CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA

CURSO DE GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

FERNANDA RODRIGUES DOS SANTOS

SEGURANÇA DA INFORMAÇÃO NAS TRANSAÇÕES ONLINE

Jahu, SP

2013

FERNANDA RODRIGUES DOS SANTOS

SEGURANÇA DA INFORMAÇÃO NAS TRANSAÇÕES ONLINE

Monografia apresentada à Faculdade de Tecnologia de Jahu, como parte dos requisitos para a obtenção do título de Tecnólogo em Gestão da Tecnologia da Informação.

Orientador: Prof. Ícaro Saggioro

Jahu, SP

2013

DEDICATÓRIA

Dedico estre trabalho aos familiares e amigos pelo apoio, incentivo e paciência que tiveram para comigo ao longo dos três anos de graduação.

AGRADECIMENTOS

Primeiramente agradeço à Deus pelas oportunidades dadas a mim até hoje, pela força nos momentos difíceis e por não permitir que eu parasse no meio caminhada.

Agradeço também aos familiares e amigos que sempre me incentivaram.

Ao Prof. Ícaro Saggioro pela prestatividade, disponibilidade e orientação.

Aos professores dedicados e comprometidos, em especial professores Wdson, José Renato Luchini, Sergio Castro e Ciccone que mesmo nos conteúdos mais entediantes, conseguiam transformar em aulas divertidas e prazerosas.

Aos colegas de classe pelas inúmeras risadas.

EPÍGRAFE

“A segurança é uma corrente, é tão segura quanto seu elo mais fraco.”

(Fernando Nery)

RESUMO

O número de usuário de web sites tem crescido de uma forma exponencial e o progresso tecnológico na construção de interfaces destes sistemas tem sido perceptível, gerando a necessidade de uma eminente variedade de aplicações para diversas áreas da *internet*, dentre as quais se encontra a segurança. A preocupação com esse setor e de extrema importância, pois as transações realizadas através da *internet* vai desde o fornecimento de informações sigilosas à proliferações de dados pessoais. Todos os dias são criados novos métodos e processos visando melhorar a segurança e privacidade ao usuário desde o envio até o recebimento dados confidenciais e outros tipos de informações, contudo do lado aposto a quem deseja garantir a integridade das informações, há pessoas interessadas em faz mal uso das mesmas.

Palavras-chave: Segurança, Privacidade, Informação, *Internet*.

ABSTRACT

The number user of the web sites have grow exponential way, and the technological progress on building interfaces for that systems have been seen noticeable, generating a need for a variety of applications for several areas on the internet, “among which the security” The discomfort with this sector is of extreme importance, because of the transactions realized on the web that covers from supply of sensitive information to proliferations of personal data. Everyday are created news methods and process to improve the security and privacy to the user at the time that will send or receive confidential data and other types of information, but there are many opposite people that to want make bad use that informations.

Keywords: Security, Privacy, Information, Network.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE SIGLAS

SSL: Security Socket Layer
TSL: Transport Layer Security
CID: Confiabilidade, Integridade e Disponibilidade
PPT: Pessoas, Processos e Tecnologia
CD: Certificado Digital
AC: Autoridade Certificadora
AR: Autoridade de Registro
MAC: Message Authentication Code
HTTP: HyperText Transfer Protocol
HTTPS: HyperText Transfer Protocol Secure
VPN: Virtual Private Network
URL: Uniform Resource Locator
PCI Payment Card Industry

SUMÁRIO

1 INTRODUÇÃO

Atualmente as pessoas vêm sofrendo inúmeras ameaças no que se diz respeito a sua segurança, sendo assim, eram esperadas que o ambiente da *Internet* também se tornasse alvo de ataques.

Assim como no mundo real, onde as pessoas precisam de proteger de mal feitores com seguranças, grades, alarmes, rastreadores e tudo mais, no ambiente virtual também se faz necessária uma proteção efetiva dos dados e informações sigilosas.

Devido as facilidades oferecidas, milhares de usuários domésticos, empresas, instituições, entre outros, vem usando a *Internet* para se realizar(por exemplo) transações bancárias, compras (*e-commerce*) e etc. Desta forma, com os “olhares” voltados para transações online, a segurança de informação se problema potencialmente crítico.

Falaremos a seguir da segurança de transações de dados *online* de ângulos diferentes, assim como ameaças envolvidas nas transações, criptografia de dados, certificados digitais, ferramentas, protocolos e gerência de segurança, a fim de tornar os sistemas e a redes mais seguras e confiáveis.

1.1 TEMA

Devido ao aumento expressivo das pessoas na utilização do ambiente virtual, o mesmo vem -cada vez mais- sendo alvo constante de ataques. Neste sentido, há necessidade de buscar um planejamento de gestão da segurança da informação para estabelecer e evitar os riscos e ameaças no momento em que as transações de dados são realizadas.

1.2 DEFINIÇÃO DO PROBLEMA

Visto que a cada dia o ambiente virtual vem se tornando alvo de ataques que tentam constantemente derrubar a sua segurança, que ações concretas e visíveis a sua organização e a população têm realizado para evitar a fraude de integridade, confidencialidade e disponibilidade em ambientes virtuais onde são realizadas as transações de dados?

1.3 OBJETIVOS

1.3.1 Objetivos Gerais

Com base nas pesquisas realizadas, pretende-se que haja um aprofundamento maior no que tange a Segurança da Informação com relação as Transações *Online* e assim utilizá-las no dia-a-dia, tanto na área pessoal quanto na profissional.

1.3.2 Objetivos Específicos

São objetivos específicos deste trabalho acadêmico:

- Adquirir maior conhecimento sobre Transações *Online*;
- Analisar a que riscos os dados e informações estão sujeitos ao serem processamos na *internet*;
- Verificar os métodos e ferramentas disponíveis que oferecem maior segurança para o trafego de dados.

1.4 METODOLOGIA

Visando um embasamento melhor sobre o tema, o tipo de pesquisa a ser realizada será por meio de levantamento bibliográfico.

A pesquisa terá por objetivo obter maiores informações sobre o próprio tema e também assuntos relacionados.

Após o levantamento de informações necessárias para o começo do desenvolvimento do projeto, será definido um escopo sobre o tema e sub temas que será abordado durante o mesmo.

Com o escopo definido, as ações a serem tomadas será organizar e desenvolver os assuntos. Ao final de todo o processo, será realizada a conclusão sobre o tema e será informada as fontes de pesquisa necessárias para a realização do projeto.

1.5 JUSTIFICATIVA

Atualmente a utilização de transações *online* de dados e informações, em substituição a vários procedimentos realizados de forma manual, é largamente empregada nas organizações. Isso porque além da comodidade, agilidade, essas operações proporcionam também um custo baixo para quem as utiliza.

Contudo, junto com os benefícios que as transações *online* proporciona, surge também os riscos e ameaças com relação a segurança das informações trafegadas no ambiente *online*. A todo momento surgem cr*ackers* em busca de informações para benefício próprio.

Assim, os motivos já citados evidenciam a importância da pesquisa realizada como forma de auxílio na prevenção de situações que possam colocar em risco a segurança de Transações *Online*.

2 REFERENCIAL TEÓRICO

Nesta seção apresentaremos os referenciais teóricos usados como parâmetros para o desenvolvimento do projeto.

Os temas abordados fazem referência aos elementos que compunham o escopo desenvolvido inicialmente do projeto, iniciando-se com a caracterização da Informação que é componente predominante do tema Transações *Online*, que por sua vez é o assunto principal abordado no projeto. Posteriormente, caracterizaremos as Transações *Online* e sua vulnerabilidade nas redes de *internet* e mencionaremos alguns recursos utilizados na rede para uma maior proteção de dados e/ou informações trafegadas e processadas.

2.1 TRANSAÇÕES E PROCESSAMENTO DE INFORMAÇÕES PELA INTERNET

2.1.1 Informações

Uma informação é um conjunto de dados que foram tratados e organizados, de modo que passam a oferecer um significado ou possuir uma utilidade a alguém.

Para Turban; Rainer; Portter(2007), a informação se refere a dados que foram organizados de modo a terem significado e valor para o receptor.

Veneziano (2009) complementa dizendo que é necessário que ela seja precisa, completa, econômica, flexível, confiável, relevante, simples, pontual, verificável, acessível e segura.

É qualquer recurso informacional, ou seja, tudo que possa gerar ou veicular informação como por exemplo base de dados e banco de dados, bibliografias, dicionários, enciclopédias, feiras, exposições, filmes, vídeos, museus, livros, manuais, dentre outras, conforme Figura 1.

