FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Amanda Pereira da Silva

CARACTERÍSTICAS E BENEFÍCIOS DA CERTIFICAÇÃO DIGITAL APLICADA AO INTERNET BANKING

Americana, S. P.

2014

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Amanda Pereira da Silva

CARACTERÍSTICAS E BENEFÍCIOS DA CERTIFICAÇÃO DIGITAL APLICADA AO INTERNET BANKING

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Profº Tecgº Marcus Vinícius Lahr Giraldi.
Área de concentração: Certificação Digital.

Americana, S. P.

2014

Silva, Amanda Pereira da

S578c Características e benefícios da certificação digital aplicada ao Internet Banking. / Amanda Pereira da Silva. – Americana: 2014.

69f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Marcus Vinícius Lahr Giraldi

1.Sistemas de informação 2. Comércio eletrônico I. Giraldi, Marcus Vinícius Lahr II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518
658.845

Amanda Pereira da Silva

CARACTERÍSTICAS E BENEFÍCIOS DA CERTIFICAÇÃO DIGITAL APLICADA AO INTERNET BANKING

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Certificação Digital.

Americana, 04 de junho de 2014.

Banca Examinadora:

_____
Marcus Vinícius Lahr Giraldi – (Presidente)
Tecnólogo
FATEC Americana

_____
Maria Cristina Aranda Batocchio – (Membro)
Doutora
FATEC Americana

_____
Gabriel de Souza Fedel – (Membro)
Mestre
FATEC Americana

“O que somos é presente de Deus para nós;
no que nos transformamos é o nosso
presente para Ele”

(Dom Bosco)

RESUMO

Nos últimos anos é visível como a tecnologia da informação está presente de forma ativa no dia a dia das pessoas, empresas e órgãos públicos. A grande maioria de processos e transações que eram realizados pessoalmente ou através de meios físicos, como por exemplo agências bancárias e terminais de autoatendimento, deu espaço a facilidade e comodidade apresentada pelos meios eletrônicos, em especial a internet. O ambiente web está sendo utilizado como uma vitrine com alta visibilidade de dados corporativos e produtos e tornou-se a plataforma do comércio eletrônico. Diante deste cenário e com o crescente número de transações realizadas pela web, principalmente com valor financeiro associado, a busca por serviços de maior segurança é elevada. A certificação digital é a tecnologia atual que atende com maior êxito os princípios básicos da segurança da informação, sendo eles: confidencialidade, integridade, autenticidade e disponibilidade dos dados que circulam via web. O objetivo deste trabalho é elaborar um estudo sobre as características e benefícios da certificação digital no ambiente de internet banking, para tanto foi realizado um estudo bibliográfico em livros, artigos, monografias, teses, dissertações e cartilhas pertinentes a área de estudo para a apresentação e definição de conceitos como: criptografia, RSA, funções hash, assinatura digital, certificação digital, ICP-Brasil, sistemas de internet banking entre outros. Por fim para desenvolvimento da pesquisa de campo e discussão dos resultados que serão apresentados ao final do trabalho, foi elaborado um questionário para coleta de dados da população em geral, esta que direta ou indiretamente esta inserida na era da tecnologia da informação.

Palavras-chave: Segurança da informação; Certificação Digital; Internet Banking.

ABSTRACT

Currently is notable how the information technology is actively present in people's lives, business and public agencies. The vast majority of cases and transactions that were conducted by person or by physical media, such as bank branch and automated tells machine, they were changed by facility and convenience presented by electronic devices, especially the internet. The web environment has been used as a showcase with high visibility of enterprise data and product and it has become the platform of e-commerce. Given this scenario and the increasing number of transactions on the Web, mainly associated with financial value, the search for greater security services is high and growing. Digital certification is current technology that contemplates with greater success the basic principles of information security, namely: confidentiality, integrity, authenticity and availability of data circulating on web. The aimed of this paper is prepare a study about the technical features of Digital Certification in Internet Banking. To perform this, a study was made based on books, articles, monographs, theses, dissertations and textbooks for the presentation of concepts such as: cryptography, RSA, *hash* functions, digital signatures, digital certificates, PCI-Brazil, internet banking systems and others more. Finally for the development of field research and discussion of the results that will be presented at the end of the work, a questionnaire for collecting data from the general population was realized, because they are directly or indirectly inserted in the era of information technology.

Keywords: Information Security; Digital Certification; Internet Banking.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
ACR	Autoridade Certificadora Raiz
AES	*Advanced Encryption Standard* (Padrão de Encriptação Avançado)
AR	Autoridade de Registro
CG	Comitê Gestor
CG-ICP	Comitê Gestor da Infra Estrutura de Chaves Públicas
COTEC	Comitê Técnico
DES	*Data Encryption Standard* (Padrão de Encriptação de Dados)
e-CNPJ	Cadastro Nacional de Pessoa Jurídica eletrônico
e-CPF	Cadastro de Pessoa Física eletrônico
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
ICP	Infra estrutura de Chaves Públicas
ICP-Brasil	Infra estrutura de Chaves Públicas do Brasil
ITI	Instituto Nacional de Tecnologia da Informação
MP	Medida Provisória
NF-e	Nota Fiscal eletrônica
PKI	*Public Ky Infrastructure* (Infra estrutura de Chaves Públicas)
SSL	*Secure Sockets Layer*

SUMÁRIO

1. INTRODUÇÃO

Ao longo dos últimos anos é possível observar as mudanças em processos que até então eram realizados pessoalmente ou com auxílio de meio físico por meios digitais, tornando-se cada vez mais comum o relacionamento entre pessoas através de computadores, rede de computadores e internet.

A partir da segunda metade do século XX, vivencia-se a terceira revolução tecnológica também denominada revolução digital, cujo principal objetivo é o da redução do esforço mental, tendo como base que a primeira revolução tecnológica que ocorreu no final do século XVIII cumprindo seu objetivo de reduzir o esforço físico do homem (SANTOS, 2006).

A demasiada disseminação da internet impacta direta e indiretamente a vida de muitas pessoas, sendo crescente seu número. Milhares de processos são realizados diariamente através da internet, como por exemplo utilização de e-mails, e-commerce, home banking, declaração de imposto de renda, troca de documentos eletrônicos através da identidade digital.

Devido ao número crescente de transações realizadas por meio eletrônico, principalmente aquelas com valor financeiro associado, a palavra de ordem da atualidade é a segurança da informação. É necessário assegurar que a facilidade proporcionada pelos meios eletrônicos garanta a segurança dos processos realizados e integridade dos dados emitidos. Esta problemática induz pesquisadores na busca de soluções mais seguras; tornando-se necessário o desenvolvimento de novas tecnologias que atendam os requisitos de segurança, considerando que as tradicionais já não suportam (MONTEIRO; MIGNONI, 2007, p.16).

A certificação digital é definida pelo ITI (2003, p. 7)[1] como "Conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos."

Ao tratar de segurança da informação, quatro princípios básicos devem ser considerados: confidencialidade, integridade, autenticidade e disponibilidade. Conceitos e técnicas de criptografia e certificação digital são tecnologias de maior êxito que atendem os princípios básicos de segurança.

---

1 ITI–Instituto Nacional de Tecnologia da Informação. Brasília, DF. Certificação Digital: Entenda e Utilize. Instituto Nacional de Tecnologia da Informação. 2003. Disponível em: <http://www.iti.gov.br/publicacoes/cartilhas/3893-certificacao-digital-entenda-e-utilize>. Acesso em: 29 Ago. 2013.

1.1. Objetivos

O objetivo deste trabalho é ressaltar os processos de certificação digital, indicando as principais características e benefícios de seu uso nos sistemas de internet banking, considerando a integridade, disponibilidade e confidencialidade da informação, que é o maior ativo de uma organização.

Pesquisa de campo e outras investigações sobre o tema foram realizadas a fim de produzir uma verídica discussão e conclusão dos argumentos apresentados.

1.2. Metodologia de Desenvolvimento

Baseado na pesquisa bibliográfica feita com autores renomados em livros, artigos, monografias, teses e dissertações da área de estudo, este trabalho tem como principal objetivo apresentar detalhadamente conceitos e técnicas de criptografia e certificação digital e sua aplicação no ambiente de *internet banking*, a fim de demonstrar como a certificação digital é capaz de aumentar o grau de segurança das informações envolvidas nas transações bancárias; informações estas de extrema importância por estarem associadas a valor financeiro.

O capítulo 2 fornece uma ampla explanação sobre criptografia dos dados, técnicas de criptografia simétrica e assimétrica, RSA, funções *hash* e assinatura digital.

A certificação digital é o assunto do capitulo 3 e todos seus conceitos relacionados como a infra-estrutura de chaves públicas, autoridade certificadora, autoridades de registro, padrão x.509, ciclo de vida do certificado, protocolos SSL e HTTPS, ICP-Brasil, tipos de certificados e algumas das principais aplicações da certificação digital compõem este capítulo.

No capitulo 4 é feita toda a explanação sobre a segurança do *internet banking*, a realidade do *internet banking* brasileiro, evolução das fraudes, gerenciamento de riscos e modelos de segurança adotados no ambiente de *internet banking*.

Por fim, com intuito de aumentar a veracidade dos argumentos expostos em todo o trabalho, foi desenvolvido um questionário com perguntas direcionadas ao publico em geral para ser utilizados como pesquisa de campo e de acordo com as respostas, gráficos foram elaborados para dinamizar as discussões e conclusão ao final do trabalho.

2. CRIPTOGRAFIA

Utilizado inicialmente para fins militares, os processos criptográficos estão presentes na história da humanidade desde tempos antigos. O termo criptografia é originário da fusão das palavras gregas “kryptós” e “gráphein” que significam “oculto” e “escrever”, respectivamente.

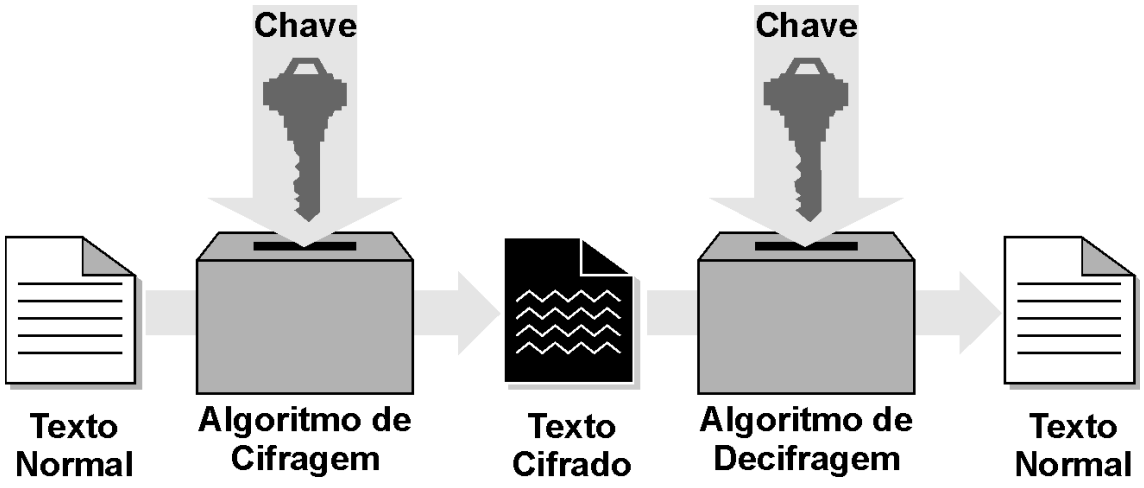
De acordo com Monteiro e Mignoni (2007, p. 22), “a criptografia consiste na arte de escrever em cifras ou em códigos não decifráveis a olhos nus.”

Já Silva et al (2008), explicam de forma simples a criptografia como a ciência capaz de fazer com que o custo para obter uma informação de maneira inoportuna seja maior que o custo obtido com a informação propriamente dita.

Considerada a base da certificação digital, a criptografia fornece técnicas e mecanismos capazes de converter uma mensagem de seu formato original para um formato ininteligível, inibindo o acesso não autorizado aos dados e assegura a confidencialidade e autenticação dos mesmos. Operações matemáticas responsáveis pela efetivação dos processos de cifragem e decifragem são denominados algoritmos criptográficos.

Criptografar, cifrar, codificar ou encriptar são termos sinônimos que definem o processo de conversão da mensagem original (texto claro) para um formato de mensagem ininteligível (texto cifrado) utilizando um algoritmo criptográfico e uma chave criptográfica. Para a recuperação da mensagem original utiliza-se o processo inverso, denominado descriptografar, decriptografar, decifrar ou decodificar que é o processo que retorna ao seu formato original, dados previamente cifrados (BRAGA, 2008, p. 42). A figura 1 ilustra o processo citado.

Figura 1: Cifragem e Decifragem de uma mensagem



Fonte: Trinta; Macedo (1998).

No conceito de criptografia moderna, a chave criptográfica a ser utilizada tem grau de relevância imediatamente superior ao próprio algoritmo criptográfico, as principais utilizadas são: chave simétrica e chave assimétrica (chave pública).

De acordo com Luz (2008), define-se chave criptográfica (similar a uma senha) como um valor matemático determinante que produz um texto cifrado a partir do texto claro. Para o processo inverso é necessário o conhecimento da chave criptográfica, assim é possível retornar o texto cifrado no texto original. O tamanho da chave é determinado pelo número de *bits* necessários em seu armazenamento, quanto maior o número de *bits*, mais difícil será sua descoberta.

Segundo Monteiro e Mignoni (2007) existem alguns conceitos básicos na segurança da informação, os quais são possíveis através de métodos criptográficos atingir:

- **Autenticidade:** Garante a origem da informação e permite a comprovação da origem.
- **Integridade:** Garante a acurácia e a certeza que a informação não foi modificada de maneira acidental ou não autorizada.
- **Confidencialidade:** Assegura o acesso a informação, somente para pessoas autorizadas.
- **Não repúdio:** Não será possível ao emissor, negar a autoria da mensagem.

Os princípios citados acima devem ser considerados em todos os contextos onde existe informação, inclusive em meio digital, afinal, grande parte das empresas atualmente tem suas informações mais valiosas armazenadas em servidores, computadores e em locais que sequer sabem onde é: as nuvens.

2.1. Criptografia Simétrica

Denominada também como criptografia de chave única, a criptografia simétrica tem como principal característica a utilização da mesma chave nos processos de criptografia e descriptografia. Com este processo é possível transformar o texto claro em texto cifrado utilizando um algoritmo de criptografia e uma chave secreta, para retomar o texto cifrado em texto claro utiliza-se um algoritmo de descriptografia e a mesma chave secreta (STALLINGS, 2008).

Ainda de acordo com Stallings (2008), nos tempos antigos, anterior ao uso do computador, as tradicionais cifras simétricas utilizavam técnicas de substituição e/ou transposição. Técnicas de substituição delineiam elementos do texto legível (caracteres, bits) em elementos de texto cifrado, já as técnicas de transposição transpõem as posições dos

elementos do texto claro. A cifra simétrica mais conhecida e utilizada ao longo de anos é o DES (*Data Encryption Standard*) que foi substituída pelo 3DES e logo após pelo AES (*Advanced Encryption Standard*).

