas à Receita Federal, como Certisign e Serasa. Os preços não são padronizados, variando de acordo com a instituição fornecedora e o tipo de certificado”.

5 CONSIDERAÇÕES FINAIS

Pode-se afirmar ao final deste artigo que devido à crescente utilização do meio digital pela sociedade, tornam-se necessárias tecnologias eficientes e seguras. Os objetivos propostos no início desta pesquisa foram atingidos, pois a certificação digital é uma ferramenta que consegue garantir uma maior preservação e segurança das informações contidas em transações eletrônicas por meio da utilização da criptografia assimétrica, proporcionando confidencialidade e assegurando que as informações em transação serão mantidas em sua forma original. A assinatura digital também tem um papel fundamental, porque com ela é possível identificar, por meio da assinatura, o autor da mensagem e a função *hash* certifica que as mensagens enviadas não serão alteradas.

O segundo propósito, que era descrever as categorias de certificados digitais existentes, foi alcançado, porque pode-se ver ao longo do trabalho que o uso dos tipos de certificados digitais está diretamente relacionado às necessidades do seu utilizador, pois cada classificação de certificado é recomendada para uma determinada tarefa e usuário. A terceira proposta da pesquisa, que era apresentar os modos de utilização dos certificados, também foi atingida, pois o trabalho demonstra o uso mais comum através dos certificados de assinatura digital. No Brasil, a certificação digital é utilizada em crescente escala, pois dados do ITI afirmam que do período de janeiro a setembro deste ano foram emitidos 2.693.298 certificados nos tipos e-CPF e o e-CNPJ pela ICP-Brasil.

Nesse sentido, também é possível perceber que a existência da ICP-Brasil garante confiança e segurança às práticas envolvendo as chaves privadas dos certificados, além de tornar válidos os documentos digitais, emitir os certificados e gerenciar as ACs.

As aplicações da certificação digital trazem inúmeros benefícios para todos que a utilizam. Suas vantagens estão ligadas à redução de custos e insumos, agilidade nos processos realizados e maior eficiência no gerenciamento das operações eletrônicas realizadas diariamente.

REFERÊNCIAS

ALECRIM, Emerson. **O que é Certificação Digital?**. Disponível em: <https://www.infowester.com/assincertdigital.php>. Acesso em: 12 set. 2017

BROCARDO, Marcelo Luiz. **Tipos de certificados digitais**. Disponível em: <https://blog.bry.com.br/tipos-de-certificados-digitais/>. Acesso em: 16 set. 2017.

BENEFÍCIOS E APLICAÇÕES DA CERTIFICAÇÃO DIGITAL. Apresenta informações sobre: conceitos da certificação e classificação dos certificados digitais, hierarquia da ICP-Brasil e utilização dos certificados digitais. Disponível em: http://www.beneficioscd.com.br/>. Acesso em 03 out. 2017.

CARTILHA DE SEGURANÇA PARA INTERNET. Apresenta informações sobre: recomendações de como os usuários devem se comportar para aumentar sua segurança e se proteger de possíveis ameaças. Disponível em: <https://cartilha.cert.br/>. Acesso em 05 jun. 2017.

CERTISIGN. Apresenta informações sobre: produtos de certificado digital fornecidos pela autoridade certificadora, informações relacionados a certificação digital e recomendações de

uso dos certificados. Disponível em:< https://www.certisign.com.br/>. Acesso em 10 set. 2017

INFOSEC INSTITUTE. Apresenta informações sobre: treinamentos na área de segurança da informação e conceitos da área de segurança da informação. Disponível em: < http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/the-security-cia-triad/#gref>. Acesso em 07 jun. 2017.

ITI – INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. Apresenta informações sobre: ICP-Brasil e sua estrutura, certificação digital e dados relacionados a emissão de certificados. Disponível em: <http://www.iti.gov.br/>. Acesso em 12 set. 2017.

MARTINI, Renato da Silveira. **Tecnologia e Cidadania Digital:** ensaio sobre tecnologia, sociedade e segurança. Rio de Janeiro: Brasport, 2008.

MONTEIRO, Emiliano S.; MIGNONI, Maria Eloisa. **Certificados digitais:** conceitos e práticas. Rio de Janeiro: Brasport, 2007.

MOREIRA, Danilo Gomes. **A CERTIFICAÇÃO DIGITAL NA SOCIEDADE DA INFORMAÇÃO BRASILEIRA**. 2009. 56 f. Trabalho de Conclusão de Curso (Bacharelado em Sistemas de Informação) – Faculdades Unificadas Doctum de Cataguases, Cataguases, 2009. Disponível em: <https://pt.slideshare.net/danilogmoreira/monografia-oficial-danilo-gomes-moreirav2>. Acesso em: 20 mai. 2017.

RED HAT ENTERPRISE LINUX 4. **Guia de Segurança.** Disponível em: <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/index.html>. Acesso em 07 jun. 2017.

STALLINGS, William. **Criptografia e segurança de redes:** princípios e práticas. 4. ed. Tradução de D. Vieira. Revisão técnica de A. Barbosa e M. Succi. São Paulo: Pearson Prentice Hall, 2008.

VALID CERTIFICADORA. Apresenta informações sobre: produtos de certificado digital fornecidos pela certificadora, bem como dados e informações relacionados a certificação digital e segurança da informação. Disponível em:<http://blog.validcertificad ora.com.br/>. Acesso em 12 set. 2017