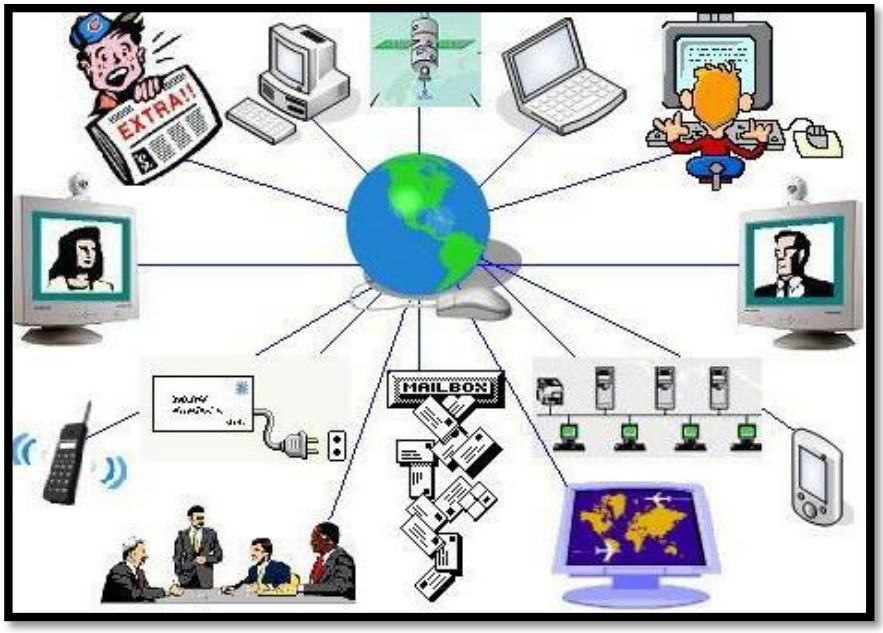
As fontes de informação podem ser divididas em três tipos:

- **Fontes Primárias**: Onde o próprio autor produz ou veicula suas informações. Exemplo: Congressos e Conferências, Legislação, Nomes e Marcas Comercias, Normas Técnicas, Patentes, etc.

- **Fontes Secundárias**: Onde um segundo autor gera ou veicula suas próprias informações a partir de uma informação de outro autor, ou seja, geram informações a partir de fontes primárias. Exemplo: Biografias, Revistas de títulos e de resumos, Bibliografias, Revisão da literatura, Enciclopédias, etc.

- **Fontes Terciárias:** Onde há tanto informações primárias, quanto secundárias. Exemplo: Bibliografia de bibliografia, Diretórios, etc.

Figura 1: Fontes de Informação



Fonte: TAKATA, 2011

Conforme apresentado, informações são dados tratados e organizados, porém não necessariamente uma informação deverá ser considerada verdadeira, isso porque as informações podem ser obtidas através de dados falsos, o que implicará na veracidade da informação.

É imprescindível que ao se obter alguma informação, haja pensamento crítico quanto ao assunto, analisando sua fonte de dados para verificar se a informação é boa(é verdadeira) ou ruim(falsa).

Uma informação boa, é um argumento essencial para a geração de conhecimento sobre um determinado assunto (e posteriormente para um processo de tomada decisão acertada), pois ter a informação certa, no momento certo é fundamental se obter êxito em um negócio, por exemplo. Isso porque quem detém uma informação e é consciente (saber onde e como aplicar), detém o “poder” de ir além, de fazer mais e melhor do que os demais que não possui tal conhecimento, a fim de gerar vantagens sobre os outros.

É importante ressaltar que a informação é apenas um fato isolado quando não se há de fato conhecimento sobre ela. A partir do momento que se tem uma informação concisa sendo transformada em conhecimento, passa a ter um significado mais amplo e agregar valor a quem a detém.

2.1.2 Transações Online

Transações *Online* pode ser classificada como toda operação de envio e recebimento de dados e informações no ambiente da *internet*. Quando nos referimos ao envio e recebimento de dados estamos nos referindo a trafego e processamento dos mesmos.

O processo de Transação *Online* funciona com base em solicitações, onde a partir de um conteúdo disponível e compartilhado em um servidor de *internet*, pessoas de todo o mundo poderá ter acesso a este conteúdo. Quando um computador envia uma solicitação de acesso a uma determinada página(ou informação) na *internet* e há um fornecimento de algum tipo de dado, o processo pode ser considerado como uma Transação *Online*.

Atualmente podemos encontrar as transações na maior parte dos locais na *internet*, isso porque ações como ao acessar um e-mail, acessar uma rede social, um blog, um site dentre outros conteúdos, onde se é solicitado um e-mail, uma senha ou alguma autenticação a rede de *internet* está realizando uma transação desses dados do usuário que solicitou o acesso para o servidor de *internet* a qual os dados estiverem disponibilizados.

2.1.3 Ameaças e Ataques

2.1.3.1 Ameaças

Uma ameaça consiste em uma possível violação de um sistema computacional e pode ser acidental ou intencional. (PINHEIRO, 2008).

2.1.3.2 Ataques

Um ataque ocorre quando uma ameaça intencional é realizada. Os ataques ocorrem por motivos diversos. Variam desde a pura curiosidade, passando pelo interesse em adquirir mais conhecimento até o extremo, envolvendo ganhos financeiros, extorsão, chantagem de algum tipo, espionagem industrial com a venda de informações confidenciais[...](PINHEIRO,2008).

Os ataques pode ser classificados em dois grandes grupos: passivos e ativos.

- **Passivo**: O objetivo do ataque passivo é descobrir ou utilizar informações do sistema, mas sem afetar seus recursos e/ou alterar a mensagem durante a transação.

- **Ativo**: Um ataque ativo tem como objetivo alterar os recursos do sistema ou afetar suas operações, para isso o invasor empenha-se em alterar o conteúdo da mensagem durante a transação.

2.1.4 Segurança da Informação nas Transações Online

Pode-se definir a segurança da informação como a proteção das informações e de seu respectivo sistema computacional contra manipulações não autorizadas,

falhas e desastres, de forma a reduzir a probabilidade de incidentes. (PINHEIRO,2008).

Em outras palavras, podemos dizer que é o processo de proteger as informações de ameaças e possíveis ataques de invasores, e de garantir aos usuários corretos(autorizados) confiabilidade ao realizar transações online, ou seja, é obter privacidade ao realizar alguma operação online.

A Segurança da Informação segue três princípios básicos, o CID, que é responsável pela Confiabilidade, Integridade e Disponibilidade das informações:

- **Confidencialidade**: Visa assegurar que as informações sejam protegidas de qualquer um que não esteja autorizado para acessá-la. Assim, as medidas envolvidas para garantir este princípio, envolverão controle físico e lógico.

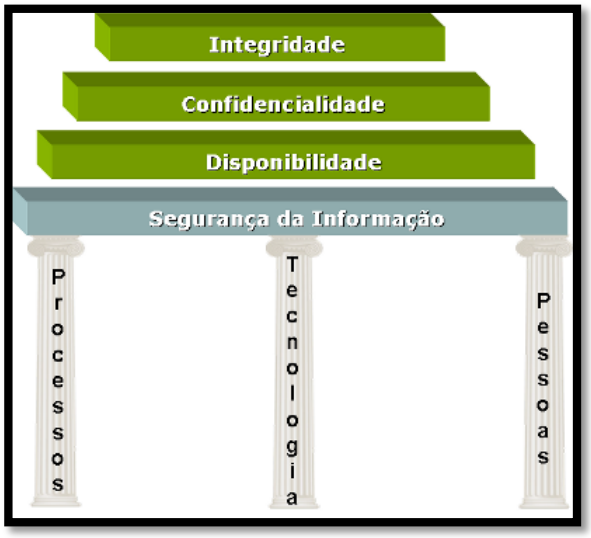
- **Integridade**: Visa assegurar a veracidade de uma mensagem(informação), para que a mesma não seja alterada sem a permissão explícita de seu proprietário.

- **Disponibilidade**: Tem como objetivo garantir que mesmo em situações adversas, o sistema continuará atuando como o esperado e apenas se torne indisponível a partir de autorização do responsável, ou seja, visa assegurar que as informações sempre que solicitadas estarão disponíveis para aqueles que possuem tal permissão.

A Segurança da Informação tem como sustentação o PPT, que são Pessoas, Processos e Tecnologia. Não há como falar em separado de cada item citado, pois, um é totalmente dependente dos demais. Uma empresa deve se munir de profissionais qualificados para criarem (e executarem) bem os processos, além de ter as melhores tecnologias, adequadas a cada caso a qual a segurança está sendo implementada.

A Figura 2 a seguir representa a relação entre os princípios básicos e os elementos de sustentação dos mesmos, ou seja, CID X PPT.