O autor também relata que há duas técnicas para o ataque à criptografia simétrica, são elas:

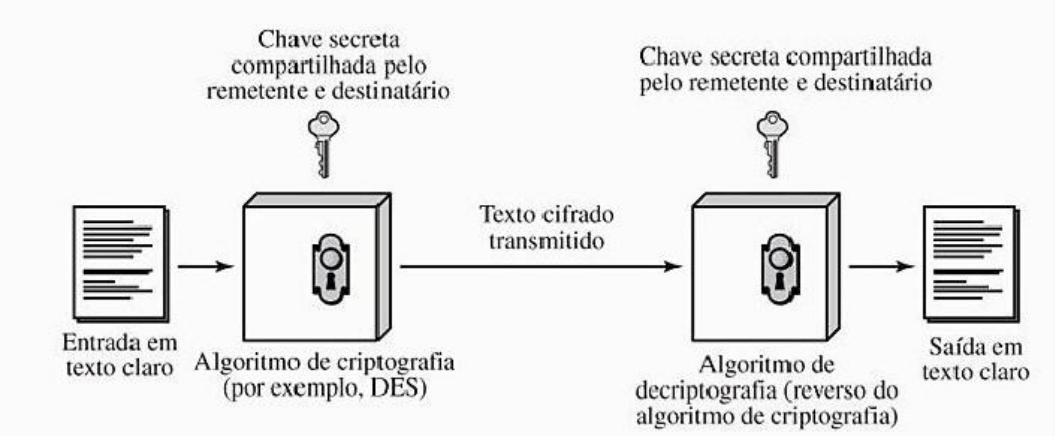
Criptoanálise: Utiliza o processo usualmente denominado "quebra do código" que através de técnicas matemáticas tem como principal objetivo decifrar informações cifradas, sem o conhecimento prévio da chave de criptografia.

Força bruta: Considerada por estudiosos como a forma menos eficiente, tenta descobrir a chave criptográfica através de inúmeras tentativas de todas as combinações possíveis e quanto maior o tamanho da chave, mais complexo é o seu descobrimento por esta técnica.

Segue abaixo o esquema de criptografia simétrica, apresentado na figura 2, onde:

I. **Texto claro:** Mensagem original que constará no algoritmo de criptografia como entrada.
II. **Algoritmo de criptografia:** Processo responsável por realizar substituições e transformações na mensagem original (texto claro).
III. **Chave secreta:** Elemento de entrada do algoritmo de criptografia, a chave é definida por técnicas matemáticas e de acordo com a chave específica utilizada é determinada a saída do texto cifrado.
IV. **Texto cifrado:** Mensagem ilegível, produzida como saída do algoritmo, ela depende diretamente da mensagem original e chave criptográfica utilizada no processo.
V. **Algoritmo de descriptografia:** Processo inverso do algoritmo de criptografia que retorna a mensagem ilegível para a mensagem original.

Figura 2: Modelo de criptografia simétrica.



Fonte: Stallings (2008).

Na criptografia simétrica o sigilo dos dados encontra-se na chave criptográfica utilizada. O algoritmo criptográfico poderá ser do conhecimento de terceiros, porém só é possível retornar uma mensagem em seu formato original com a posse da chave correta. Neste cenário o grande problema de segurança da informação encontrado é compartilhar a chave criptográfica em segredo.

2.2. Criptografia Assimétrica

Após a criptografia simétrica, em 1976 foi apresentado por *Whitfield Diffie e Martin Hellman* no artigo *New Directions in Cryptography na IEEE transactions on Information Theory* o conceito de criptografia assimétrica também denominada criptografia de chave pública. Neste método cada entidade possui duas chaves distintas, uma chave pública que pode ser divulgada a terceiros e uma chave privada que deve ser mantida em sigilo pelo proprietário do par de chaves (DIFFIE; HELLMAN, 1976 apud CIVIDANES, 2008, p. 46).

Devido ao uso de duas chaves distintas, este criptossistema tem como um dos intuitos solucionar problemas de segurança relacionado à distribuição de chaves como ocorre na criptografia simétrica.

Considerado por Stallings (2008, p. 182) "como a maior e talvez a única verdadeira revolução na história da criptografia", a criptografia de chave pública pode ser utilizada para assegurar a confidencialidade, autenticação ou ambos. As duas chaves relacionam-se entre si, no sentido que um texto codificado com a chave pública, só poderá ser decodificado com a chave privada correspondente ao par de chaves e vice-versa.

É praticamente inviável deduzir uma chave conhecendo a outra chave do seu par de chaves. A relação entre o par de chaves é baseado em funções matemáticas e torna-se computacionalmente impraticável derivar uma chave pelo conhecimento da outra, dessa forma mesmo que uma chave se torne pública o nível do segurança do criptossistema não será afetado (BRAGA, 2008, p. 45).

Também apresentado por Stallings (2008), o esquema de criptografia de chave pública é classificado em cinco parâmetros:

I. **Texto claro:** Mensagem original que constará no algoritmo de criptografia como entrada.
II. **Algoritmo de criptografia:** Responsável por realizar várias alterações na mensagem original.
III. **Chave pública e chave privada:** Par de chaves selecionado, de tal maneira que quando uma é utilizada no processo de criptografia, consequentemente a outra será

utilizada para a descriptografia. A mensagem só retornará ao seu formato original se a chave utilizada na descriptografia pertencer ao par de chaves selecionado.

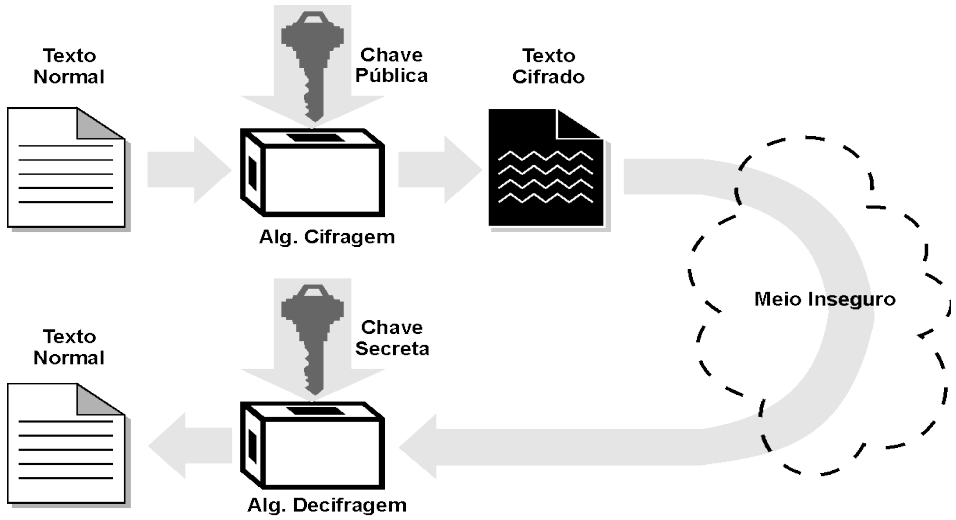
IV. **Texto cifrado:** Mensagem codificada produzida como saída, a decodificação depende diretamente do par de chaves e algoritmo de criptografia utilizado no processo.

V. **Algoritmo de descriptografia:** Produz a mensagem original, de acordo com o texto criptografado e a chave correspondente.

Cada entidade é responsável por disponibilizar a chave pública em um diretório ou repositório, com intuito de facilitar sua localização pelas entidades que desejar manter uma comunicação sigilosa. A chave privada por sua vez é pessoal e intransferível e pode ser armazenada em um arquivo no computador, denominado *smart card* ou *token* (CIVIDANES, 2008, p. 47).

Para garantir a confidencialidade, a entidade A criptografa a mensagem utilizando a chave pública de B, quando a entidade B recebe a mensagem descriptografa utilizando sua chave privada. Dessa forma, somente a entidade B será capaz de descriptografar a mensagem enviada por A (STALLINGS, 2008, p. 183). A figura 3 ilustra o processo citado.

Figura 3: Modelo de criptografia assimétrica.



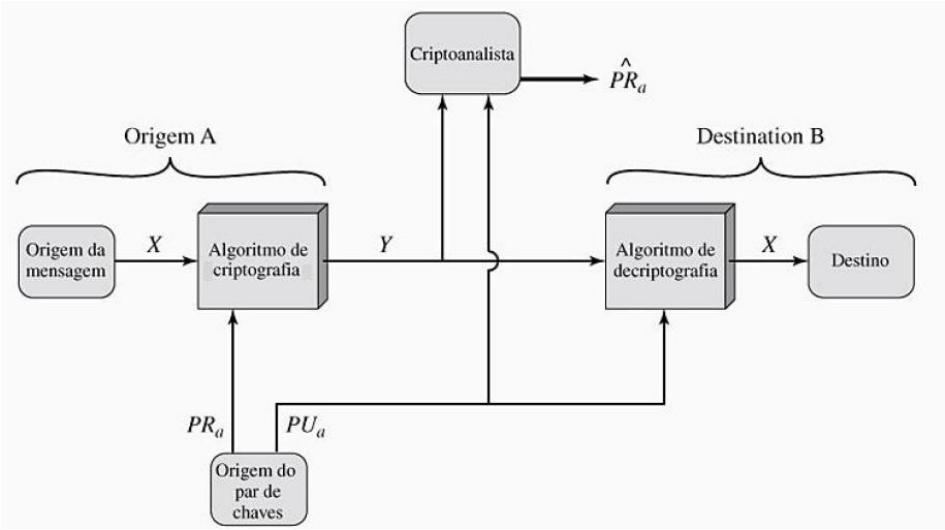
Fonte: Trinta; Macedo (1998).

Para garantir a autenticação, a entidade A envia uma mensagem para a entidade B criptografando com a chave privada de A, ao recebê-la a entidade B apenas conseguirá decifra-la utilizando a chave pública de A, dessa forma fica claro que apenas A poderia ter encaminhado a mensagem, pois é a única entidade que tem a informação desta chave privada.

O processo realizado desta forma é a base da “assinatura digital” (STALLINGS, 2008, p. 186). A figura 4 ilustra este processo.

Para facilitar a compreensão da figura 4, o termo *PRa* refere-se a chave privada da entidade A que faz o processo de criptografia e emissão da mensagem e o termo *PUa* faz referência a chave pública de A que é utilizada no processo de descriptografia pela entidade B para ter acesso ao texto claro.

Figura 4: Criptografia de chave pública: autenticação.



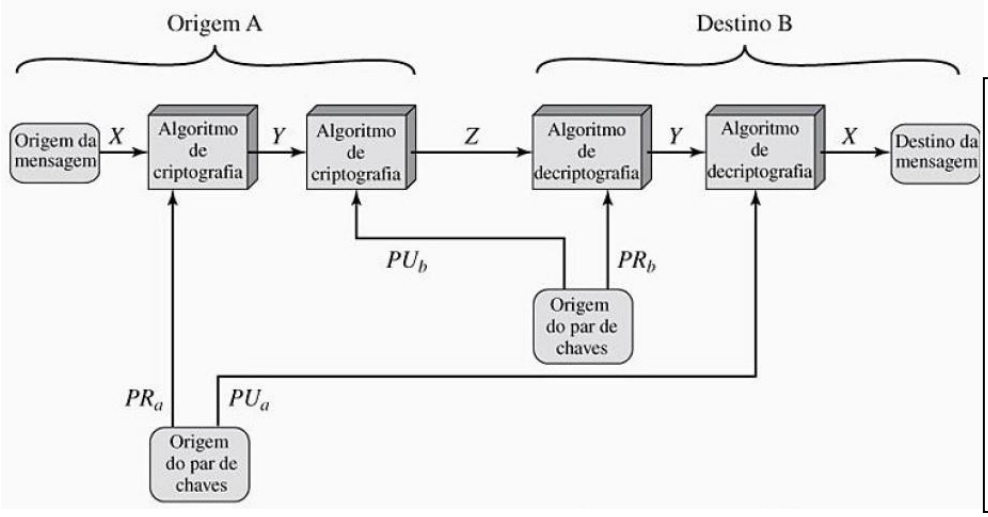
Legenda:
PRa = Chave Privada de A (Criptografia).
PUa = Chave Pública de A (Descriptografia).

Fonte: Stallings (2008).

É relatado também por Stallings (2008, p. 186) que é possível disponibilizar a função de confidencialidade e autenticação, utilizando um duplo esquema de criptografia de chave pública acrescentando mais segurança aos dados.

Neste processo, primeiramente é criptografada a mensagem utilizando a chave privada do emissor (*PRa*), este é o processo base para a assinatura digital. Logo após, a partir do resultado da primeira criptografia, é realizado novamente o processo de criptografia utilizando a chave pública do receptor (*PUb*). Este é o final da criptografia, a partir deste ponto é iniciado a descriptografia que só poderá ser realizado pelo receptor a quem foi destinado, pois é o único que possui a chave privada equivalente ao segundo processo de criptografia realizado (*PRb*) e para finalizar é realizado novamente a descriptografia referente a primeira criptografia, ou seja, o processo de descriptografia da chave pública do emissor (*PUa*), enfim tem-se a mensagem original. A figura 5 exemplifica o processo:

Figura 5: Criptografia de chave pública: confidencialidade e autenticação.



Legenda:
PRa = Chave Privada de A (Criptografia).
PUb = Chave Pública de B (Criptografia).
PRb = Chave Privada de B (Descriptografia).
PUa = Chave Pública de A (Descriptografia).

Fonte: Stallings (2008).

Um aspecto de alguns algoritmos é que qualquer uma das chaves de um par pode ser usada tanto para a criptografia quanto para a descriptografia dos dados, um exemplo é o algoritmo de RSA.

2.2.1. RSA

Considerado por estudiosos como o algoritmo de chave pública mais utilizado, o RSA (Rivest-Shamir-Adleman) foi o primeiro algoritmo assimétrico desenvolvido, criado por Ron Rivest, Adi Shamir e Leonard Adleman o algoritmo é baseado na complexidade de encontrar os fatores primos de um número composto muito grande.

Existem quatro formas possíveis de ataques ao algoritmo RSA, segundo descreve Stallings (2008):

Força bruta: Envolve tentar todas as chaves privadas possíveis, para maior segurança o tamanho da chave deve ser grande. Porém quanto maior o tamanho da chave, mais lento será o sistema devido a complexidade dos cálculos na geração das chaves e nos processos de criptografia e descriptografia.

Ataques matemáticos: Há várias técnicas com o mesmo intuito de fatorar o produto de dois números primos.

Os números primos exercem uma importante função na teoria dos números e na criptografia. Podendo ser definido como um número inteiro que possui apenas dois divisores distintos, sem resto, sendo eles valores positivos e negativos de si mesmo e 1.

Ataque de temporização (timing attack): Baseia-se no tempo gasto na execução de um algoritmo de decriptografia.

Ataques de texto cifrado escolhido: Explora as propriedades do algoritmo RSA.

2.2.2. Funções *Hash*

Uma possível desvantagem da criptografia de chave pública em relação a criptografia simétrica é a lentidão nos processos de cifragem e decifragem devido a complexidade das operações matemáticas presente neste método.

Neste cenário, é possível utilizar o recurso de codificação de um representante dos dados, um resumo da mensagem denominado *hash*.

De acordo com Monteiro; Mignoni (2007), a função *hash* é:

> "...uma função que recebe como entrada uma mensagem de qualquer tamanho e produz um resumo de tamanho fixo, que representa o conteúdo da mensagem. O propósito de uma função *hash* é produzir uma "impressão digital" da mensagem" (p. 24).

Funções *hash* são unidirecionais, ou seja, funções de caminho único. A partir do *hash* gerado de uma mensagem, é computacionalmente inviável retornar à mensagem original a partir do respectivo *hash* (CIVIDANES, 2008, p. 54).

Tornam-se importantes para assegurar a integridade da mensagem, considerando que quando o emissor deseja enviar uma mensagem o *hash* correspondente é gerado e transmitido, o receptor irá calcular outro *hash* de acordo com os dados recebidos e conferir com o hash enviado. Se forem idênticos, está comprovado que não houve alteração na mensagem enviada. Qualquer alteração na mensagem original produz um resumo *hash* diferente e não compatível com o primeiro gerado anteriormente (MONTEIRO; MIGNONI, 2007, p. 25).

De acordo com Monteiro; Mignoni (2007), os algoritmos de funções *hash* mais utilizados são o MD-5 (Message Digest-5) criado por Ron Rivest e FIPS PUB 180 que tornou-se padrão em 1993, já em 1995 uma nova versão deste padrão ficou conhecida como SHA-1, em 2002 foram apresentadas as versões SHA-256, SHA-384 e SHA-512 também denominados SHA-2 que apresentam maior complexidade.