Figura 2: CID x PPT



Fonte: BERNARDI,2013

A Segurança da Informação está fortemente ligada a questões éticas relacionados a crimes contra privacidade de algo/alguém.

Visando o valor da informação no cenário atual é que a segurança das informações trafegadas fica ameaçada.

Crackers em busca de se beneficiar das informações, acabam por burlar muitos dos métodos utilizados na rede de *internet* e apoderam-se dessas informações, por esse motivo é que cada vez mais as empresas vem investindo em novas tecnologias e métodos que possam assegurar o máximo os seus dados que são processados na *internet*.

2.2 RECURSOS UTILIZADOS NA SEGURANÇA DAS TRANSAÇÕES ONLINE

2.2.1 Criptografia

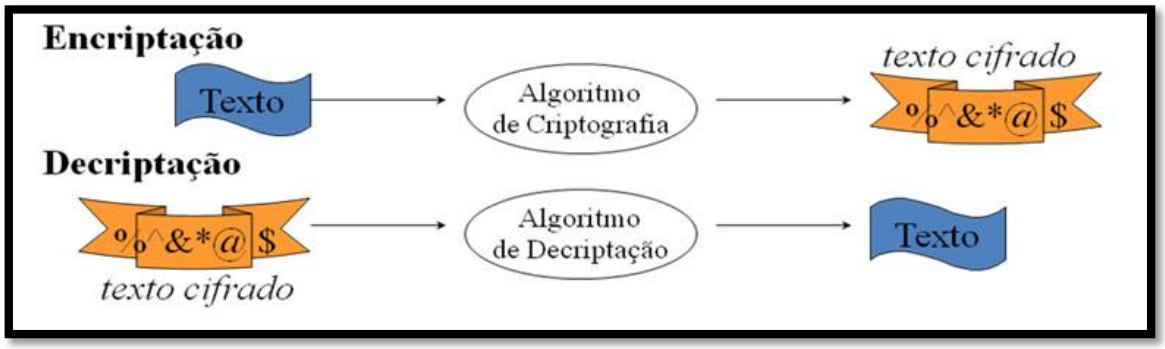
O método de criptografia é comumente usando nas redes e consiste em codificar a informação, assim a mesma passa a ser chamada de texto cifrado. O

processo de codificar ou ocultar os dados é chamado de Encriptação (ou popularmente chamado de Cifragem), e o processo contrário, ou seja, obter a informação original a partir do texto codificado, chama-se Decriptação(ou popularmente chamado de Decrifragem).

A Encriptação e a Decriptação são processos realizados através de programas de computacionais chamados(respectivamente) de cifradores e decifradores. Os programas cifradores ou decifradores, além das informações (que será cifrada ou decifrada), recebem também o número da chave que será usado para definir que ação programa irá realizar, isso porque a cada chave o programa se comportará de uma maneira.

A informação apenas será decifrada se o decifrador possuir a chave correta. Desta forma, para que uma informação seja secreta, é necessário que seja cifrada e que sua chave esteja em sigilo, vide Figura 3.

Figura 3: Processo de Encriptação e Decriptação

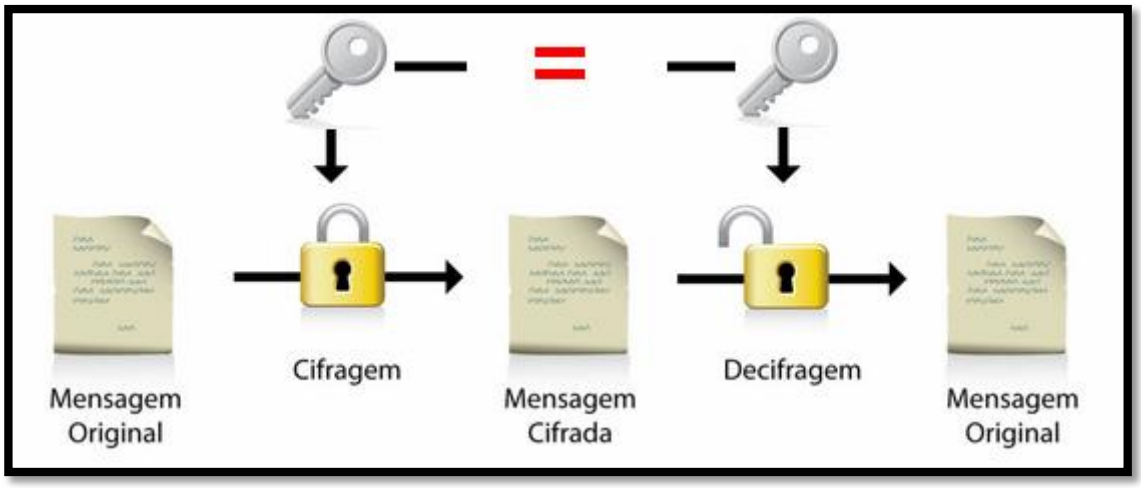


Fonte: PEREIRA e BATISTA, 2013

A criptografia pode ser simétrica ou assimétrica.

- **Simétrica**: A criptografia Chave Simétrica utiliza uma única chave tanto para criptografar quanto para descriptografar os dados. Este tipo de chave é vulnerável, pois pode assegurar sua confidencialidade, mas não a integridade da mesma, isso porque como é utilizado a mesma chave para encriptar e descriptar, um usuário pode facilmente alterar a mensagem, conforme representada pelo fluxograma da Figura 4.

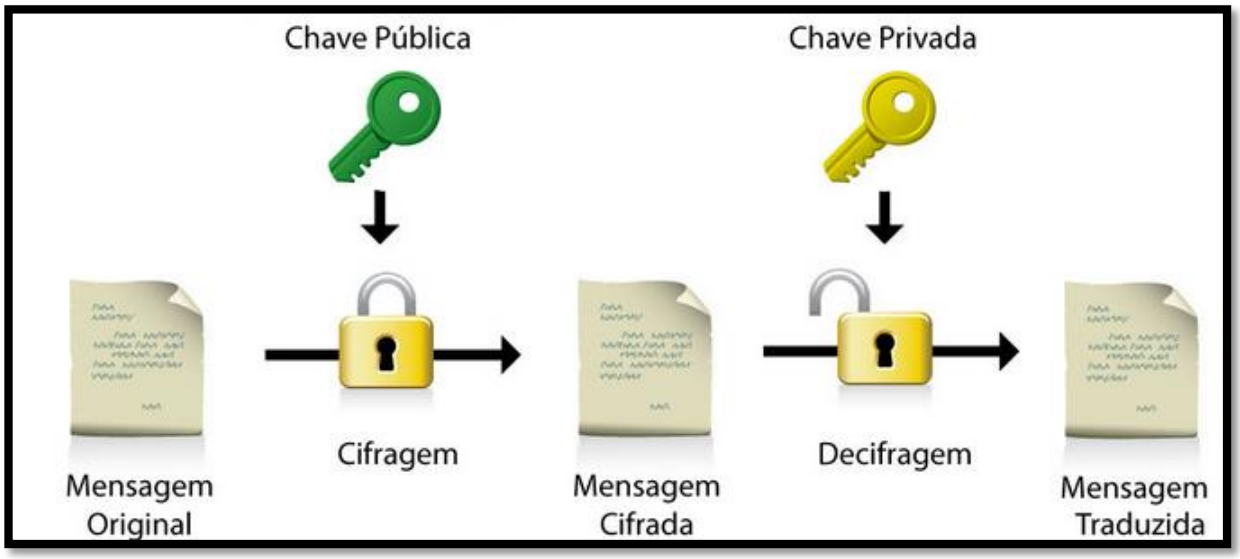
Figura 4: Criptografia Chave Simétrica



Fonte: Adaptado de SOBRAL, 2012

- **Assimétrica**: A criptografia Chave Assimétrica consiste em um método que utilizam uma chave pública e uma chave privada, onde a informação cifrada por uma chave(pública) e é decifrada com outra chave(privada), conforme representada pela Figura 5.

Figura 5: Criptografia Chave Assimétrica



Fonte: Adaptado de SOBRAL, 2012

2.2.2 Autenticação de mensagens

Autenticar uma mensagem significa confirmar sua autenticidade, afirmando que a mesma é verdadeira. A função principal deste recurso, é garantir a segurança das partes que estão realizando a troca de mensagens, para garantirem quem enviou a mensagem e que a mesma não foi alterada durante a transação.

2.2.2.1 Métodos de autenticação

Atualmente existem vários métodos que realizam a autenticação tanto do usuário, quando de programas ou máquinas.

A autenticação de usuário normalmente acontece a partir do acesso de um usuário em um sistema, e sua autenticação pode ser realizada de diversas maneiras, tais como: Login e senha, biometria, cartões numéricos, etc.