Os algoritmos de *hash*, com suas características, podem ser combinados ao esquema de criptografia de chave pública, dando origem assim a Assinatura Digital.

2.2.3. Assinatura Digital

Um serviço disponibilizado pela criptografia de chave pública é a assinatura digital. Este processo pode ser considerado análogo à assinatura de próprio punho, uma vez que apenas uma entidade é capaz de assinar um documento e em seguida outras entidades são capazes de verificar se aquela assinatura é verídica. Dessa forma é possível verificar a autenticidade de uma mensagem criada por uma determinada entidade (CIVIDANES, 2008, p. 52).

Para a geração de uma assinatura digital, deve ser utilizada a chave privada do emissor, criptografando um valor de resumo (*hash*) ou a mensagem completa e o resultado deste processo é transmitido ao destinatário. Ao criptografar a mensagem completa com a chave privada do emissor (assinatura digital) será assegurado a autenticidade dos dados. Porém a principal desvantagem na codificação da mensagem completa é que os processos de criptografia assimétrica são lentos e trará impactos ao desempenho de todo o processo (BRAGA, 2008, p. 52).

É possível conceituar a assinatura digital como um processo da chave privada sobre um resumo da mensagem, obtendo como resultado a assinatura. O emissor é o único que tem a informação de sua chave privada (como o próprio conceito de chave privada define, a mesma é pessoal e intransferível, devendo ser mantido em sigilo), sendo portanto o único capaz de assinar a mensagem. As outras entidades por sua vez, estarão habilitadas a analisar a veracidade da assinatura digital, através da chave pública do emissor que deve ser de conhecimento de todos (CIVIDANES, 2008, p. 53).

De acordo com Silva (2004 apud BRAGA, 2008, p. 51), a assinatura digital atende aos cinco critérios da assinatura convencional, sendo eles:

- Não poderá ser falsificada; considerando que apenas o emissor tem acesso a sua chave privada;
- É autentica; ao receber a mensagem o destinatário compara o conteúdo da mensagem original com a mensagem cifrada, com intuito de garantir que não houve alterações;
- Não é reutilizável; é gerada com base em um resumo da mensagem original e não pode ser transferido a outro documento;
- É inalterável; caso haja alterações na mensagem original, produzirá um resumo diferente e sem ligações com o primeiro resumo gerado;
- Garante o não repúdio; quando um documento é assinado pelo emissor o mesmo não poderá negar que a gerou.

Conforme evidenciado acima, é importante destacar que cada trecho da mensagem original produz uma assinatura digital distinta, concluindo que cada assinatura é única para o resumo de mensagem (*hash*) e chave privada utilizada no processo (BRAGA, 2008, p. 52). É possível destacar também que em uma assinatura digital através da emissão de um carimbo de tempo pode ser identificado além do autor, a data e hora da assinatura (STALLINGS, 2008, p. 273).

O DSA (*Digital Signature Algarithm*) é o algoritmo proposto pelo NIST e designado exclusivamente às assinaturas digitais, o mesmo utiliza o padrão DSS (*Digital Signature Standard*), porém no mercado o mais utilizado é o RSA (STALLINGS, 2008, p. 272).

De acordo com dados coletados entre outubro/2013 e abril/2014, através de uma pesquisa detalhada em sites bancários que analisou os aspectos mais relevantes dos certificados digitais das principais instituições bancárias, a tabela 1 comprova de uma forma esquemática a utilização do RSA como algoritmo de assinatura das principais instituições bancárias presentes no Brasil.

Tabela 1: Certificados digitais das principais instituições bancárias do Brasil.

	Versão	**Algoritmo de assinatura**	**Algoritmo de hash de assinatura**	**Chave pública**	**Algoritmo de identificação**	**Conexão criptografada utiliza**
Itaú	V3	sha1RSA	sha1	RSA (2048 Bits)	sha1	AES_128_CBC
Bradesco	V3	sha1RSA	sha1	RSA (2048 Bits)	sha1	RC4_128
Banco do Brasil	V3	sha1RSA	sha1	RSA (2048 Bits)	sha1	RC4_128
Santander	V3	sha1RSA	sha1	RSA (2048 Bits)	sha1	RC4_128
CEF	V3	sha256RSA	sha256	RSA (2048 Bits)	sha1	AES_128_CBC
HSBC	V3	sha1RSA	sha1	RSA (2048 Bits)	sha1	RC4_128
Banco Votorantim	V3	sha1RSA	sha1	RSA (2048 Bits)	sha1	AES_256_CBC

Fonte: Autoria própria.

2.2.4. Geração e Verificação de Assinaturas Digitais

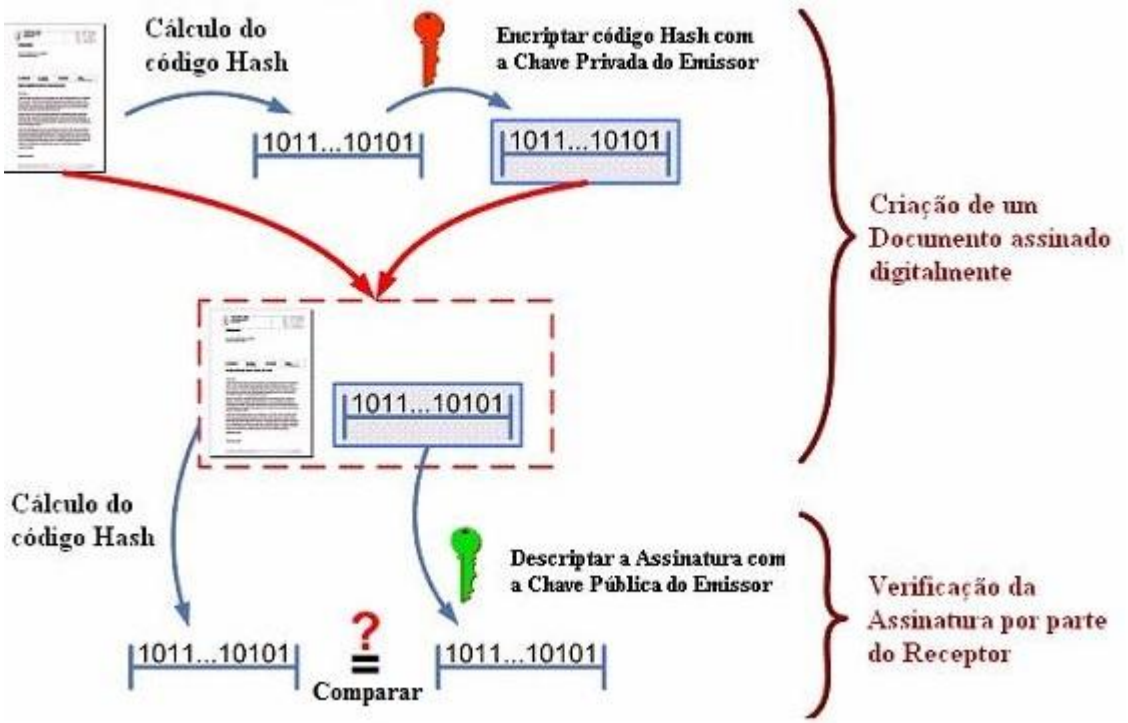
A associação da criptografia de chave pública e funções *hash* tornam eficaz o processo de assinatura digital e aplicável em documentos eletrônicos. O processo de assinatura digital pode ser detalhado e dividido em duas partes, sendo elas:

1. O emissor executa a função *hash* sobre a mensagem original, a fim de adquirir o resumo criptográfico de tamanho fixo;
2. Com o resultado do processo acima o emissor realiza o processo de criptografia utilizado sua chave privada, dando origem à assinatura digital.

Ao receber a mensagem criptografada, o destinatário realiza o processo de verificação da assinatura digital, também definido em duas partes (CIVIDANES, 2008, p. 57):

1. O destinatário executa a mesma função *hash* sobre a mensagem recebida, a fim de obter o resumo criptográfico de tamanho fixo;
2. Através da chave pública do emissor o destinatário fará a descriptografia da assinatura digital e adquire o resumo criptográfico gerado pelo emissor da mensagem, este resumo será comparado ao resumo elaborado no passo acima, sendo idênticos, a assinatura foi verificada com sucesso. A figura 6 ilustra o processo citado acima:

Figura 6: Assinatura Digital.



Fonte: Adaptado de (ASSINATURA DIGITAL, 2014).

3. CERTIFICAÇÃO DIGITAL

Os meios eletrônicos através da internet são amplamente utilizados para a transmissão de dados entre governos, empresas e cidadãos. No entanto, é necessário mecanismos de segurança que garantam integridade, autenticidade e confidencialidade às transações eletrônicas (MESQUITA, 2010, p. 18).

Nesse contexto surge o certificado digital para promover a identificação individual através de meios eletrônicos, análogo a uma "identidade digital". Seu intuito é assegurar a autenticidade e integridade dos dados; o mesmo é auxiliado pela criptografia de chave pública, pois obtém a chave publica da entidade identificada no certificado e a chave privada é guardada secretamente pelo "titular do certificado" (MONTEIRO; MIGNONI, 2007, p. 32).

O processo de Certificação Digital é definido como um conjunto de técnicas e processos que fornecem mais segurança às comunicações e transações eletrônicas e permite a guarda segura dos documentos. Através dela, é possível certificar-se de quem foi o autor de uma transação ou mensagem e também preservar dados confidenciais protegendo-os contra a leitura e alteração por pessoas não autorizadas (ITI, 2003, p. 07)[2].

Alguns dos principais usos da Certificação Digital são:

- Implementar Fluxo de Documentos em meio digital de maneira rápida e simples;
- Automatizar o recolhimento e apuração de impostos e contribuições;
- Diminuir o volume de contribuintes presentes às repartições públicas;
- Diminuir o tempo de trâmite de processos;
- Implementar recursos sofisticados de segurança, auditoria e combate à fraude e sonegação;
- Reduzir os custos de escrituração e armazenamento de livros fiscais obrigatórios;
- Contribuir na Inclusão Digital.

O certificado digital é caracterizado por ter um ciclo de vida, com início na solicitação e término com a data de expiração ou revogação, também obedece a uma hierarquia, pois é emitido e assinado por uma Autoridade Certificadora com posição imediatamente superior (BRAGA, 2008, p. 53).

---

[2] ITI–Instituto Nacional de Tecnologia da Informação. Brasília, DF. Certificação Digital: Entenda e Utilize. Disponível em: <http://www.iti.gov.br/publicacoes/cartilhas/3893-certificacao-digital-entenda-e-utilize>. Acesso em: 29 Ago. 2013.

3.1 Infra-Estrutura de Chaves Públicas

Segundo Stallings (2008, p. 309) a infra-estrutura de chave pública (ICP), do inglês, *public key infrastructure (PKI)* pode ser definida como "conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais com base na criptografia de chave pública".

Silva (2004) apud Braga (2008, p. 54) relata que a infra-estrutura de chave pública é uma arquitetura de confiabilidade que as empresas podem determinar para suas redes corporativas e políticas de segurança. Por ela é possível realizar transações via internet com a mesma segurança de negócios presenciais entre pessoas.

Para que uma ICP seja considerada como um órgão de confiabilidade além de obter uma tecnologia adequada, também deve dispor de uma estrutura hierárquica aprovada pela legislação regulamentadora especifica e legitimada pelo Governo Federal. Existem ICPs reconhecidas no mercado (Exemplo: Verisign), que tiveram sua confiabilidade reconhecida em virtude de suas boas práticas, comprovada através de auditorias independentes (MESQUITA, 2010, p. 24).

Certificado digital também pode ser entendido como um conjunto de dados à prova de possíveis falsificações que declara a associação de um par de chaves criptográficas a uma entidade distinta. Os certificados são emitidos por terceiros confiáveis denominados Autoridades Certificadoras (AC), que é uma entidade considerada confiável pelas partes envolvidas. Uma AC é análoga a um cartório de títulos, a diferença é que todos os processos são digitais (ITI, 2003, p. 07).

A tabela 2 relaciona recursos de segurança do mundo real e seus respectivos correspondentes proporcionados pela infra-estrutura de chaves públicas:

Tabela 2: Mecanismos de segurança do mundo real e equivalentes na ICP.

Mundo Real	Equivalente na ICP
Envelopes e firmas de envio seguro	Criptografia de dados
Assinaturas físicas e selos de autenticação	Assinaturas digitais
Documentos de identificação Ex: CPF, CNPJ	Equivalentes emitidos digitalmente Ex: e-CPF, e-CNPJ
Fé pública por meio de tabelionatos	Fé pública por meio de Autoridades Certificadoras
Prova testemunhal em documentos	Não repúdio de assinaturas digitais
Operações financeiras presenciais	Operações financeiras on-line com identificação do usuário através de sua chave privada

Fonte: Adaptado de (SILVA 2004 apud MESQUITA, 2010, p. 24).

3.1.1. Autoridade Certificadora

Considerada como entidades confiáveis, as autoridades certificadoras (AC) são responsáveis por receber requerimentos de certificados, fazer a autenticação, gerir dados de status e emitir certificados digitais para outras entidades, empresas, órgãos governamentais a fim de garantir a autenticidade e integridade dos dados transmitidos pelo requerente do certificado. As AC's atuam como uma "terceira parte confiável", gerencia o processo de certificação digital e todo seu ciclo de vida (CIVIDANES, 2008, p. 65).

Suas principais responsabilidades são:

- Emitir certificados de acordo com a relação de compatibilidade de um usuário a uma chave pública, através da assinatura digital;
- Programar data de expiração para certificados;
- Atestar a revogação de certificados, através da publicação das Listas de Certificados Revogados (LCR).

As responsabilidades, regras e encargos legais de uma AC e de usuários de certificados, são expressas em um termo denominado DPC (Declaração de Práticas de Certificação). Neste documento está claro métodos de trabalho, grau de confiabilidade dos certificados e das AC's pertencentes ao processo de certificação. De acordo com Monteiro e Mignoni (2007, p. 35), as AC's estão divididas em três classes, sendo elas:

- Interna: Processo realizado por uma instituição, para a emissão de certificados digitais internos;
- Terceirizada: Processo realizado por uma entidade contratada por uma instituição ou empresa para a emissão de certificados internos e para clientes;
- Autônoma: Entidade governamental e privada, que comercializa serviços de certificação aos usuários finais.

3.1.2. Autoridades de Registro

As entidades responsáveis pela autenticação das informações fornecidas pelo usuário final são denominadas autoridades de registro (AR), esta atua como um órgão de apoio a uma AC (autoridade certificadora) e tem como objetivo descentralizar algumas funções da AC aumentando o desempenho na autenticação dos dados do usuário final, pois a mesma pode solicitar a presença do requisitante do certificado digital para a verificação de documentos apresentados (MONTEIRO; MIGNONI, 2007, p. 35).

Após a autenticação do usuário final, a AR está apta a enviar para a AC a solicitação de certificado, para que esta gere, assine digitalmente e emita o certificado de acordo com as informações analisadas pela AR. A qualidade presente no processo de autenticação define o grau de confiança que será atribuído ao certificado. De acordo com Cividanes (2008, p. 68), algumas funções realizadas por uma AR estão descritas a seguir:

- Estabelecer e confirmar a identidade de um usuário final ou entidade;
- Iniciar o processo de certificação com uma AC em nome de usuários finais, através da requisição para emissão de certificados;
- Obter das AC's certificados digitais assinados e armazená-los em um repositório local, para logo após distribuir aos usuários finais;
- Gerenciar as chaves e ciclo de vida do certificado.

É válido observar que a emissão propriamente dita de certificados é uma função exclusiva das Autoridades Certificados, não sendo possível realizá-la por uma Autoridade de Registro.

3.2. Padrão X.509

É exigido um formato padronizado para que qualquer aplicação seja capaz de ler ou escrever certificados, independente de qual autoridade certificadora os emitiu. Um certificado pode conter outros dados além da chave pública e a identidade do assinante.