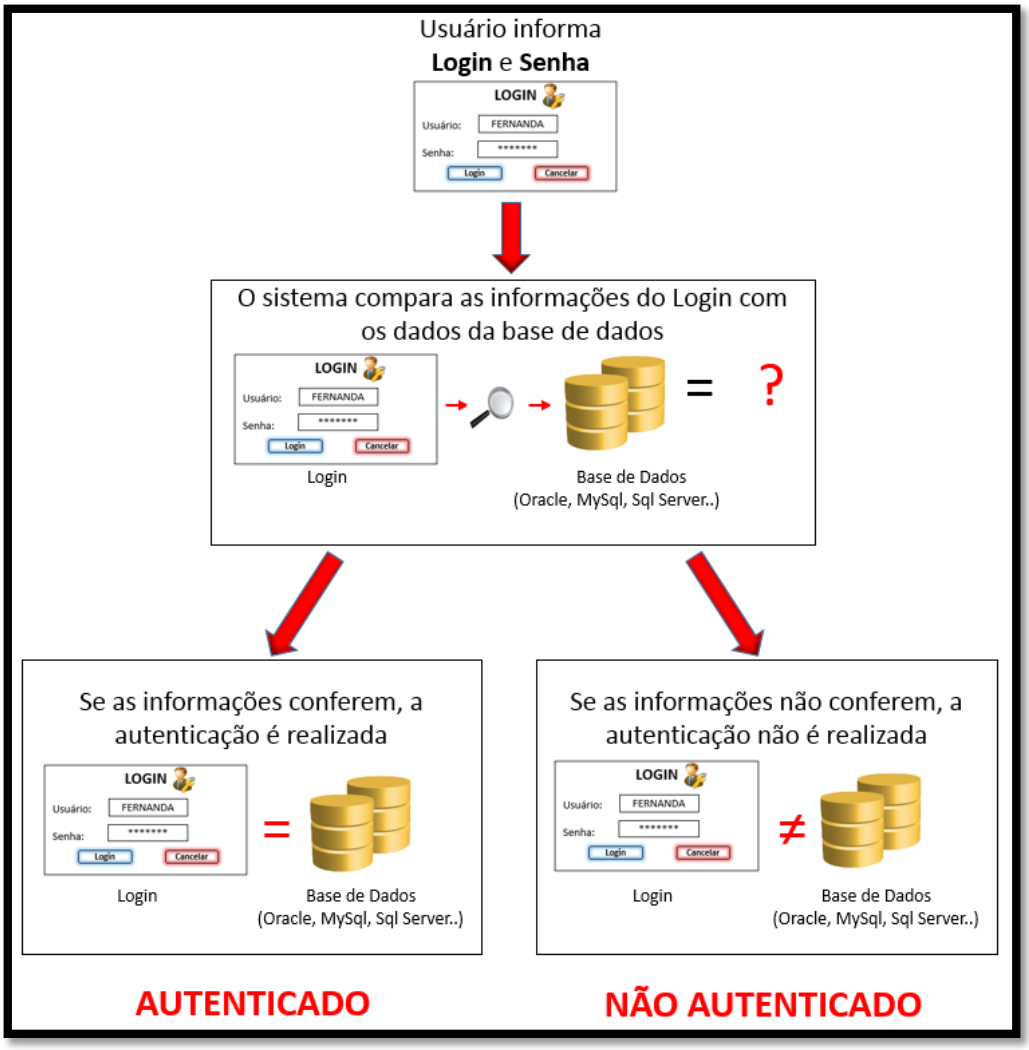
Já a autenticação de programas ou de máquinas, é a rede que se torna responsável por verificar a identidade do programa ou da máquina, exemplo certificados digitais.

A seguir, abordaremos alguns métodos de autenticação mais utilizados atualmente.

- **LOGIN E SENHA**

Neste método o site (ou sistema), solicita o Usuário e a Senha usados pela usuário para acessar o conteúdo disponibilizado para ele. Após ser informado o Usuário e a Senha correspondente, o sistema realiza uma varredura na base de dados e verifica se o usuário está devidamente cadastrado e se a senha informada corresponde a aquele usuário. Se as informações estiverem corretas o usuário terá seu acesso efetivado, caso contrário será barrado e não conseguira acessar conteúdo interno do site/sistema. O fluxo seguido para a autenticação de mensagens através de login e senha é representado pela Figura 6.

Figura 6: Fluxo para validação de Login e Senha



Fonte: A autora

- **BIOMETRIA**

Dispositivos de controles biométricos usam sensores com propósitos especiais para medir e digitalizar um perfil biométrico da voz, digitais e outro traço físico de um indivíduo. O sinal digital é processado e comparado com um perfil processado previamente do indivíduo armazenado em um disco magnético. Se o perfil combina, a pessoa consegue entrar na rede do computador e ter acesso a recursos do sistema de segurança.(MARAKAS; O'BRIEN,2013).

O termo biometria refere-se ao processo de usar características físicas únicas do ser humano para sua identificação. Este método é realizado por meio de sensores biométricos, que fazem a abstração matemática das características únicas de cada

usuário e convertem em padrões, que posteriormente são armazenados (em formato digital) como um dado criptografado.

Para realizar a biometria podemos utilizar as seguintes características:

Veias das mãos – É considerado um dos métodos mais seguros e confiável para o reconhecimento de pessoas, isso porque, além de não ser alterado, realizar a falsificação deste tipo de informação é quase impossível.

Impressão digital – Atualmente é a maneira mais comum de identificação, pois além da rapidez para cadastrar ou validar a impressão digital, este método requer um baixo custo.

Reconhecimento facial – Não é muito utilizado em comparação com outros métodos, como impressão digital (por exemplo), isto porque a aparência é algo que se altera com facilidade, além de os sistema biométricos serem de alto custo.

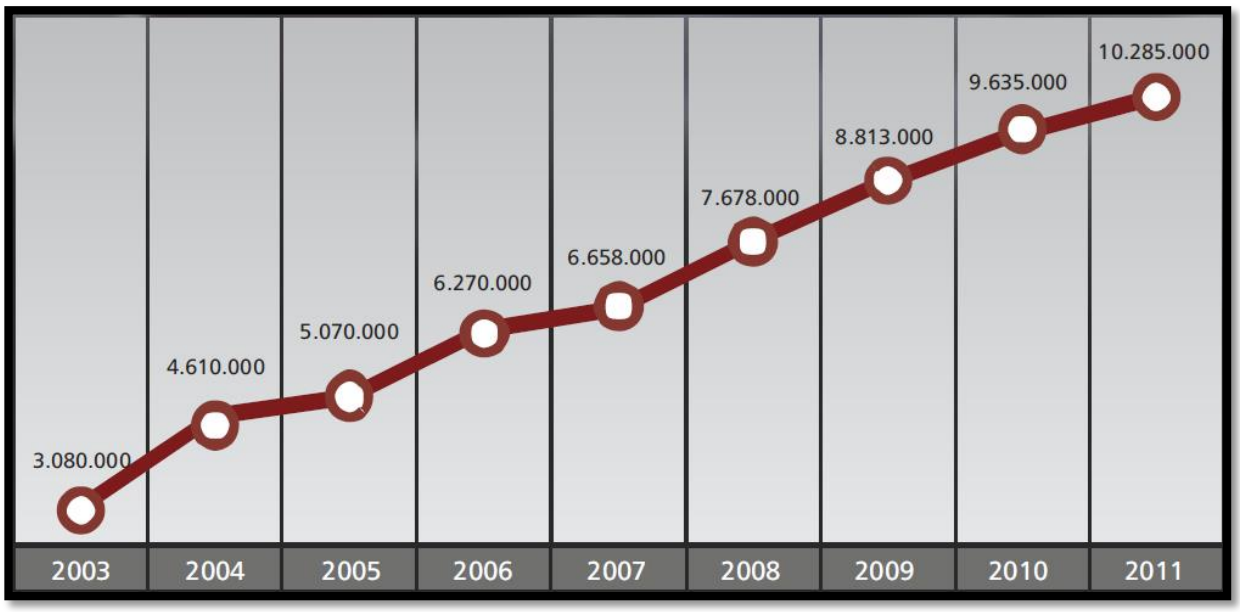
Íris – Apesar de os equipamentos biométricos serem de alto custo para análise, a íris é um método extremamente confiável para identificação de pessoas. Isto porque mesmo ao longo dos anos não se altera e considera-se quase impossível de ser realizada a clonagem.

Voz – Pode ser considerado como de baixa confiabilidade, isto porque a voz de uma pessoa pode se alterar ao longo dos dias. Por exemplo, se uma pessoa estiver doente ou um pouco rouca, o som da sua voz não será “normal”, o que poderá comprometer a sua identificação.

Qualquer sistema biométrico é idealizado para que reconheça e identifique uma pessoa que foi previamente (e devidamente) cadastrada, porém o seu sucesso efetivo dará pela qualidade do sensor – quanto melhor sua qualidade, maior e melhor será a possibilidade de reconhecimento da biometria cadastrada – e também da característica que está analisando (se a mesma não foi alterada desde quando foi cadastrada).

Observe através do Gráfico 1, a evolução do número de registro de Base de Dados Biométricos no Brasil.

Gráfico 1:Número de Registros de Base de Dados Biométricas no Brasil



Fonte: MONTREAL, 2013

- **TOKEN**

São dispositivos físicos (Figura 7) que tem por objetivo gerar senhas temporárias com códigos aleatórios que nunca se repetem, a fim de reforçar a proteção para as contas dos usuários.

Assim como descrevem BURNETT; PAINE(2002), os tokens de autenticação fornecem um meio para autenticar e identificar um usuário final. Em vez de memorizar senhas, os usuários finais protegem sua identidade utilizando um objeto físico que é único para cada usuário.

O token surge como um grande aliado para uma utilização segura de contas bancárias pelo *Internet Bank,* pois como seu código é aleatório, é difícil que criminosos consigam supor qual a próxima sequência válida. Além disso, os códigos exibidos no visor do dispositivo é valido por poucos segundos, pois é pré-estabelecido seu intervalo de tempo para que o código se altere(Exemplo, a cada 10 segundo há troca de códigos), o que dificulta ainda mais a ação de quem deseja burlar esse recurso.

Ao criar um token de autenticação já é possível prever em média sua vida útil, com relação a quantidade de códigos que o dispositivo irá gerar. Isto porque ao criar o dispositivo, é realizado um cálculo- em média- da durabilidade bateria dividido pelo intervalo de tempo que cada código gerado ficará disponível.

Figura 7: Token

Fonte: FONSECA, 2009.

- **CARTÕES NUMÉRICOS**

Assim como o Token, os cartões numéricos(ou cartões de Segurança) são largamente utilizados por bancos com a finalidade de oferecer maior segurança aos usuários do *internet banking*.

Os cartões numéricos são cartões comuns, sem chip, porém no verso contém vários códigos numéricos(em posições diferentes) em posições diferentes(Figura 8). Quando o usuário receber um cartão numérico, o mesmo será relacionado à conta do usuário, assim ao acessar a conta *online* ou realizar alguma transação na conta, o sistema pedira aleatoriamente um código de uma determinada posição e o usuário necessitará informar os algarismos da posição, sem repetir as posições. Após o sistema validar os algarismos informados a ação será realizada e o usuário poderá acessar a conta, por exemplo.

Figura 8: Cartão Numérico

Fonte: SANTANDER, 2013

- **CERTIFICADO DIGITAL**

O Certificado Digital(CD) é o instrumento pelo qual pode-se assinar eletronicamente uma informação. O CD é formado por um conjunto de informações pessoais e pela chave pública do dono do certificado. Esse CD é emitido por uma

Autoridade Certificadora que garante que os dados registrados no certificado são realmente referentes à pessoa que utiliza o certificado (FONTES, 2008).

Através do CD é possível que sistemas de informação realizem confirmação de autenticidade e validações em documentos recebidos eletronicamente, assim asseguram maior privacidade das partes envolvidas (quem envia e quem recebe os documentos) e intensificam a segurança nas transações.

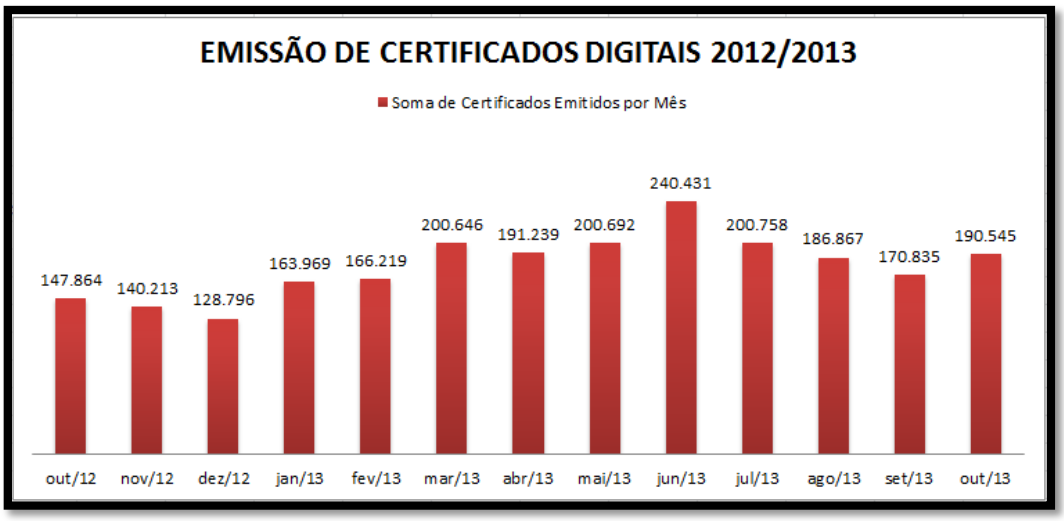
O CD pode ser e-CPF ou e-CNPJ. O e-CPF é utilizado por Pessoas Físicas que necessitam validar transações eletrônicas, como por exemplo: Trabalhadores Autônomos. Já o e-CNPJ é utilizado por Pessoas Jurídicas para validar transações eletrônicas como: Admissão e Demissão de funcionários, recolhimento de FGTS, dentre outros.

Para uma se obter um CD(e-CPF ou e-CNPJ), é necessário realizar uma solicitação junto a uma entidade Autoridade Registro(AR) - adequadamente autorizada pela Receita Federal do Brasil -, que fará a identificação da solicitação, cadastramento dos usuários solicitantes e, posteriormente, dará encaminhamento das solicitações para uma AC.

As instituições de AC, também devidamente autorizadas pela Receita Federal, então farão o processo de emissão, renovação e até mesmo revogação dos certificados expedidos.

Observe através do Gráfico 2, a sazonalidade ocorrida entre Outubro de 2012 e Outubro de 2013 com a emissão de Certificados Digitais.

Gráfico 2:Emissão de Certificados Digitais em 2012 e 2013



Fonte: Adaptado ITI, 2013.

No Brasil, são conhecidos oito tipos de Certificados Digitais, divididos em duas séries, contendo quatro tipos de certificados cada série. Na série A(A1, A2, A3,e A4), são certificados que confirmam, por meio de uma verificação de integridade, uma identidade na web, assinaturas de documentos, transações eletrônicas e/ou online e etc.

Na série S(S1, S2, S3, S4), são certificados que usados para a codificação de documentos, mensagens, bases de dados, dentre outras.

Dos certificados citados, os mais usados são o A1 e o A3. O A1 oferece um nível menor de segurança pois são gerados e posteriormente armazenados na estação do usuário. Já o certificado A3, oferece um nível mais alto de segurança, pois, é gerado e armazenado em um hardware criptográfico a parte, podendo este hardware ser um token ou um cartão inteligente.

Segundo Bolzani (2004), certificado A1 tem validade de um ano e contém um par de chaves públicas e privadas. Certificado A3 oferece maior segurança, pois o par de chaves é gerado em hardware (Cartão Inteligente ou Token) que não permite a exportação ou qualquer outro tipo de reprodução ou cópia da chave privada.

Além da vantagem em relação a maior segurança dos dados transitados, o Certificado Digital oferece também:

- Agilidade nos processos;
- Redução de custos;
- Validade jurídica;
- Assinatura Digital;

2.2.3 Protocolos

2.2.3.1 Protocolos SSL/TLS

O protocolo (Secure Sockets Layer) é uma tecnologia de segurança que usa uma combinação de criptografia de chave pública e chave simétrica utilizada pra codificar os dados trafegados entre computador do usuário e de um website, prevenindo que os dados trafegados possam ser capturados, alterados no curso entre

o navegador e o site ao qual está relacionando, garantindo que as informações sigilosas e confidenciais das transações como do cartão de crédito.

O SSL foi concebido pela necessidade de se ter um recurso tecnológico de segurança que possibilita a garantia absoluta das informações e a garantia de autenticidade dos mesmos nas transações eletrônicas em ambientes virtuais em conexões cliente/servidor, assim evitando que a mensagem (pacote de informações) sejam decifrados.

Atualmente muitos websites fazem uso do SSL apenas em algumas páginas nas quais são transmitidas informações confidenciais, tais como: senhas, códigos privados, números de cartões de crédito, dentre outros.