Com o ideal de atender a exigência de padronização foi desenvolvido pela *International Telecommunication Union, Telecommunication Standartization Sector* (ITU-T)[3] o formato X.509, inicialmente emitido em 1988. A primeira versão (V1) foi revisada para resolver alguns problemas de segurança e uma recomendação revisada foi emitida em 1993 para incorporar dois novos campos utilizados em controle de acesso, resultando na versão dois (V2). Logo após fez-se necessário mais um recurso e em 1996 foi lançada a terceira versão (V3) possibilitando a utilização de campos de extensão (STALLINGS, 2008, p. 302).

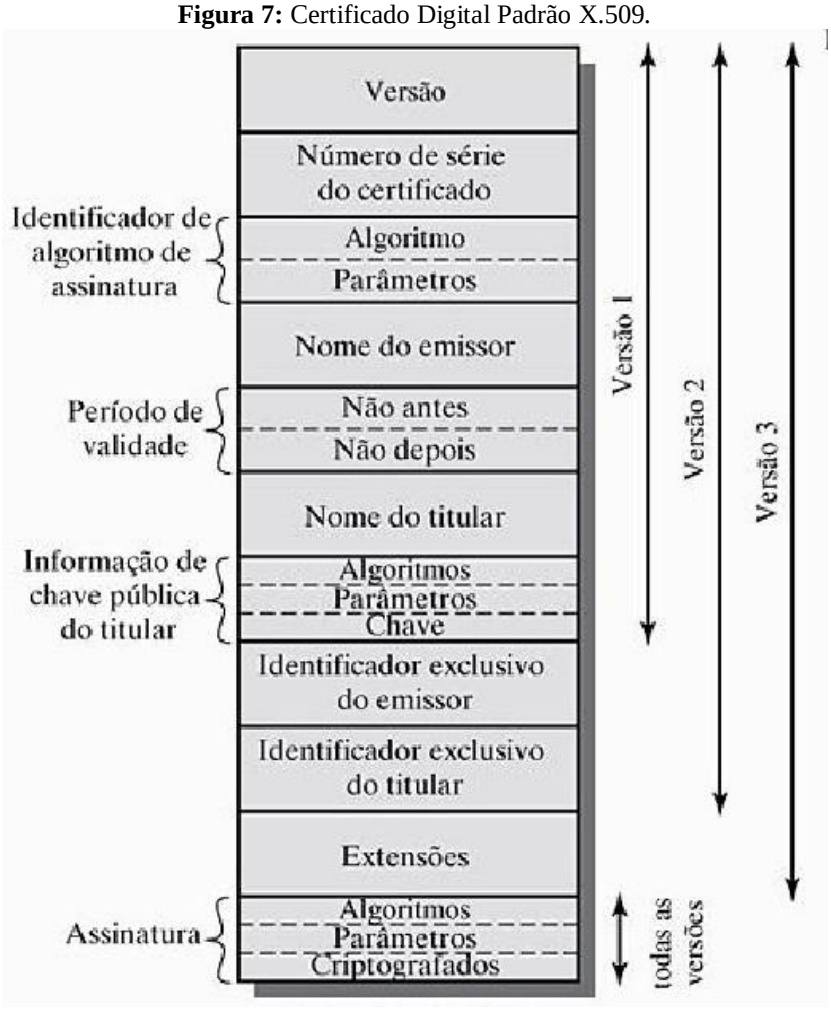
As extensões incluídas no formato X.509 (V3) disponibiliza uma forma de associar dados adicionais a uma entidade, chave pública autoridade certificadora ou outros dados pertencentes ao certificado.

---

[3] ITU-T (*International Telecommunication Union, Telecommunication Standartization Sector)* é o Setor de Normatização das Telecomunicações, uma área da União Internacional de Telecomunicações responsável por coordenar padronizações relacionadas a telecomunicações. Atualmente o ITU-T é uma agência intergovernamental que congrega mais de 700 organizações públicas e privadas de 191 países.

De acordo com Stallings (2008, p. 302) o padrão X.509 é baseado no uso da criptografia de chave pública e assinaturas digitais. Nele é recomendado o uso do algoritmo RSA e no esquema de assinatura digital é exigido que uma função *hash* seja utilizada. Na figura 7 é apresentado a evolução dos campos de um certificado no padrão X.509:

Figura 7: Certificado Digital Padrão X.509.



Fonte: Stallings (2008).

Na tabela 3 estão descritos detalhadamente os principais campos de um certificado no padrão X.509:

Tabela 3: Descrição de campos de um certificado padrão X.509.

Nome do Campo	Descrição
Versão	Número da versão X.509 do certificado, tendo como válido apenas 1, 2 e 3.
Número de Série	Identificador único do certificado e representado por um número inteiro. Não deve haver mais de um certificado emitido com o mesmo número de série por uma mesma autoridade certificadora.
Algoritmo de Assinatura	Identificador do algoritmo usado para assinatura do certificado pela autoridade certificadora.
Emissor	Nome da autoridade certificadora que produziu o assinou o certificado.
Período de Validade	Intervalo de tempo de duração que determina quando um certificado deve ser considerado válido pelas aplicações.
Assunto	Identifica o dono da chave pública do certificado. O assunto deve ser único para cada assunto no certificado emitido por uma autoridade certificadora.
Chave Pública	Contém o valor da chave pública do certificado junto com informações de algoritmos com o qual a chave deve ser usada.
Identificador único de Emissor (opcional)	Campo opcional para permitir o reuso de um emissor com o tempo.
Identificador único de Assunto (opcional)	Campo opcional para permitir o reuso de um assunto com o tempo.
Extensões (opcional)	Campos complementares com informações adicionais personalizadas.

Fonte: Adaptado de Stallings, p. 303

O campo de extensão consiste em três partes distintas, são elas (SOUSA, 2010, p. 42):

- Tipo de Extensão: Objeto identificador que provê semântica e tipo de informação (texto, data, numero inteiro ou estrutura complexa) para o valor da extensão;
- Valor de Extensão: Valor real de um campo de extensão que é descrito pelo seu tipo;
- Indicador Crítico: Instrui aplicações de softwares que utilizam certificados que desconsidera o valor do campo quando o tipo de extensão é conhecido, indica se uma extensão pode ser ignorada com segurança.

3.3. Ciclo de Vida do Certificado

Um certificado digital no formato X.509, distintamente de outros documentos utilizados para identificação pessoal como CPF e RG, possui um período de validade. As aplicações apenas aceitarão o certificado enquanto o mesmo for válido, após o vencimento do prazo de validade o certificado digital é automaticamente considerado expirado, sendo assim, quaisquer documentos assinados após a data de expiração, não possuirão validade legal. Documentos assinados durante o período de validade do certificado digital estão assegurados por tempo indeterminado.

Segundo Monteiro e Mignoni (2007, p. 106), os certificados digitais apresentam um ciclo de vida formado por sete itens que exercem todo o processo da certificação digital, desde a solicitação até a finalização das atividades de um certificado. São eles:

- **Solicitação:** Os processos para a solicitação de certificados incluem exigências quanto a geração, proteção do par de chaves e lista de informações necessárias em cada classe de certificados, o preenchimento de uma solicitação e o envio a uma determinada autoridade certificadora. As informações enviadas são mantidas em confidencialidade pela AC responsável

- **Validação:** Ao receber uma solicitação, a autoridade de registro (AR) irá efetuar as validações obrigatórias, estabelecidas como pré-requisitos para a emissão do certificado. Esta autoridade de registro (AR) fará a confirmação se as informações fornecidas são válidas ou não. Se todas as informações forem confirmadas, a autoridade de registro (AR) enviará a autoridade certificadora (AC) a solicitação de certificado, caso contrário, a solicitação é rejeitada;

- **Emissão:** Este processo ocorrerá após a autoridade certificadora (AC) receber uma solicitação aprovada pela autoridade de registro (AR), a emissão indica a aprovação final da solicitação pela autoridade certificadora (AC). O certificado digital é valido no momento em que o assinante o aceita.

- **Aceitação:** Os meios de aceitação diferenciam-se de acordo com a classe. Ao aceitar um certificado, o assinante tem como dever garantir a integridade da chave privada, a veracidade das informações e o certificado serão de seu uso exclusivo. Ao aceitar um

certificado o assinante concorda com os termos e condições da declaração de práticas de certificação (DPC).

- **Uso de Certificados:** A garantia de que os certificados são usados corretamente, é realizada pela conferência da assinatura digital.

- **Suspensão/Revogação de Certificados:** Poderá ocorrer por vários motivos, como: comprometimento, roubo, perda, modificações, divulgação da chave privada do assinante, violação de obrigações da declaração de práticas de certificação (DPC), ações causadas por desastres naturais, falta de pagamento de taxas e outras ações consideradas relevantes por uma autoridade certificadora (AC).

- **Vencimento:** A autoridade certificadora (AC) deverá emitir notificações aos assinantes através de correio eletrônico, deixando-o ciente do vencimento do certificado. A autoridade certificadora (AC) não se responsabiliza pela utilização de certificados vencidos.

3.4. Sigilo nas Comunicações: SSL e HTTPS

Grande parte das empresas, órgãos governamentais e muitas pessoas possuem sites *Web*, o acesso a internet por organizações e pessoas cresce de forma exponencial e cada vez mais rápido.

O autor Stallings (2008) argumenta que a *web* é cada vez mais empregada como uma vitrine com alta visibilidade de dados corporativos e produtos e tornou-se a plataforma do comércio eletrônico.

O HTTP (*HyperText Transfer Protocol* ou Protocolo de Transferência de Hipertexto) é basicamente um protocolo de transferência para a interação cliente/servidor da *web* que utiliza como protocolo implícito o TCP/IP fornecendo um serviço confiável de transferência de dados (STALLINGS, 2008, p. 379).

Diante do cenário atual a demanda por serviços de maior segurança na *web* é crescente, foi projetado então o SSL (*Secure Sockets Layer*) que é um protocolo que fornece criptografia dos dados e autenticação entre dois aplicativos de comunicação (cliente/servidor) utilizando o TCP/IP (KUROSE; ROSS, 2010).

Os dados transmitidos entre cliente/servidor são criptografados utilizando algoritmo simétrico (Exemplo: DES ou RC4), para o processo de troca de chaves criptografadas e para

as assinaturas digitais é utilizado um algoritmo de chave pública (exemplo: RSA). É utilizada pelo algoritmo a chave pública no certificado digital do servidor, com o certificado digital do mesmo é possível que o cliente verifique a identidade do servidor.

As versões 1 e 2 do protocolo SSL fornecem apenas a autenticação do servidor, já a versão 3 fornece também a autenticação do cliente, aplicando os certificados digitais do cliente e do servidor (TIVOLI SOFTWARE, 2014).

3.5. MP 2200-02

A ICP-Brasil (Infra Estrutura de Chaves Públicas do Brasil) em sua implantação teve como principal objetivo estipular os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado na infra-estrutura de chaves públicas, a complexidade no sistema é significativo, pois define a confiança no certificado (GELFI, 2007, p. 25).

De acordo com a Medida Provisória n° 2.200-2 de 24 de agosto de 2001, no art. 1°, é definido:

> "Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras" (BRASIL, 2001).

O ideal de certificação faz parte de uma política do Governo Federal, instituída em 2000 através de estudos realizados pela Casa Civil da Presidência da República para a inserção do "Governo Eletrônico" (SILVESTRE, 2003 apud GELFI, 2007, p. 25).

De acordo com o Art. 2° da MP 2.200-2/01, a Infra-Estrutura de Chaves Públicas Brasileira é formada pelas entidades a seguir:

- Autoridade gestora de políticas (Comitê gestor com características de um organismo político);
- Autoridade certificadora raiz;
- Instituto Nacional de Tecnologia da Informação - ITI (Com características de um organismo administrativo);
- Cadeia de autoridades certificadoras;
- Cadeia de autoridades de registro.

3.6. ICP-Brasil (Infra-Estrutura de Chaves Públicas Brasileira)

Elaborada a partir da Medida Provisória 2.200-2 de 24/10/2001, a ICP-Brasil é um grupo de entidades prestadoras de serviços que estão de acordo com as diretrizes e normas técnicas estabelecidas por um comitê gestor. Através de certificados emitidos por autoridades certificadoras da ICP-Brasil é concedida a validade jurídica aos documentos assinados digitalmente (ITI, 2003, p. 09).

A estrutura hierárquica da ICP-Brasil é uma de suas principais características, no topo da estrutura está a autoridade certificadora raiz e abaixo dela, diversas outras entidades. As autoridades certificadoras, autoridades de registro e os prestadores de serviços de suporte fazem parte da hierarquia (ITI, 2003, p. 09).

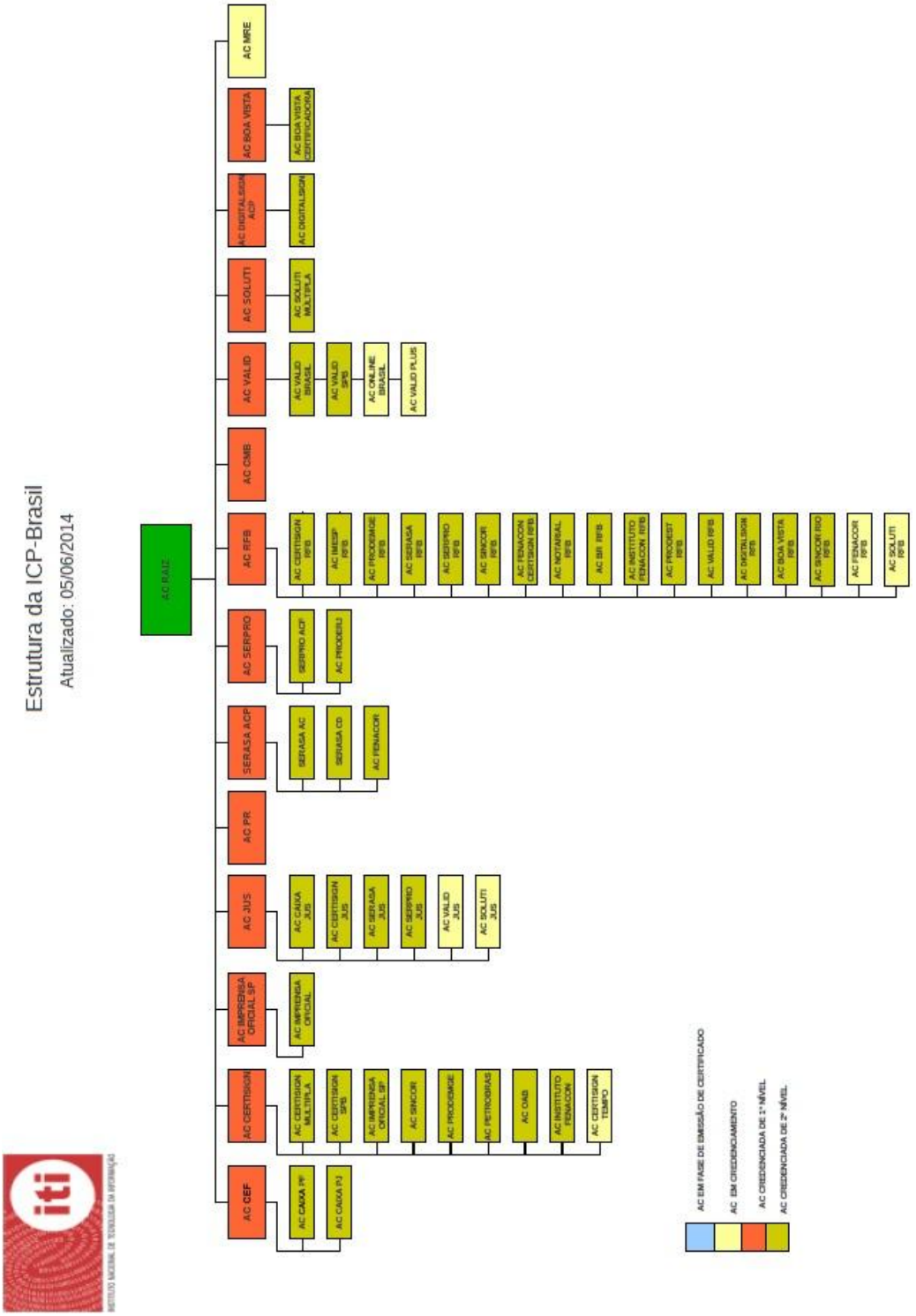
O Instituto Nacional de Tecnologia da Informação – ITI, é a autoridade certificadora raiz da ICP-Brasil, ela é responsável pela execução das políticas de certificados e normas técnicas e operacionais validado pelo comitê gestor. O certificado da AC Raiz é auto assinado e pode ser verificado através de mecanismos e processos específicos (BRAGA, 2008, p. 56).