O TLS e o SSL são muito similares, pois o TLS foi baseado no SSL 3.0 e foi criado como sucessor e ambos se interagem de uma forma sincronizada, sendo que o TLS envia um pacote de informações e o servidor SSL deve responder ele com a mesma mensagem contida no pacote criptografado que foi enviada.

Se tratando de servidores, “open source“ o TLS está substituindo o SSL, porém em aplicações na web utilizando um navegador, o TLS funciona uniteralmente onde somente o servidor é autenticado, porém suporta o modo bilateral de autenticação e é utilizado como maior frequência em configurações de conta de e-mail.

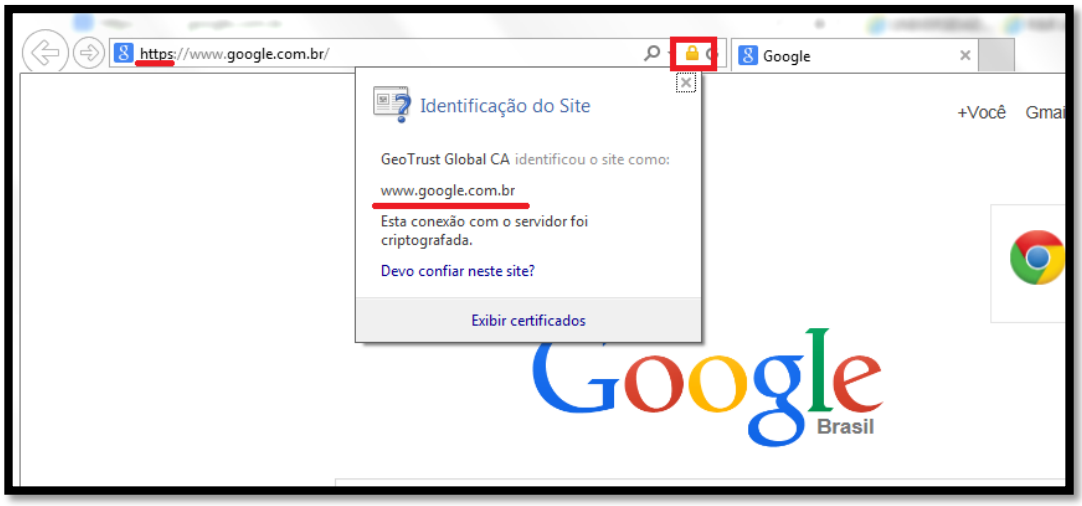
O TLS por sua vez usa um padrão imposto pela FIPS (Information Process Standard) e utiliza uma combinação de algoritmos MD5 e SHA1 para gerar suas chaves, sendo que o SSL não e padronizado pela FIPS e usa somente o padrão MD5 para geração de suas chaves. O protocolo TLS poder ser aplicado tanto para o protocolo HTTP ou HTTPs.

2.2.3.2 Protocolo HTTPS

HTTPS é a combinação/associação dos protocolos HTTP e SSL, mais utilizada atualmente pra trafegar dados de maneira segura para efetuar transações bancárias através da internet, isso porque o este protocolo criptografada os dados que irá trafegar na página.

Quando uma página utiliza o HTTPS, a informação “https://” é exibida no início da URL, para páginas com HTTPS e Certificado Digital(Figura 9), quando não usa na URL é exibido apenas “http://”, sem o “s”.

Figura 9: Página com HTTPS e Certificado Digital



Fonte: Adaptado de GOOGLE, 2013

2.2.4 Firewall

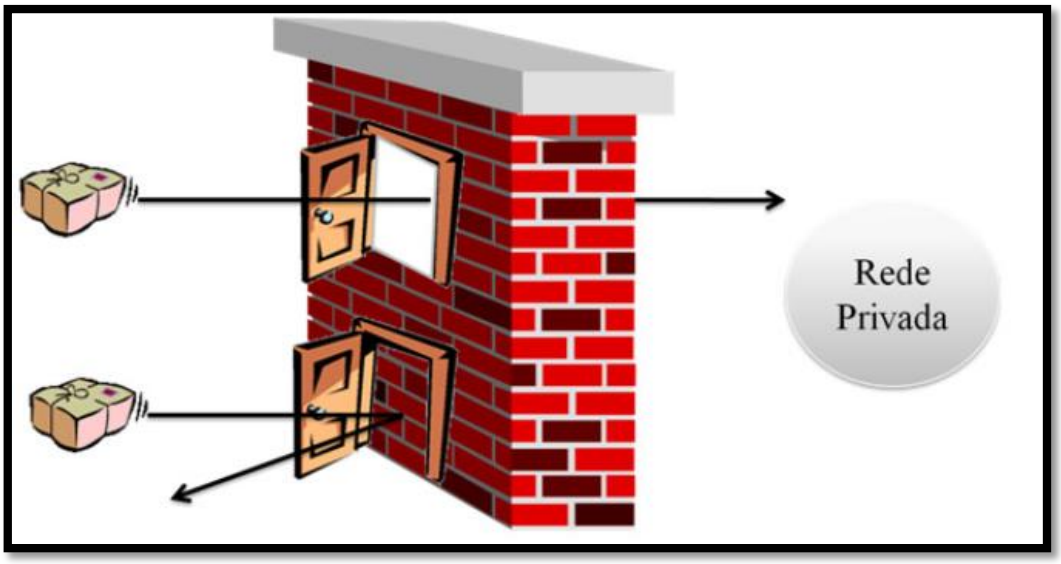
É um dispositivo de defesa composto por um sistema, ou um grupo de sistemas, que reforça o cumprimento de políticas de controle de acesso entre duas ou mais redes, permitindo somente tráfego de informações autorizadas.(FINKELSTEIN, 2011).

Um firewall é um hardware e/ou software que protege uma rede privadas por meio da análise das informações que entram e saem da rede. Os firewalls analisam cada mensagem que tenta entrar na rede. A não ser que a mensagem tenha as marcações corretas, eles a impedem de entrar. Os firewalls podem detectar, atém mesmo, computadores que se comunicam com a internet sem aprovação. (BALTZAN; PHILLIPS, 2012)

O firewall serve como barreira para a comunicação de duas redes, pois, através de uma política de acesso, controla o tráfego de pacotes entre as mesmas. Isso porque todo o conteúdo direcionado a rede passa primeiro pelo firewall e depois (se autorizado) é encaminhado a.

Em uma analogia simples, podemos dizer que o firewall tem "portas", das quais seleciona o conteúdo que pode ou não entrar em cada porta da rede a qual foi instalado, como por exemplo um computador (ou uma rede deles), um roteador e etc., conforme Figura 10.

Figura 10: Ilustração da funcionalidade do Firewall



Fonte: PEREIRA e BATISTA, 2013

2.2.4.1 Vantagens e desvantagens

A utilização do firewall em uma rede, como praticamente tudo, tem suas vantagens e desvantagens.

Vantagens:

-Facilidade de gerenciamento da segurança e localização de problemas (quando houver), pois oferece apenas um ponto de acesso à rede.

-Apenas o tráfego que foi autorizado na política de acesso (e segurança) é permitido adentrar na rede.

Desvantagens:

-Maior vulnerabilidade da rede, pois a violação de um *firewall* afeta e prejudica a rede toda.

-Impossibilidade de controlar situações como vírus de e-mail ou tentativas de *phishing*, pois, na abertura de um e-mail o firewall não consegue determinar o conteúdo das mensagens trafegadas. Já na tentativa de *phishing*, onde o usuário é induzido a informar algo pessoal ou informações financeiras em sites aparentemente confiável, mas que na realidade são fraudulentos, não é possível muitas vezes determinar a autenticidade de um site.

2.2.5 VPN

VPN (*Virtual Private Network* ou Rede virtual Privada), como próprio nome já diz, é uma rede privada de computadores que por meio da internet (rede pública), “faz” com que os dados sejam criptografados e trafeguem por meio de túnel denominados tunelamento, assim diminui-se o risco de interceptação das informações e garante-se maior segurança aos dados trafegados, pois é criado um protocolo de internet (IP), onde o mesmo é protegido pela empresa ao qual oferece o serviço de VPN.

FINKELSTEIN(2011), define a VPN como a tecnologia que permite a troca segura de informações por meio de redes públicas, utilizando criptografia, criando um túnel seguro.

2.2.5.1 Aplicações e benefícios

Sua aplicabilidade está voltada para empresas, pois garante que as informações estejam integradas em tempo real com uma velocidade superior as conexões tradicionais, compartilhando o acesso à banco de dados para a empresa e conectividade com os parceiros, fornecedores, distribuidores, clientes e usuários.

Dentre as inúmeras vantagens (benefícios) podemos destacar as seguintes:

Segurança: Ponto crucial da tecnologia, pois permite que os dados privados sejam trafegados pela rede pública, porem protegidos não sendo possível ser modificados ou interceptados;

Redução de custos: coma VPN há uma unificação da rede, garantindo um desempenho alto e agilidade nas integrações dos dados e comunicação de voz e multimídia entre a rede;

Help desk: Facilidade e agilidade no suporte on line.

2.2.6 Moeda virtual: Bitcoin

São moedas digitais baseadas em criptografia, que podem ser enviadas e recebidas pela internet.

Moeda virtual com base em criptografia, não vinculadas a governos e/ou bancos, criada por Satoshi Nakamoto, especificado pelo seu pseudônimo, sendo a primeira moeda digital descentralizada, sendo utilizada para compras de bens materiais, eletrônicos através da internet.

O diferencial do bitcoin em relação as moedas reais, é o anonimato dos operadores, pois não há uma entidade reguladora que intermediam as transações, pois a moeda não existe fisicamente e sim um código alfanumérico entre os negociadores.

2.2.6.1 Funcionamento do Bitcoin

Seu funcionamento se dá em rede de dados ponto-a-ponto, denominado P2P, e seu protocolo tem código aberto e descentralizado, onde uma parte dos dados das transações ficam armazenados em cada computador que faz parte da rede.

Os Bitcoins são gerados através de aplicativos, que após várias tentativas e erro, quebram chaves criptográficas dos bancos de dados de transações que tem sua composição por uma série de blocos encadeados, criam um novo bloco de transações, denominando assim este processo como mineração de Bitcoins, onde o sistema libera novas moedas ao qual são distribuídas para os computadores que emprestaram seu poder de processamento para quebrar a chave criptográfica.

Para se tornar um minerador de Bitcoins, é necessário ter um computador com conexão com a internet, um aplicativo para minerar os Bitcoin e uma carteira virtual.

.

2.2.6.2 Vantagens e desvantagens

As vantagens da moeda virtual, é que as transações são mais transparentes, rápidas, anônimas e possuem poucas taxas, além do mais todas as transações são registradas, rastreadas e vistas por qualquer pessoa no mundo por meio do Block Explorer.

As desvantagens são as seguintes: alta variação do valor e a garantia do seu valor, pois a moeda não tem lastro; a dificuldade em manipular as transações para os usuários comuns; a vulnerabilidade perante à segurança das informações e poucos estabelecimentos que aceitam a moedas em suas negociações

2.2.6.3 Estratégia para atingir o mercado físico

No intuito de impulsionar suas vendas, alguns varejistas adotaram como estratégia a oferecer incentivos e fidelizar os consumidores oferecendo moedas virtuais, incentivando os mesmos a visitarem suas lojas.

Ao instalar o aplicativo disponibilizado pelo estabelecimento nos smartphones, *tablets* o mesmo é estimulado à visitar a loja e interagir o aplicativo instalado em seu aparelho com um hardware onde serão creditados as moedas virtuais que poderão serem acumulados e trocados por ingressos de cinemas, créditos de celulares pré-pago e vales presentes por empresas participantes do programa.

3 ESTUDO DE CASO: USO DE CARTÃO DE CRÉDITO PARA PAGAMENTO EM UMA TRANSAÇÃO E-COMMERCE

3.1 E-COMMERCE

Comércio eletrônico (e-commerce) é uma modalidade de comércio realizada pela internet, onde há transações financeiras são efetuadas por meios de mecanismos eletrônicos, como computadores, celulares e/ou outros dispositivos de comunicação. Desta forma os consumidores tem a comodidade de adquirir produtos/serviços sem sair de casa.

3.2 FORMAS DE PAGAMENTO ONLINE

Uma questão de extrema importância para as lojas de e-commerce é escolher as formas de pagamento que irão disponibilizar ao consumidor. As requisições são inúmeras, dentre elas podemos citar seja simples, rápida e segura.

Abaixo segue algumas formas de pagamento mais usadas:

Boleto Bancário: O comprador imprime boleto no final da compra e paga no banco de sua preferência ou através do Internet Banking.

O boleto bancário atualmente ainda é um forma de pagamento muito usada em compras online, pois, apesar da popularização dos cartões de crédito, nem todos os compradores possuem este recurso, ou, até mesmo, por receio de usar os cartões e o site não ser seguro.

Cartões de Crédito: Nesta opção de pagamento, o usuário/comprador tem que informar o número do cartão de crédito e o código de segurança, que o mesmo possui, ao site. A compra fica sujeita à aprovação até que se é comprado que há créditos disponíveis para realizar tal operação.

Intermediadores: Intermediadores são empresas que fornecem serviços de recebimento de pagamento de compradores, mediante a uma taxa pelos serviços de recebimento prestado. Funciona da seguinte maneira, um comprador pode se cadastrar em um site de um intermediador e fornecer todos os seus dados. Ao realizar uma compra em um determinado site e escolher a opção de pagamento de um intermediador, o comprador tem a possibilidade de escolher uma forma de pagamento que o site não fornece. Exemplo: Se o site aceita apenas pagamento por cartão de crédito e o intermediador aceita além de cartões de crédito, mas também transferências bancárias e boletos bancários, o comprador pode optar pelas demais opções, entretanto negociará o pagamento com o intermediador e não mais com o site.

Alguns dos intermediadores mais conhecidos são: *PagSeguro*, Mercado Pago, *PayPal* e etc.

Débito Online: Esta forma de pagamento surge para substituir os boletos bancários, porém na realidade esta forma de pagamento é realizada uma transferência entre contas. Saindo da conta do comprador e vai para a conta da loja em pouco tempo.

3.3 MASTERCARD: POLÍTICA DE CONFORMIDADES

Como forma de assegurar maior privacidade e segurança às informações, a Mastercard tem o programa PCI, que é um padrão de segurança para indústrias de cartões criado para auxiliar bancos e parceiros (estabelecimentos/usuários finais) a proteger suas informações durante o processo de pagamento e transação dos dados.

É disponibilizado pela Mastercard disponibiliza aos seus parceiros(estabelecimentos) os padrões necessários para a parceria, se o mesmo não atingir os padrões de segurança, conforme o PCI determina, a Mastercard se reserva o direito de cobrar uma taxa de não-conformidade.

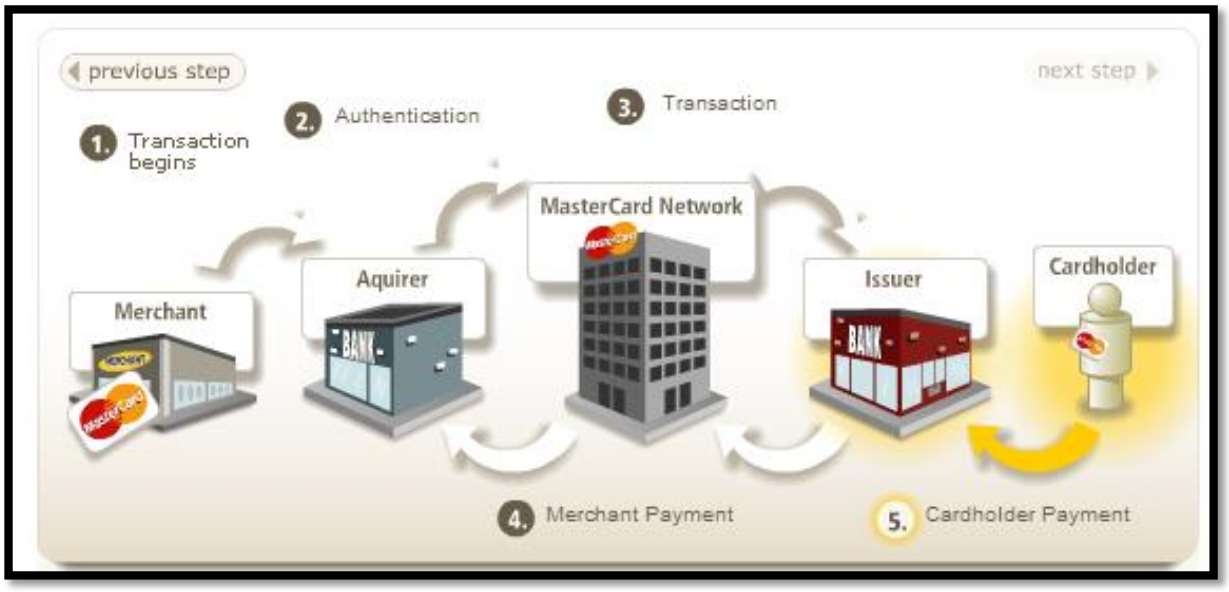
Na realidade, o programa tem como meta a proteção efetiva de todos os participantes do PCI, desde Mastercard, bancos, estabelecimentos e até mesmo usuário final, e quando não há conformidade em alguém item pré determinado, toda a segurança almejada é colocada em risco.