São responsabilidades do ITI emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras (AC) de grau imediatamente inferior ao seu; a gerência da lista de certificados emitidos, revogados e vencidos; a fiscalização e auditoria das autoridades certificadoras (AC), autoridade de registro (AR) e prestadores de serviços de suporte (PSS) e a verificação se as ACs atuam de acordo com as diretrizes e normas técnicas estabelecidas pelo comitê gestor, também estão em sua responsabilidade (ITI, 2014).

Os certificados digitais seguem uma estrutura hierárquica de certificados assinados por consecutivas autoridades certificadoras. A figura 8 apresenta a estrutura resumida da ICP-Brasil.

O Comitê Gestor da ICP-Brasil é a autoridade que gerencia as políticas e responsável por consolidar a política, critérios e normas técnicas e fiscalizar a atuação da Autoridade Certificadora Raiz. Já o Comitê Técnico (COTEC) presta suporte técnico e assistência ao Comitê Gestor da ICP-Brasil.

Figura 8: Estrutura resumida da ICP-Brasil.



Fonte: ITI (2014)[4]

[4]ITI–Instituto Nacional de Tecnologia da Informação. Brasília, DF. Estrutura da ICP-Brasil. Disponível em: <http://www.iti.gov.br/images/icp-brasil/estrutura/2014/atualizacao11/Estrutura_da_ICP-Brasil_-_site.pdf>. Acesso em: 05 jun 2014.

3.6.1. Tipos de Certificados

Conforme informações da Resolução nº 53 de 28 de novembro de 2008 que altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, no momento atual os certificados digitais destinados a usuários finais da ICP-Brasil estão classificados em 10 (dez) tipos distintos, sendo 6 (seis) relacionados com assinatura digital que são utilizados na confirmação de identidade na web, e-mails, redes privadas e em documentos eletrônicos e 4 (quatro) relacionados com sigilo que são utilizados na codificação de documentos.

Os tipos de certificados de assinatura digital são: Tipo A1; Tipo A2; Tipo A3; Tipo A4; Tipo T3 e Tipo T4.

Os tipos de certificados de sigilo são: Tipo S1, Tipo S2; Tipo S3 e Tipo S4.

Certificados do tipo T3 e T4 serão emitidos apenas para equipamentos das autoridades de carimbo do tempo (ACTs) credenciadas na ICP-Brasil, estão associados aos mesmos requisitos de segurança com exceção do tamanho das chaves criptográficas utilizadas.

Uma autoridade certificadora de tempo (ACT) é definida como uma entidade onde os usuários de serviços de carimbo do tempo confiam para emitir carimbos de tempo, ela tem como responsabilidade fornecer o carimbo do tempo de acordo com os atributos concedidos pela parte confiável do tempo que adjunto a uma assinatura digital, prova sua existência em um período especifico. Na prática uma ACT assegura a questão temporal de uma transação e também seu conteúdo (ITI, 2013).

A tabela 4 ilustra de acordo com a Resolução nº 91 de 05 de julho de 2005, que aprova a versão 5.0 do documento requisitos mínimos para as políticas de certificados na ICP-Brasil, que demonstra a comparação de requisitos mínimos por tipo de certificado (CG ICP-BRASIL, 2012).

Tabela 4: Requisitos dos certificados digitais na ICP-Brasil.

Tipo de Certificado	*Chave Criptográfica*			*Validade máxima do certificado (anos)*	*Freqüência de emissão de LCR (horas)*	*Tempo limite para revogação (horas)*
	Tamanho (bits)	*Processo de Geração*	*Mídia Armazenadora*			
A1 e S1	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Software	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma do item 6.1.1	1	6	12
A2 e S2	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Software	Cartão Inteligente ou *Token*, ambos sem capacidade de geração de chave e protegidos por senha e/ou identificação biométrica	2	6	12
A3 e S3	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Hardware	Cartão Inteligente ou *Token*, ambos com capacidade de geração de chave e protegidos por senha e/ou identificação biométrica, ou *hardware* criptográfico homologado junto à ICP-Brasil	5	6	12
T3	RSA 1024 (V0 e V1), 2048 (V2) ECDSA 256	Hardware	*Hardware* criptográfico homologado junto à ICP-Brasil	5	6	12
A4 e S4	RSA 2048 (V0 e V1), 4096 (V2) ECDSA 512	Hardware	*Hardware* criptográfico homologado junto à ICP-Brasil	6	6	12
T4	RSA 2048 (V0 e V1), 4096 (V2) ECDSA 512	Hardware	*Hardware* criptográfico homologado junto à ICP-Brasil	6	6	12

Fonte: Resolução nº 91 de 05 de julho de 2012 (CG ICP-BRASIL, 2012).

3.7. Aplicações da Certificação Digital

Com a presença da certificação digital torna-se possível a utilização da internet como meio de comunicação alternativo com intuito focado na economia de recursos ou aumento de lucros e de maior facilidade para organizações de diversos segmentos como, governo federal, governo estadual, governo municipal, poder judiciário e organizações privadas (SOUSA, 2010, p. 43).

Dentre os diversos benefícios provindos da certificação digital, destacam-se a facilidade proporcionada aos usuários na realização de transações on-line, a rapidez e eficiência nos processos internos de uma organização, a economia no tráfego, conservação de

documentos e na busca manual por informações, a eliminação do uso de papel e a utilização de arquivos eletrônicos, a redução de fraudes devido a certificação digital fornecer garantias adicionais em assinaturas digitais, assegurando que documentos não serão alterados sem detecção após a aplicação da assinatura e também garante os princípios básicos da segurança da informação: autenticidade, integridade, sigilo e validade jurídica de documentos digitais.

Os tipos de aplicações da certificação digital são basicamente:

- **Assinatura Digital e Confidencialidade:** Aplicado em conteúdo eletrônico, como por exemplo, mensagens de e-mail e banco de dados.
- **Autenticação de agentes:** Aplicados para identificação remota de pessoas, processos, sistemas e dispositivos.

Algumas aplicações que utilizam certificados digitais com intuito de assegurar a privacidade e autenticidade dos dados são:

Comércio Eletrônico

As empresas virtuais com certificação digital asseguram e conquistam maior credibilidade nas transações e negócios feitos via internet, considerando que os dados em tráfego estão protegidos. Isso é essencial, especialmente no Brasil, onde existe um grande receio por parte dos consumidores em relação à segurança de compras na *web*.

As principais vantagens que são destacadas no comércio eletrônico são: a agilidade na comunicação, redução de custos em diversos setores de uma empresa convencional como, almoxarifado, marketing, vendas, gastos com a edificação e arranjos físicos, e a empresa é capaz de manter um estoque reduzido, renovado e direcionado ao público alvo.

Outra vantagem competitiva a ser considerada é que através da web a empresa estará 24 horas aberta ao público e há constatações de empresas que o maior número de compras ocorre no período de 17:00h às 07:00h, horário que convencionalmente a empresa física não estaria aberta (CAMARA-E.NET, 2014).

Conectividade Social

Considerado o canal de comunicação entre a Caixa Econômica Federal (CEF) e as empresas que fazem o recolhimento do Fundo de Garantia por Tempo de Serviço (FGTS), desde 02 de maio de 2011 a Conectividade Social é acessada com um nível maior de segurança, através da utilização da certificação digital ICP-Brasil.

Este canal é obrigatório para a transmissão do arquivo SEFIP e exige a certificação digital da empresa que realiza o procedimento (ITI, 2014)[5].

Receita Federal

A Secretaria da Receita Federal do Brasil é um dos órgãos federais que mais utilizam a certificação digital, através deste processo é proporcionada maior agilidade e comodidade ao contribuinte, garantindo também o sigilo fiscal determinado por lei, a privacidade e autenticidade das informações (RECEITA FEDERAL, 2014).

Abaixo constam algumas das principais utilizações:

- **Central Virtual de Atendimento ao Contribuinte (e-CAC):** Nesta seção constam todos os serviços da Receita Federal do Brasil e da Procuradoria da Fazenda Nacional que são possíveis ser realizados via internet, é possível consultar a situação fiscal dos contribuintes, prestação de contas, procuração eletrônica e outros serviços;

- Emissão de declaração de imposto de renda de pessoa física e pessoa jurídica;

- **Sistema Público de Escrituração Digital (SPED):** Instituído em 2007, o SPED representa um avanço tecnológico para a relação entre o fisco e os contribuintes. A escrituração fiscal das empresas é enviada ao fisco por meio de arquivos eletrônicos validados através da certificação digital.

  Este sistema é dividido em três subprojetos, sendo eles: Escrituração Contábil Digital, Escrituração Fiscal Digital e Escrituração Digital das Instituições Financeiras.

- **Nota Fiscal Eletrônica (NF-e):** Tem como principal objetivo proporcionar maior facilidade aos contribuintes e as atividades de fiscalização sobre operações e prestações tributadas pelo Imposto sobre Circulação de Mercadorias e Serviços (ICMS) e pelo Imposto sobre Produtos Industrializados (IPI). As empresas fazem a implantação do documento fiscal eletrônico e dessa forma substitui a emissão do documento fiscal em papel.

---

[5] ITI–Instituto Nacional de Tecnologia da Informação. Brasília, DF. Certificação Digital: Benefícios. Disponível em: <http://www.iti.gov.br/certificacao-digital/beneficios>. Acesso em: 09 mai 2014.

Internet Banking e Mobile Banking

O processo de certificação digital possibilita um elevado nível de segurança de dados para a realização das transações eletrônicas realizadas entre as instituições bancárias e clientes. Senhas alfanuméricas tornam-se frágeis para um nível maior de segurança exigida para determinadas transações, pois são passíveis de interceptação e em um ataque de força bruta é possível deduzi-la. Para autenticar um processo de transação, a instituição bancária utiliza a chave pública do cliente para garantir autenticidade da mensagem previamente assinada pelo cliente com sua chave privada.

Este nível de segurança é alcançado, pois a criptografia de chave pública permite estabelecer autenticação, sigilo e não repúdio garantindo que não houve alterações no conteúdo da mensagem entre o período da emissão e recebimento, também identifica de forma evidente o emissor das transações. Um dos benefícios deste processo é a agilidade alcançada nas transações bancárias.

4. INTEGRAÇÃO E SEGURANÇA DO *INTERNET BANKING*

Utiliza-se o termo *internet banking* para definir transações bancárias por meio da internet realizadas por uma página segura do banco. Com o início do *internet banking* as principais operações financeiras, pagamentos, transferências, consultas a extratos e outras operações passam a ser eletrônicas e realizadas de uma maneira mais eficaz e eficiente.

A comodidade, disponibilidade dos serviços bancários 24 horas por dia, possibilidade de mobilidade, proposta de acabar com filas e de não ser necessário a intervenção de um colaborador de agência bancária para que clientes sejam capazes de ter acesso aos dados e operações que necessitam são vantagens destacáveis para a adoção desta tecnologia.

A evolução do *internet banking* ocorreu de forma rápida e tornou-se destaque nos últimos anos. O número de transações realizadas através da internet já supera as transações feitas de forma tradicional e comprova a popularidade e facilidade oferecida pelo serviço. O Brasil é um dos pioneiros a aderir ao *internet banking* (DAMIANO, 2013, p. 33).

A segurança tornou-se um grande desafio a ser enfrentado pelas instituições bancárias que utilizam o *internet banking*, pois este canal expõe as informações a riscos de segurança e tornou-se alvo de fraudes. Neste cenário, torna-se essencial a existência de uma gestão de segurança integrada, proativa, com respostas rápidas, que reflita rapidamente as mudanças organizacionais, tecnológicas, operacionais e eficientes contra ameaças e vulnerabilidades (DAMIANO, 2013, p. 34).

De acordo com o Febraban (2013), com intuito de solucionar os problemas de segurança que se agravam de acordo com as mudanças e evoluções tecnológicas, em 2012 houve um investimento de R$ 20,1 bilhões em tecnologia da informação, este número demonstra que as instituições bancárias buscam na tecnologia da informação um importante aliado para alcançar a segurança, desenvolvimento de inovações e estratégias de crescimento idealizado.

As principais características da ISO/IEC 27002:2013[6], que apresenta as melhores práticas e recomendações para a gestão da segurança da informação, são: integridade, os dados não podem ser corrompidos durante a manipulação ou transmissão; confidencialidade, os dados não podem ser acessados por pessoas não autorizadas; disponibilidade, a comunicação entre computadores deve estar disponível sempre que solicitado; privacidade, os dados apenas podem ser acessados a quem foi destinado; autenticidade, mecanismos de confirmação do emissor dos dados.

4.1. O Papel da Tecnologia da Informação no Setor Bancário

Com o processo de globalização da economia, as fronteiras mundiais se tornam mínimas e até inexistentes de acordo com o processo em questão, essa nova realidade mundial é possível com o avanço da tecnologia da informação que tem sua importância cada vez mais destacada em todos os setores econômicos.

O setor bancário é considerado um dos que mais investem em tecnologia da informação, o Brasil é um dos líderes neste processo evolutivo e com a implantação de novos sistemas bancários agrega-se maior facilidade e comodidade aos clientes. Com a automação bancária uma das ideias principais é que o dinheiro apresenta forte tendência em se transformar exclusivamente em informação o que valoriza de maneira mais acentuada a presença da tecnologia da informação no dia a dia dos processos (DAMIANO, 2013, p. 29).

Os principais benefícios que conduziram os bancos na aderência da internet são: redução de custo operacional e processual; vantagem competitiva e migração de serviços da rede física para a rede virtual.

Porém, em contrapartida a todos os benefícios o fator crítico de alta relevância a ser considerado é a segurança dos dados envolvidos nos processos, pois trata-se de operações com valores agregados e com isso torna-se alvo frequente de fraudes. Esse cenário faz da tecnologia da informação essencial para a manutenção dos benefícios alcançados e para a adequação de uma gestão de segurança da informação, onde a criação e renovação de políticas nas transações bancárias e orientação aos usuários finais são pontos chave para o sucesso ou fracasso do *Internet Banking*.

4.2. Sistemas de *Internet Banking*

Um sistema de *internet banking* pode ser entendido como uma proposta de atendimento personalizado e concessão de serviços bancários como uma ferramenta tecnológica com objetivo principal de disponibilizar maior conveniência e acrescentar valor no relacionamento entre instituição bancária/cliente a fim de auxiliar na concretização de negócios e fidelizar clientes devido aos inúmeros benefícios e facilidades proporcionados neste modelo de atendimento.

---

[6] Norma ABNT NBR ISO/IEC 27002:2013: Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização. Disponível em: < http://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 14 mai 2014.

Representa também uma modalidade de comércio eletrônico, pois através dos serviços bancários disponibilizados via web a realização de negócios, contratos eletrônicos e compras *on-line* pode ser realizada de forma simplificada e com maior comodidade (MATTAR, 2007, p. 25).

Ao contrário do *home banking* (que antecede a chegada do *internet banking*) onde era necessária uma prévia instalação dos sistemas bancários nos computadores de clientes e constantes atualizações de *software*, o *internet banking* está em um cenário de solução aberta, os *softwares* utilizados são de conhecimento público e as instituições bancárias não precisam disponibilizar um treinamento prévio aos usuários, as atualizações por sua vez são feitas diretamente no servidor do banco e de imediato acesso através da *web*, não sendo necessárias atualizações unitárias em computadores de clientes (MATTAR, 2007, p. 24).

Outros benefícios na utilização no *Internet Banking* destacados são:

- Diminuição de custos de manutenção de uma agência bancária e despesa com colaboradores;
- Facilidades oferecidas aos clientes, onde a presença física em uma agencia bancária não é necessário, com isso é possível otimizar o tempo e evitar filas para atendimento;
- Alcance geográfico, devido a internet ter abrangência mundial e disponibilidade 24 horas por dia;
- Diminuição de riscos de assaltos, pois há um menor movimento de pessoas, moedas e serviços nas agências bancárias (MATTAR, 2007, p. 27).

4.2.1 A realidade do *internet banking* brasileiro

Transações bancárias realizadas através do *internet banking* em 2013 ultrapassaram pelo segundo ano consecutivo as transações efetuadas por meios tradicionais. De acordo com a Pesquisa FEBRABAN de Tecnologia Bancária 2013 em parceria com a *Booz & Company*, a *internet banking* é responsável por 39% do total de transações realizadas, o crescimento médio de transações realizadas através do *internet banking* aproxima-se de 25% ao ano. Já as agências bancárias apresenta o menor crescimento do número de transações chegando a 3% ao ano, perdendo participação de 18% para 11% no volume total de transações desde 2008. A expectativa é que até 2017 as transações via internet correspondam a cerca de 60% das operações bancárias do Brasil.

A facilidade e comodidade proporcionada pelo uso dos meios digitais auxiliaram a alavancar a abertura de contas correntes que aumentou 6% em relação a 2012 e abertura de poupança que teve um aumento de 4%.

A Pesquisa FEBRABAN de Tecnologia Bancaria 2013 ainda relata que o uso do *internet banking* cresce mais que o número de usuário de internet, este fato evidencia que maior parcela de usuários se beneficia das facilidades do *internet banking*. Com este cenário conclui-se que há necessidade de maiores investimentos com objetivo de maximizar a utilização deste canal de atendimento.

Os números também indicam a necessidade cada vez mais ascendente de desenvolvimento de novas soluções de segurança da informação de acordo com a realidade atual de aumento na quantidade de usuários e serviços, falhas de aplicações, brechas de segurança, ataques sofisticados e indisponibilidade do sistema.

4.2.2. Evolução das fraudes no ambiente do *Internet Banking*

Como já relatado anteriormente, transações bancárias via *internet banking* é a forma de atendimento com maior crescimento atual. A internet tornou-se parte do dia a dia de grande parte da população brasileira devido suas inúmeras facilidades agregadas.

Neste cenário de crescimento dos meios digitais de acesso as informações bancárias e maior digitalização dos processos, é crescente a preocupação com riscos e o aumento de fraudes eletrônicas nos sistema de *internet banking*. De acordo com o Febraban (2013), prejuízos com fraudes eletrônicas passaram de um bilhão de reais em 2012 e diante desta situação as instituições bancárias investem em soluções de segurança da informação cada vez mais complexas, a fim de assegurar a integridade, confidencialidade, disponibilidade, privacidade e autenticidade das informações presentes nas transações bancárias.

Fraude eletrônica pode ser definida como um acesso ou transação bancária não autorizada realizado através da internet, também é entendida como resultado de um conjunto de violações de controles de segurança que na última fase é efetivado uma operação financeira não autorizada (DAMIANO, 2013, p. 35).

De acordo com o CERT.br (Cartilha de Segurança para Internet, 2013), uma das principais técnicas utilizada por fraudadores para ter acesso as informações é o *Phishing* onde os fraudadores tentam obter dados pessoais e financeiros de um usuário através do envio de mensagens eletrônicas com diferentes temas, campanhas publicitárias e assuntos de destaque do momento a fim de atrair a atenção do usuário.

Uma forma de *phishing* constantemente utilizado no *internet banking* é o envio de e-mail, em nome de uma instituição bancária que induz o usuário a clicar em um link. Com este processo, automaticamente é direcionado a uma pagina *web* falsa idêntica ao site original da instituição bancária e são solicitados dados pessoais e financeiros (CARTILHA DE SEGURANÇA PARA INTERNET, 2013, p. 05).

Para captura das informações é utilizado o *spyware*, denominado como um tipo de código malicioso programado para monitorar as atividades de um sistema e logo após enviar os dados coletados a terceiros. São exemplos:

- ***Keylogger:*** Técnica capaz de capturar e arquivar as teclas digitadas pelo usuário. A ativação desta técnica, na maioria dos casos, é condicionada a uma ação prévia do usuário, como por exemplo, acesso a um site específico de *internet banking*;
- ***Screenlogger:*** Técnica análoga ao *keylogger*, é capaz de armazenar a posição do cursor e a tela apresentada no monitor, no momento em que o mouse é clicado ou na região próxima onde o mouse é clicado. Este técnica é utilizada por atacantes a fim de capturar as teclas digitadas em teclados virtuais, usados em *internet banking*.

Os fraudadores também utilizam os *Trojan Banker* que é um tipo de *trojan* capaz de coletar dados bancários através da instalação de *spywares* ativados quando sites de *internet banking* são acessados.

A tabela 5 apresenta que muitos riscos relacionam-se aos próprios usuários e outros aos meios de utilização dos serviços.

Tabela 5: Principais riscos à cadeia de valor digital.

	RISCOS DOS USUÁRIOS			RISCOS DO MEIO		
	Usuário	**Identidade digital**	**Dispositivo**	**Infraestrutura**	**Aplicativos**	**Serviços**
Principais Ameças	O humano é o alvo Ataques visam as informações carregadas pelos usuários ao invés dos computadores	A identidade é o alvo Ataques se concentram no comprometimento de credenciais para obter informações	O dispositivo é o alvo Dispositivos carregam informações valiosas não protegidas pela segurança tradicional	A infraestrutura é o alvo Infraestrutura desenvolvida para suportar o processamento da informação	O aplicativo é o alvo Corromper aplicativos para obter informação para ataque aos clientes	O serviço é o alvo Ataques de DoS derrubando os serviços das empresas
Exemplos	Técnicas usadas para obter login, senha e outras informações diretamente dos usuários Dificuldade dos usuários de desenvolver, implementar ou seguir políticas e práticas de segurança	Informações de internet banking e de cartões de crédito atacadas para roubo e venda Nomes, endereços e números de identificação usados como base para o roubo de identidade	Ataques Zero-day, que visam dispositivos antes da instalação de proteção Furto de computadores / pen drives contendo informação confidencial Dispositivos desenhados com poucas funcionalidades de segurança	Ataques Man-in-the-Middle explorando vulnerabilidades da infraestrutura iludindo usuários a acreditar que estão interfaceando com as entidades legítimas	Vulnerabilidades em aplicações utilizadas para comprometer websites e acessar informação sigilosa	Programas maliciosos para coordenar ataque de diversos usuários zumbis

Fonte: Booz & Company (CIAB FEBRABAN, 2012)[7]

4.2.3. Gerenciamento de Riscos no *Internet Banking*

Entende-se como risco a situação que cria oportunidades ou produz perdas. Tratando-se de segurança da informação, os riscos são condições que criam ou potencializam danos e perdas. É avaliado de acordo com a possibilidade de um fato se concretizar e produzir perdas (DANTAS, 2011).

De acordo com a norma NBR ISO 31000:2009[8], a gestão de riscos é definida como um conjunto coordenado de atividades e métodos usados com intuito de direcionar uma organização para o controle de diversos riscos capazes de prejudicar a capacidade de alcance dos objetivos.

Segundo informações do cert.br, ao realizar transações bancárias através do *internet banking* os principais riscos são:

---

[7] CIAB FEBRABAN 2012. Disponível em: <http://www.ciab.com.br/_pdfs/publicacoes/AnuarioFebraban.pdf>. Acesso em: 14 mai 2014.

[8] Norma ABNT NBR ISO 31000:2009: Fornece princípios e diretrizes genéricas para a gestão de riscos. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=57311>. Acesso em: 14 mai 2014.

- **Perdas financeiras:** As contas bancárias podem ser utilizadas para ações maliciosas como transferências indevidas de dinheiro e pagamentos de contas de terceiros;
- **Invasão de privacidade:** Ao ter acesso indevido a contas bancárias é possível ter acesso a informações pessoais sobre as transações bancárias e consequentemente expor a privacidade do titular da conta bancária;
- **Violação de sigilo bancário:** O sigilo bancário é direito adquirido do titular da conta e há possibilidades de violação, caso a conta bancária seja acessada indevidamente por terceiros;
- **Participação em esquemas de fraudes:** A conta bancária poderá ser utilizada na aplicação de golpes e fraudes.

Foi publicado pelo Comitê da Basiléia (órgão internacional que incentiva a cooperação entre bancos) um manual com princípios de gerenciamento de riscos para o *internet banking*, neste manual os princípios desenvolvidos estão classificados em três categorias, sendo elas:

Princípios de vigilância da comissão de diretoria e gerência sênior:

- Gerenciamento efetivo das atividades de *internet banking*;
- Criação de um processo de controle de segurança que seja de fácil entendimento;
- Planejamento de terceirização de acordo com analise de consequências;

Princípios de controles de segurança:

- Autenticação dos usuários de *internet banking*;
- Não repudio e contabilização das transações realizadas pelo *internet banking*;
- Medidas que asseguram segregação de funções;
- Controles apropriados de autorização em sistemas de *internet banking*, banco de dados e aplicações;
- Integridade dos dados de transações, registros e informações do *internet banking*;
- Estabelecimento de um caminho de auditoria para as transações realizadas via *internet banking*;
- Confidencialidade em informações bancárias essenciais;

Princípios legais e de reputação do gerenciamento de riscos:

- Apresentação adequada dos serviços de *internet banking*;
- Privacidade das informações do cliente;
- Capacitação, plano de continuidade e contingência de negócio que asseguram a disponibilidade do sistema e serviços de *internet banking*;
- Plano de respostas para incidentes.

4.3. Modelos atuais de segurança adotados pelos bancos brasileiros

As instituições bancárias que disponibilizam atendimento aos clientes via *internet banking*, pesquisam modelos de segurança que sejam capazes de identificar os usuários e simultaneamente autorizar as movimentações financeiras, criando um método de proteção contra fraudes eletrônicas. Porém, os modelos de segurança da atualidade, atuam em um cenário de identificação de fraudes eletrônicas, dessa forma o modelo torna-se sempre reativo e não proativo, pois somente quando há fraude algum processo de segurança é iniciado (MELO, 2012).

Serão apresentados a seguir, os principais modelos de segurança implantados pelos sete maiores bancos no Brasil, de acordo com informações do Banco Central do Brasil. A maioria dos sistemas de segurança utilizam no início uma forma de identificação baseada em credenciais e senhas, esse modelo de segurança que se baseia em informações conhecidas pelo usuário é utilizado como método de autenticação e aplica-se quando movimentações de recursos financeiros é realizado (MELO, 2012).

Dispositivos *One-Time Password* (*Token*): Geralmente utilizados como um segundo fator de autenticação forte. Neste modelo de dispositivo é disponibilizado senhas que são utilizadas uma única vez. O objetivo principal é evitar que dados já exibidos sejam reutilizados, a senha torna-se descartável.

Cartões *One-Time Password*: Pertence ao mesmo segmento do *One-Time Password* (*Token*), porém é um método com menores custos para a implantação de senhas dinâmicas e também concede um segundo fator de autenticação, porém em algumas instituições bancárias estas senhas são reutilizáveis e torna o sistema vulnerável a ataques.

Proteção do navegador: Neste método, a intenção é proteger o usuário através da utilização do navegador de internet utilizado para acesso ao *internet banking*. Com este processo o usuário fica protegido contra ataques de *malwares* conhecidos, através do monitoramento da área de memória alocado pelo navegador, com intuito de detectá-los e impedir o roubo de credenciais e acesso a informações confidenciais.

Teclados Virtuais: Método desenvolvido para dificultar a captura de credenciais dos usuários através do *keyloggers*, os teclados virtuais utilizam a linguagem de programação Java com criptografia baseada em software.

Dispositivos Registrados: Restringe o acesso ao sistema bancário apenas à dispositivos previamente cadastrados, técnica também conhecida como "impressão digital de *hardware*" é utilizada juntamente com a identificação do usuário através de credenciais. Porém, atualmente algumas instituições bancárias optaram por retirar o cadastramento e utilizar apenas a identificação para facilitar o acesso.

Identificação Positiva: Neste método é solicitado informações aos usuários que teoricamente apenas o usuário legítimo tem como fornecer, com intuito de identificar-se. É aplicado como método de autenticação secundário.

CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*): O objetivo desse método é tornar inválidos os ataques automatizados contra sessões autenticadas pelas instituições bancárias. Neste processo o usuário deverá digitar informações (solicitadas pelo site da instituição bancária) apresentadas em imagens difíceis de serem reconhecidas e processadas por robôs automatizados, inibindo sua ação.

SMS (*Short Message Service*): Método utilizado para confirmar a autenticação, conhecido como um canal de segunda autenticação é enviado ao usuário um conjunto de caracteres que devem ser informados, a fim de autorizar e processar a transação através do *internet banking*.

Monitoramento de Transação: Cada instituição bancária poderá utilizar este método através de várias técnicas, como por exemplo: inteligência artificial, análise de

históricos de transações e outros métodos capazes de identificar padrões de fraudes em transações realizadas anteriormente.

4.4. Aplicações da Cerificação Digital nas Instituições Bancárias

A presença da certificação digital nas instituições bancárias é evidenciada nas aplicações:

Certificados Digitais

São utilizados para autenticar os usuários (pessoa física e pessoa jurídica) e também o sistema bancário, este processo é possível se houver uma infraestrutura de chave pública (ICP) e uma autoridade certificadora (AC) representando uma terceira parte confiável capaz de assinar os certificados e atestar a validade do mesmo. No Brasil é utilizado pelas instituições bancárias os certificados A1 e A3 emitidos e assinados pela ICP Brasil.

É uma identidade eletrônica capaz de permite que uma transação via *web* seja segura. Esta tecnologia de segurança proporciona qualidade, compromisso social e modernidade, diminuindo a distância física, evitando fraudes e falsificações.

Assinatura de Contratos de Câmbio

O Banco Central do Brasil fez a alteração na regulamentação de contratos de câmbio, que são mecanismos específicos entre o vendedor e comprador de moeda estrangeira, onde são acordadas as condições para a realização da operação de câmbio. As alterações tem intuito de permitir a assinatura digital de acordo com novos procedimentos e padrões técnicos. Com este processo, acredita-se na maior agilidade para a liberação de contratos de câmbio nas instituições financeiras (BANCO CENTRAL DO BRASIL, 2004).

Sistema de Pagamentos Brasileiro (SPB)

Desde 22 de abril de 2002, o Sistema de Pagamentos Brasileiro (SPB) apresenta alto grau de automação, através da utilização de meios eletrônicos para transferência de fundos e liquidação de pagamentos por meios eletrônicos substituindo arquivos em papel e por fazer a ligação das instituições financeiras credenciadas ao Banco Central do Brasil[9].

O Sistema de Pagamentos Brasileiro (SPB) utiliza certificados digitais da ICP-Brasil para realizar a autenticação e verificação da identidade dos participantes em todos os processos realizados.

---

[9] BANCO CENTRAL DO BRASIL. Disponível em: < http://www.bcb.gov.br/?SPBVISGER >. Acesso em: 14 mai 2014.

5. PESQUISA DE CAMPO

Com intuito de responder ao questionamento principal e atingir o objetivo proposto é importante a aplicação de um método capaz de fornecer embasamento confiável para a análise e reflexão dos dados a fim de alcançar conclusões reais. Dessa forma, foi definida como método a pesquisa quantitativa, esta acredita que tudo pode ser quantificável, ou seja, é possível representar em números as informações, opiniões, reações, hábitos e atitudes e assim classifica-las e analisa-las (FABENY, p. 42, 2007).

Ao longo da discussão dos resultados, hipóteses poderão ser construídas que darão abertura para a produção de trabalhos futuros na intenção de construir um aprofundamento do tema e contexto em questão.

5.1. DETALHAMENTO DA PESQUISA

A pesquisa foi dividida em duas fases: a pesquisa bibliográfica e a pesquisa qualitativa-descritiva. A fase inicial, baseada em pesquisas bibliográficas feita com autores renomados e outras fontes de informação (artigos, monografias, teses e dissertações) buscou detalhar conceitos e técnicas de criptografia e certificação digital e sua aplicação no ambiente de *internet banking*.

O principal objetivo de uma pesquisa bibliográfica é proporcionar maior nível de familiaridade entre o pesquisador e o tema proposto e adquirir dados que possibilitem uma apuração mais detalhada e completa sobre o objeto de estudo. Com os dados alcançados nesta primeira fase, foi possível estruturar o questionário de coleta de dados utilizado na segunda fase de pesquisa (FABENY, p.43, 2007).

A segunda fase é a pesquisa qualitativa-descritiva que tem como objetivo descrever as características de uma população, classificar e interpretar os resultados, afim de apresentar as relações entre segurança da informação, certificação digital e *internet banking*. As pesquisas deste tipo caracterizam-se pelo questionamento de uma população amostral, na qual se deseja conhecer o comportamento dos mesmos.

O questionário estruturado de coleta de dados contém 10 questões (APÊNDICE A) predominantemente fechadas. O período de coleta foi de 01/05/2014 até 31/05/2014, esta abordagem teve como objetivo analisar o grau de utilização do *internet banking* e satisfação com esta ferramenta pelos usuários da população amostral.

5.2. RESULTADOS E DISCUSSÕES

Nesta seção é feita a análise dos resultados, que compreende a tabulação dos dados, análise e interpretação dos mesmos. O questionário de coleta de dados contém dois blocos de questões, as iniciais tem a intenção de identificar aspectos básicos de perfil da população amostral e as seguintes, são questões que englobam comportamentos, conhecimentos, atitudes e opiniões sobre o *internet banking*.

5.2.1. PERFIL DA AMOSTRA

Abaixo, através dos gráficos 1 e 2, são apresentados os dados que caracterizam o perfil da população amostral que participou do questionário, os dados em questão são a faixa etária e qual o tipo de empresa/ organização pertencem. Neste questionário houve a participação de 100 pessoas.

Gráfico 1: Faixa Etária

Opções de resposta	Respostas	
Até 20 anos	18,00%	18
Entre 21 e 30 anos	49,00%	49
Entre 31 e 40 anos	28,00%	28
Entre 41 e 50 anos	5,00%	5
Entre 51 e 60 anos	0,00%	0
Mais de 60 anos	0,00%	0
Total		100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

Gráfico 2: Tipo de empresa/organização pertence

Opções de resposta	Respostas	
Indústria	12,00%	12
Comércio	16,00%	16
Empresa do setor de serviços	34,00%	34
Universidade/escola	19,00%	19
Empresa pública	14,00%	14
Autônomo	5,00%	5
Total		100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

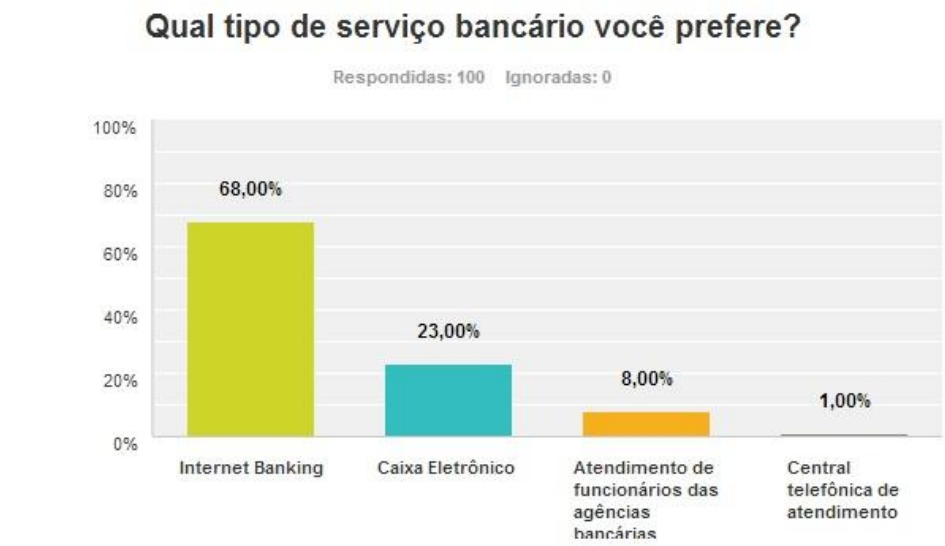
De acordo com os percentuais alcançados é perceptível que a faixa etária predominante na população amostral da pesquisa, apresenta idades entre 21 a 30 anos com um percentual de 49,00%, entretanto, a faixa etária com menor percentual esta entre 41 e 50 anos com 5,00% e idade acima de 50 anos o percentual é 0,00%. Com isso, é possível aferir que as faixas etárias mais elevadas demonstram dificuldades na utilização de novas tecnologias e por vezes são resistentes às mudanças, dando preferência a métodos tradicionais. Em contrapartida, a população amostral mais jovem se adapta com facilidade as novas tecnologias e a integram em seu dia a dia.

Em relação ao tipo de empresa/ organização, há uma predominância do setor de serviços, com um percentual de 34,00%. O perfil deste setor que cresce constantemente nos últimos anos, concentra empresas inovadoras e de mais alta tecnologia o que confirma o crescimento e desenvolvimento de novas tecnologias, conforme tratado no decorrer do trabalho.

5.2.2. ASPECTOS RELATIVOS AO *INTERNET BANKING*

Os dados e percentuais apresentados a partir deste tópico, referem-se às atitudes, preferências, conhecimento e opiniões a respeito dos sistemas de *Internet Banking* e dispositivos de segurança utilizado nos mesmos.

Gráfico 3: Preferência de serviço bancário



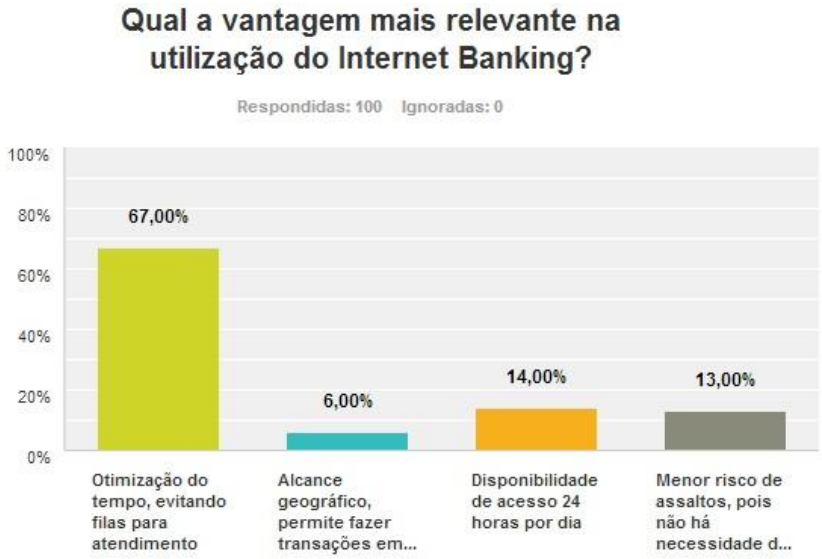
Opções de resposta	Respostas	
Internet Banking	68,00%	68
Caixa Eletrônico	23,00%	23
Atendimento de funcionários das agências bancárias	8,00%	8
Central telefônica de atendimento	1,00%	1
Total		100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

Correlacionando as questões 03 e 09 (APÊNDICE A), é possível observar mais um aspecto da aderência às novas tecnologias motivada na maioria das vezes, pelos muitos afazeres da vida moderna, tempo cada vez mais escasso e limitado no dia a dia das pessoas. O gráfico 3 aponta que 68,00% da população amostral desta pesquisa tem preferência em realizar transações *online*. Conforme é tratado no capítulo 4, a evolução do *internet banking* nos últimos anos é cada vez mais rápida e torna-se destaque no cenário atual, o número de transações via *internet banking* já supera as transações feitas de forma tradicional (dado demonstrado no gráfico 3). Esta predileção explica-se pela facilidade, comodidade e agilidade oferecida por esta forma de atendimento.

O gráfico 4 vem de encontro a este cenário, indicando com 67,00% que a vantagem mais relevante na escolha dos processos realizados via *internet banking* é devido a otimização do tempo, evitando filas para atendimento.

Gráfico 4: Vantagem na utilização do *Internet Banking*



Opções de resposta	Respostas
Otimização do tempo, evitando filas para atendimento	67,00% 67
Alcance geográfico, permite fazer transações em qualquer lugar do mundo	6,00% 6
Disponibilidade de acesso 24 horas por dia	14,00% 14
Menor risco de assaltos, pois não há necessidade de deslocamento a uma agência bancária	13,00% 13
Total	100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

Como historicamente ocorre quando há mudanças e avanços, alguns aspectos de grande importância tornam-se evidentes, com a ascensão do *internet banking* não foi diferente. A segurança tornou-se um grande desafio para as instituições bancárias que disponibilizam e investem em tecnologias para sistemas de *internet banking*. Esta forma de atendimento expõe as informações a riscos de segurança e tornou-se alvo de fraudes por ter valor financeiro agregado.

A questão de segurança para realizar transações bancárias através da internet é de tão grande importância, que é apontado no gráfico 5 com 73,74% como o principal fator de restrição a utilizá-lo ou demora em começar a utilizar os benefícios deste sistema de atendimento.

Gráfico 5: Restrição mais importante para a não utilização do *Internet Banking*

Opções de resposta	Respostas	
Sensação de falta de segurança; receio da ocorrência de fraudes ou violação de privacidade	73,74%	73
Dificuldade de navegação no site do banco	9,09%	9
Preferencia por outras formas de atendimento (atendimento pessoal; auto atendimento; central de atendimento por telefone)	17,17%	17
Total		99

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

Com a intenção de solucionar problemas de segurança, o setor bancário é considerado um dos que mais investem em tecnologia da informação, este é essencial para a manutenção dos benefícios alcançados. Neste cenário, além de toda a parte técnica a ser desenvolvida para garantir a integridade dos dados e prevenção de fraudes, é de grande importância um trabalho voltado à conscientização quanto aos cuidados básicos a ser feito pelos clientes, conscientização do aspecto humano deste processo.

Uma página da instituição bancária com informações de segurança, cartilhas, tutoriais e até mesmo projetos de encontros e fórum de discussões com clientes, poderá além de fortalecer a relação de confiança com o banco, criar hábitos de cuidados básicos que evitam fraudes bancárias, o gráfico 6 aponta que 49,00% da população amostral já visualizou a página com informações de segurança da instituição bancária, porém um fato de importante relevância neste gráfico é que 39,00% não procuram informações de segurança antes de realizar transações, ou seja, há um grande trabalho a ser feito relacionado a conscientização, a engenharia social.

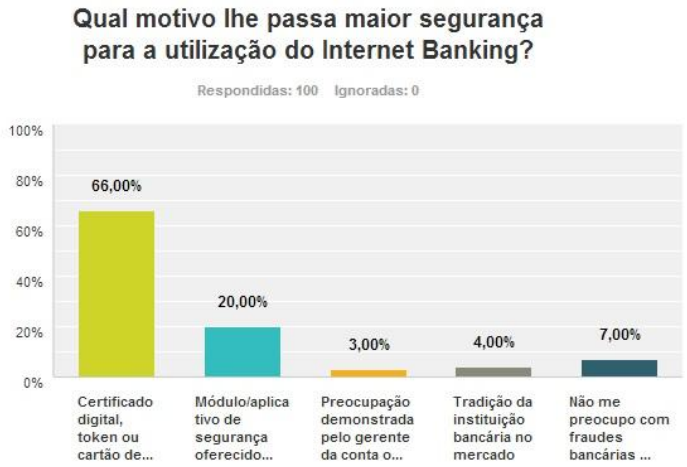
Gráfico 6: Dicas para prevenção de fraudes bancárias

Opções de resposta	Respostas
Sim, há uma página direcionada a segurança e de fácil entendimento	49,00% 49
Sim, há uma página direcionada a segurança porém as informações são difíceis de serem entendidas	11,00% 11
Não há uma página web com informações de segurança contra fraudes bancárias	1,00% 1
Não sei dizer, pois não procurei no web site bancário informações de segurança	39,00% 39
Total	100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

O gráfico 7 comprova a importância de alguns dispositivos de segurança para o acesso seguro ao *internet banking*, dentre eles 66,00% da população amostral aponta o certificado digital, *token* e cartão de segurança como os principais. Neste momento, o certificado digital ganha destaque como importante ferramenta a ser utilizada tanto por pessoa física como pessoa jurídica para o acesso seguro, considerando todo o processo interno de segurança de um certificado digital, conforme tratado em grande parte deste trabalho, sua aplicação no *internet banking* confirma seus benefícios para um ambiente *web* mais confiável e seguro, principalmente quando trata-se de transações financeiras com alto valor agregado.

Gráfico 7: Motivo de maior segurança na utilização do *Internet Banking*



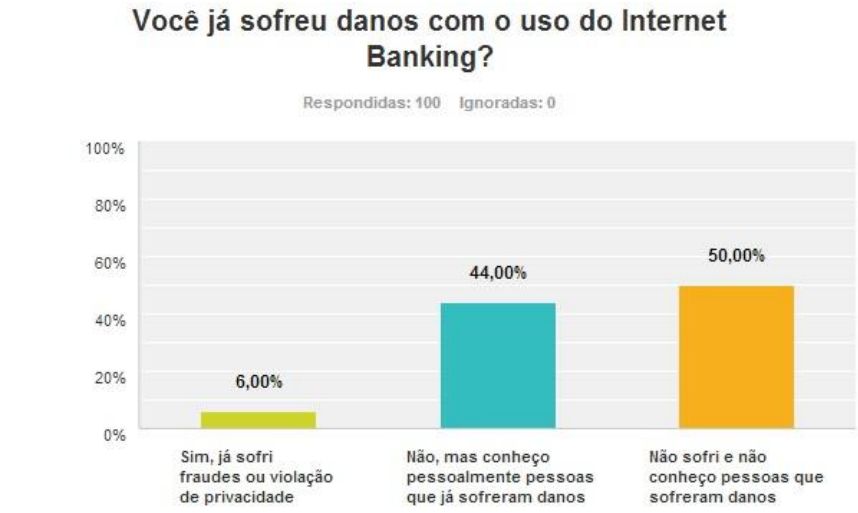
Opções de resposta	Respostas	
Certificado digital, token ou cartão de segurança solicitados para que seja possível acessar a conta	66,00%	66
Módulo/aplicativo de segurança oferecido pelo banco, para que seja possível acessar a conta somente com este aplicativo instalado	20,00%	20
Preocupação demonstrada pelo gerente da conta ou informações disponibilizadas no web site para a prevenção de fraudes bancárias	3,00%	3
Tradição da instituição bancária no mercado	4,00%	4
Não me preocupo com fraudes bancárias ao acessar o internet banking	7,00%	7
Total		100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

É possível observar no gráfico 8 que apenas 6,00% da população amostral relata ter sofrido fraudes ou violação de privacidade no *internet banking*, porém 44,00% dizem conhecer pessoalmente pessoas que sofreram danos neste ambiente, este grande percentual aponta a necessidade de ser feito cada vez mais investimentos no desenvolvimento de novas soluções de segurança da informação e a utilização mais disseminada da certificação digital, considerando que, de acordo com informações da FEBRABAN, a estimativa é que até 2017 transações via internet correspondam cerca de 60,00% das operações bancárias.

Por fim, o gráfico 9 demonstra que 57,00% da população amostral esta satisfeita com o ambiente *web* de *internet banking*, esse percentual é resultado dos investimentos feito até então pelas instituições bancárias, a fim de proporcionar uma forma de atendimento mais ágil, com grande comodidade, facilidade, grande alcance geográfico, disponibilidade 24 horas por dia, diminuindo os riscos de assaltos e com projetos e investimentos para a diminuição de fraudes *online*.

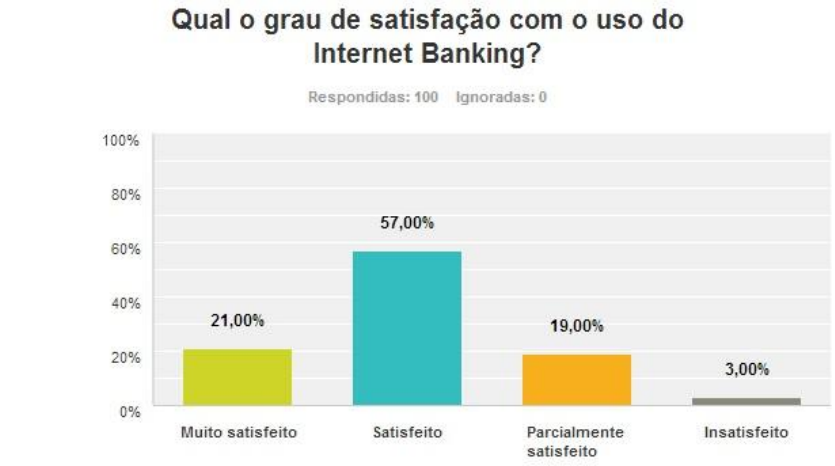
Gráfico 8: Danos com o uso do *Internet Banking*



Opções de resposta	Respostas	
Sim, já sofri fraudes ou violação de privacidade	6,00%	6
Não, mas conheço pessoalmente pessoas que já sofreram danos	44,00%	44
Não sofri e não conheço pessoas que sofreram danos	50,00%	50
Total		100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

Gráfico 9: Grau de satisfação com o *Internet Banking*



Opções de resposta	Respostas	
Muito satisfeito	21,00%	21
Satisfeito	57,00%	57
Parcialmente satisfeito	19,00%	19
Insatisfeito	3,00%	3
Total		100

Fonte: Instrumento de coleta – Questionário *Internet Banking* (2014)

6. CONCLUSÃO

O propósito deste trabalho foi analisar as características e benefícios da certificação digital e sua aplicação no ambiente *web*, em especial nos sistemas de *internet banking*, que se apresenta como uma ferramenta em constante crescimento e desenvolvimento, permitindo que os clientes façam suas transações bancárias com maior agilidade, praticidade, comodidade e segurança.

A certificação digital é uma tecnologia de segurança que ganha cada vez mais espaço no cenário atual, pois seu método eficaz vem de encontro às necessidades que surgem com o avanço das transações *online*, em especial transações realizadas em sistemas de *internet banking* que frequentemente tornam-se alvo de fraudadores por ter valor financeiro associado. Além de métodos eficazes que garantem a segurança dos dados, como discorrido ao longo do trabalho, a certificação digital apresenta garantia jurídica, considerando que há uma autenticação que assegura e valida a transação, processo de responsabilidade das autoridades certificadoras.

Para atingir os objetivos propostos, inicialmente foi argumentado sobre os principais conceitos técnicos de criptografia simétrica e assimétrica, RSA, funções *hash* e assinatura digital. Em seguida, foi detalhado o que a certificação digital pode oferecer através da Infra Estrutura de Chaves Públicas, foi destacado o trabalho realizado pelas autoridades certificadoras, autoridades de registro, qual o ciclo de vida de um certificado digital, argumentado também sobre o sigilo das comunicações, padrão x.509, a medida provisória 2200-02, a Infra Estrutura de Chaves Públicas do Brasil e algumas aplicações da certificação digital.

Após estas abordagens, foi dado um enfoque nos sistemas de *internet banking*, que tem grande destaque neste trabalho por oferecer diversos benefícios tanto para as instituições financeiras quanto aos clientes, foi discorrido sobre o papel da tecnologia da informação no setor bancário, evolução de fraudes no ambiente de *internet banking*, modelos atuais de segurança adotado pelas instituições bancárias e enfim apresentado a pesquisa de campo que confirma alguns aspectos que fazem parte da argumentação teórica.

A análise dos resultados da pesquisa de campo possibilitou também a conclusão de que grande parte da população amostral se diz satisfeita com os serviços disponibilizados nos ambientes de *internet banking* e como a certificação digital impacta positivamente a utilização segura destes ambientes. De acordo com dados estatísticos fornecidos pela FEBRABAN, até 2017 cerca de 60% das transações bancárias poderão ser feitas via internet; este dado foi comentado em alguns momentos no decorrer do trabalho para demonstrar como a estimativa

de crescimento deste ambiente é alta e como consequência a certificação terá cada vez maior destaque neste cenário para garantir a segurança do processo.

Os resultados da pesquisa não podem ser generalizados devido ao número de participantes da população amostral e questões pouco aprofundadas, sendo assim, este trabalho poderá servir como degrau para o desenvolvimento de outros trabalhos com maior amplitude sobre o tema e contexto.

6.1. TRABALHOS FUTUROS

Com intuito de dar continuidade a esta linha de estudo, durante o seu desenvolvimento surgiu a possibilidade de um trabalho futuro com o tema:

- Aspecto Humano: O processo de conscientização como aliado na prevenção de fraudes bancárias.

Devido ao grande percentual (39,00%) da população amostral declarar que não buscam informações de segurança antes de realizar transações bancárias, um importante ponto a ser abordado e desenvolvido é que toda parte técnica para prevenção de fraudes é de extrema importância, porém cuidados básicos que podem ser feitos pelos clientes poderão prevenir grande parte das fraudes relatadas no momento, por isso o tratamento do aspecto humano e trabalhos de conscientização são essenciais neste tema.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSINATURA DIGITAL. Funcionamento da Assinatura Digital. Disponível em: <http://www.gta.ufrj.br/grad/07_1/ass-dig/index.html>. Acesso em: 09 mai 2014.

BANCO CENTRAL DO BRASIL. Departamento de Tecnologia da Informação. Carta-Circular n° 3134, de 27 de abril de 2004. Divulga os procedimentos e padrões técnicos para uso de assinatura digital em contratos de câmbio. Diário Oficial da União, Brasília, DF, 27 abri. 2004.

BRAGA, Lamartine Vieira. Contribuições da Certificação Digital ao Desenvolvimento do Governo Eletrônico e Aperfeiçoamento de Políticas Públicas e Serviços Públicos no Brasil. 2008. 100f. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2008.

BRASIL. Medida provisória n° 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileiras – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial da União, Brasília, DF, 24 ago. 2001.

CAMARA-E.NET – Câmara Brasileira de Comércio Eletrônico. São Paulo, SP. Disponível em: <http://www.camara-e.net/>. Acesso em: 09 maio de 2014.

CARTILHA DE SEGURANÇA PARA INTERNET. São Paulo, SP. Cert.br, fascículo Internet Banking, ago. 2013.

CG ICP-BRASIL – Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileiras. Aprova a versão 5.0 do documento requisitos mínimos para as políticas de certificado na ICP-Brasil (DOC-ICP-04). Resolução n° 91, de 05 de julho de 2012.

CIAB FEBRABAN 2012, 2012. São Paulo, SP. A sociedade conectada. Setor bancário em números, tendências tecnológicas e agenda atual. São Paulo, SP. Federação Brasileira de Bancos, 2012.

CIVIDANES, Rafael de Simone. Sistemas para Gerenciamento de Chaves em ICPs – Infra-Estrutura de Chaves Públicas. 2008. 152f. Tese (Mestrado em Ciências no Curso de Engenharia Eletrônica e Computação) – Instituto Tecnológico de Aeronáutica, São José dos Campos, 2008.

DAMIANO, André Luis. As Fraudes no Internet Banking e sua evolução para o Social Banking. 2013. 107f. Dissertação (Mestrado em Engenharia de Produção) – Escola de Engenharia de São Carlos da Universidade de São Paulo, São Carlos, 2013.

DANTAS, Marcus Leal. Segurança da Informação: Uma abordagem focada em Gestão de Riscos. Olinda: Livro Rápido, 2011.

FABENY, Gilson. Fatores Geradores de Resistência ao Uso do *Internet Banking* no Banco do Brasil S.A.: Um Estudo de Caso na Agência de Itapema SC. 2007. 59f. Trabalho de Conclusão de Curso (Pós-Graduação em Administração) – Escola de Administração da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2007.

FEBRABAN – Federação Brasileira de Bancos. São Paulo, SP. Disponível em: <http://www.febraban.org.br/Noticias1.asp?id_texto=2089&id_pagina=60&palavra=>. Acesso em: 29 ago. 2013.

GUELFI, Airton Roberto. Análise de Elementos Jurídico-Tecnológicos que compõem a Assinatura Digital Certificada Digitalmente pela Infra-Estrutura de Chaves Publicas do Brasil – ICP-Brasil. 2007. 135f. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2007.

ITI – Instituto Nacional de Tecnologia da Informação. Brasília, DF. Disponível em: <http://www.iti.gov.br/>. Acesso em: 29 ago. 2013.

KUROSE, James F; ROSS, Keith W. Rede de Computadores e a Internet: Uma abordagem top-down. Pearson, 2010.

LUZ, Clarissa P. Centro de Certificação Digital: Construção, Administração e Manutenção. Rio de Janeiro: Ciência Moderna, 2008.

MATTAR, Alexandre. Critérios de Avaliação da Qualidade da Informação em Sistemas de Internet Banking. 2007. 89 f. Dissertação (Mestrado em Administração) – Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, São Paulo, 2007.

MELO, Laerte Peotta de. DAP (Dynamic Authorization Protocol): Uma abordagem segura out-of-band para e-bank com um segundo fator de autenticação visual. 2012. 118f. Tese (Doutorado em Engenharia Elétrica) – Faculdade de Tecnologia da Universidade de Brasília, Brasília, 2012.

MESQUITA, Rodrigo Ramos. Ganhos com a Certificação Digital. 2010. 49f. Trabalho de Conclusão de Curso (Graduação em Processamento de Dados) – Faculdade de Tecnologia de Taquaritinga, Centro Estatual de Educação Tecnológica "Paula Souza", Taquaritinga, 2010.

MONTEIRO, Emiliano S.; MIGNONI, Maria Eloisa. Certificados Digitais: Conceitos e Práticas. Rio de Janeiro: Brasport, 2007.

RECEITA FEDERAL – Secretaria da Receita Federal do Brasil. Disponível em: < http://www.receita.fazenda.gov.br/>. Acesso em: 09 maio 2014.

SANTOS, Humberto de Faria. Revoluções Tecnológicas e Sociedade. Revista Eletrônica da FIA, São Bernardo do Campo, n. 2, p. 11-57, Jul-Dez. 2006. Disponível em: < http://intranet.fainam.edu.br/acesso_site/fia/academos/revista2/6.pdf>. Acesso em: 29 Ago. 2013.

SILVA, Luiz Gustavo Cordeiro da et al. Certificação Digital – Conceitos e Aplicações – Modelos Brasileiro e Australiano. 1ª ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

SOUSA, Leandro Silva de. Certificação Digital: Análise da Aplicação da Certificação Digital nos Escritórios de Contabilidade da Cidade de Balsas-MA. 2010. 80f. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) – Unibalsas, Faculdade de Balsas, Balsas, 2010.

STALLINGS, William. Criptografia e segurança de redes: Princípios e Práticas. 4. Ed. São Paulo: Pearson Prentice Hall, 2008.

TIVOLI SOFTWARE. Como funciona o SSL. Disponível em: <http://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/pt_BR/HTML/admin231.htm>. Acesso em: 09 maio 2014.

TRINTA, Fernando Antonio Mota.; MACÊDO, Rodrigo Cavalcanti de. Um Estudo sobre Criptografia e Assinatura Digital. Departamento de Informática, Universidade Federal do Pernambuco, Pernambuco, Set. 1998. Disponível em: < http://www.di.ufpe.br/~flash/ais98/cripto/criptografia.htm>. Acesso em: 09 maio 2014.

APÊNDICE A – INSTRUMENTO DE PESQUISA (QUESTIONÁRIO)

Dados Sócio Demográfico

1- Faixa Etária:
( ) Até de 20 anos ( ) Entre 40 e 50 anos
( ) Entre 21 e 30 anos ( ) Entre 50 e 60 anos
( ) Entre 30 e 40 anos ( ) Mais de 60 anos

2- Qual tipo de empresa/organização você pertence?
( ) Indústria ( ) Empresa pública
( ) Comércio ( ) Autônomo
( ) Empresa do setor de serviços ( ) Outros
( ) Universidade/ escola

Uso de Serviços Tecnológicos

3- Qual tipo de serviço bancário você prefere?
( ) *Internet Banking*
( ) Caixa Eletrônico
( ) Atendimento de funcionário
( ) Central Telefônica de atendimento

4- Antes de utilizar os serviços disponíveis em *Internet Banking*, qual a restrição que considerava mais importante para não utilizar?
( ) Não confiava nas transações realizadas pela internet
( ) Falta de segurança; receio da ocorrência de fraudes ou violação de privacidade
( ) Dificuldade de navegação no site do banco
( )Preferencia por outras formas de atendimento (atendimento pessoal; autoatendimento; central de atendimento por telefone)
( ) Outros

5- O *web site* de seu banco disponibiliza uma página com dicas ou cartilhas de segurança, tutoriais ou textos com informações de como se prevenir de fraudes bancárias?
( ) Sim, há uma página direcionada à segurança e de fácil entendimento

( ) Sim, há uma página direcionada a segurança porém as informações são difíceis de serem entendidas

( ) Não há uma página web com informações de segurança contra fraudes bancárias

( ) Não sei dizer, pois nunca procurei no *web site* informações de segurança

6- Qual motivo lhe passa maior segurança para a utilização do Internet Banking?

( ) Certificado digital, *token* ou cartão de segurança solicitados para que seja possível acessar a conta

( ) Módulo/programa de segurança oferecido pelo banco, para que seja possível acessar a conta apenas com este módulo instalado

( ) Preocupação demonstrada pelo gerente da conta ou informações disponibilizadas no *web site* para a prevenção de fraudes bancárias

( ) Tradição da instituição bancária no mercado

( ) Não me preocupo com fraudes bancárias ao acessar o *internet banking*

7- Quais dispositivos de segurança você utiliza para acessar o *Internet Banking* (Pode ser selecionado mais de uma alternativa)?

( ) Certificado Digital ( ) *Tokens*

( ) Teclado virtual ( ) *Smartcards*

( ) Cartão chave de segurança ( ) Outros

8- Você já sofreu danos com o uso do *Internet Banking*?

( ) Sim, já sofri fraudes ou violação de privacidade

( ) Não, mas conheço pessoalmente pessoas que já sofreram danos

( ) Não sofri e não conheço pessoas que sofreram danos

9- Qual a vantagem mais relevante na utilização do *Internet Banking*?

( ) Otimização do tempo, evitando filas para atendimento

( ) Alcance geográfico, permite fazer transações em qualquer lugar do mundo

( ) Disponibilidade de acesso 24 horas por dia

( ) Menor risco de assaltos, pois não há necessidade de deslocamento a uma agência bancária

( ) Outros. Especificar:_____

10- Qual o grau de satisfação com o uso do *Internet Banking*?

( ) Muito satisfeito ( ) Parcialmente satisfeito

( ) Satisfeito ( ) Insatisfeito