Com relação às transações online, para procedimentos realizado via internet, a Mastercard dispõe de um rigoroso processo de criptografia das informações. Onde, através das mais atuais e seguras tecnologias, oferecem maior segurança para os dados trafegados.

3.4 COMO OCORREM TRANSAÇÕES AO REALIZAR UM PAGAMENTO COM CARTÃO DE CRÉDITO

Ao realizar um pagamento por meio de cartões de crédito, do início da solicitação até a efetivação do pagamento, é realizado um processo complexo de validações nas transações, conforme Figura 11.

Figura 11: Demonstrativo dos processos realizados em uma compra online

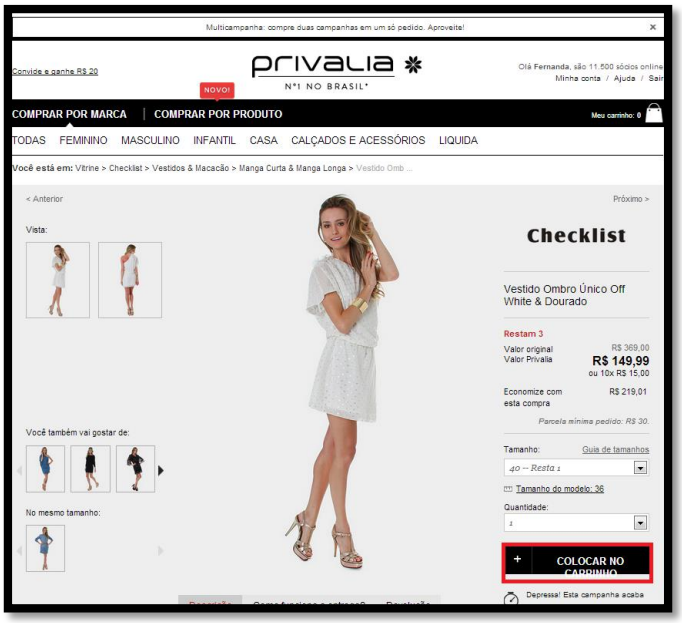


Fonte: MASTERCARD, 2013

1º A Transação se inicia

A transação se inicia quando o usuário decide comprar um produto, assim como exemplificado na Figura 12.

Figura 12: Colocando o produto no carrinho de compras

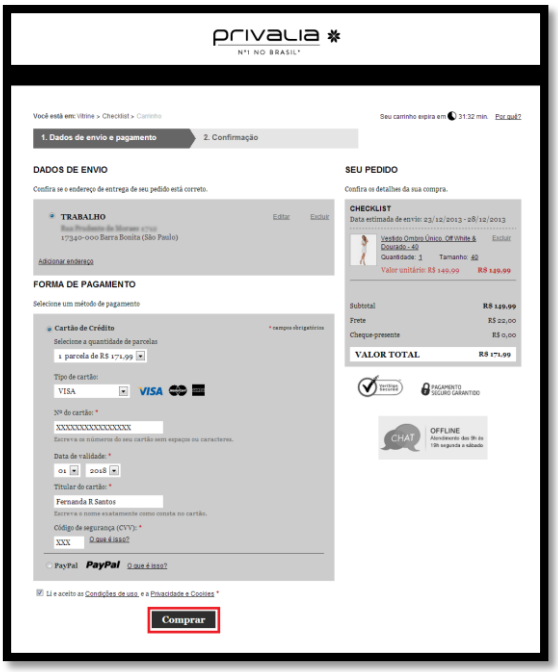


Fonte: Adaptado de PRIVALIA, 2013

O titular do cartão adquire um bem (produto/serviço) de algum comércio e usa o cartão de crédito como forma de pagamento. Os dados (número de segurança e/ou senha do cartão) são enviados criptografados do terminal (estabelecimento a qual está sendo realizado a compra) para o banco Adquirente[1].(Figura 13)

[1] Membros licenciados pela MasterCard que é responsável por analisar e, posteriormente, aceitar(ou não) estabelecimentos em seu programa de cartões e processos relacionados a transações financeiras.

Figura 13: Preenchendo os dados pessoais para a confirmação da compra



Fonte: Adaptado de PRIVALIA, 2013

2º Autenticação

Ao receber a solicitação de uso do crédito do titular do cartão, o Adquirente descriptografa as informações e realiza a validação das mesmas. Validada as informações, é feita verificado a viabilidade da compra(se tem saldo e se a mesma pode ser realizada) junto a Credenciadora.

Se a compra for aprovada(valor, parcelas e condições), a informação virá até o terminal do estabelecimento a qual foi solicitada a compra e o titular conseguirá adquirir o produto(Figura 14).

Figura 14: Confirmação da compra

Fonte: Adaptado de PRIVALIA, 2013

Após a compra ser finalizada, se a compra for realizada pela internet a maior parte das empresas disponibilizam uma página para acompanhamento do pedido. (Figura 15).

Figura 15: Acompanhamento do status do produto

Fonte: Adaptado de PRIVALIA, 2013

3º Transação Aprovada

O Adquirente envia, por meio da MasterCard, a transação para o banco Emissor[2].

[2] É a instituição financeira do titular do cartão, ou seja, o banco que forneceu o cartão ao titular.

4º Pagamento para a credenciadora

O Emissor realiza o pagamento da comprar realizada para o Adquirente, porém desconta a taxa pelo sistema de solução MasterCard, como uma comissão pelo serviço prestado.

5º Pagamento da Fatura

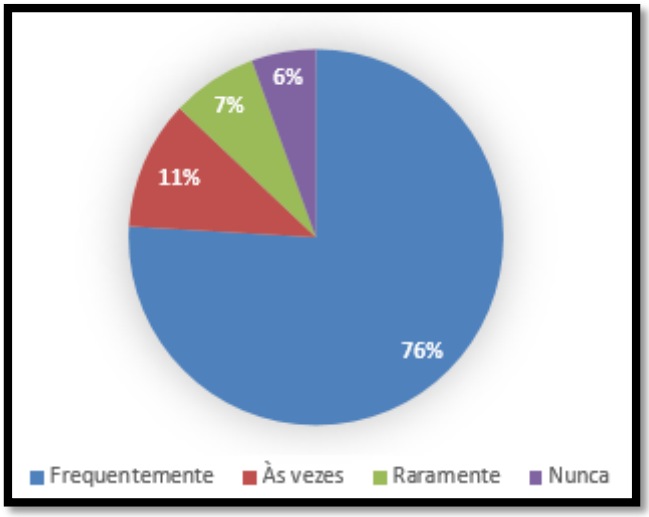
Ao final, o titular do cartão realiza o pagamento da fatura, contendo os bens e/ou serviços adquiridos de comerciantes, para o banco Emissor.

4 PESQUISA DE OPINIÃO PÚBLICA

Como intuito de conhecer a opinião dos usuário da internet, sobre o uso e frequência deste meio de comunicação, foi realizada uma pesquisa de mercado em Dezembro de 2013(com 54 pessoas), na qual foram abordados assuntos como grau de confiança em informar dados pessoais em páginas da internet, uso do cartão de crédito na rede e cuidados tomados no momento de realizar um acesso a uma rede de internet.

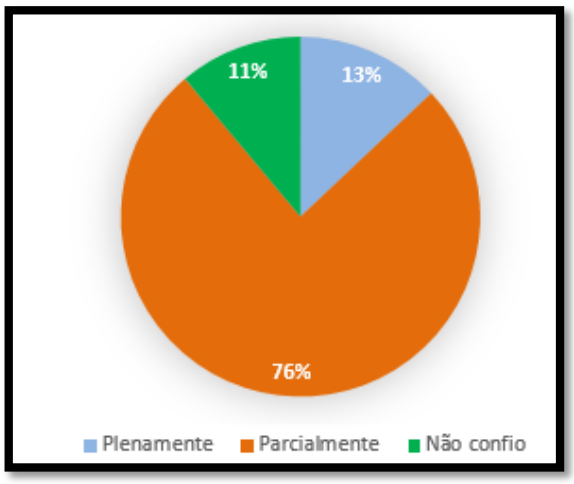
Ao questionar se os internautas verificam a veracidade de um sites antes de criar um perfil/usuário e inserir dados pessoais, 76% informaram que realizam a verificação Frequentemente, conforme Gráfico 3.

Gráfico 3: Preocupação com autenticidade de um site



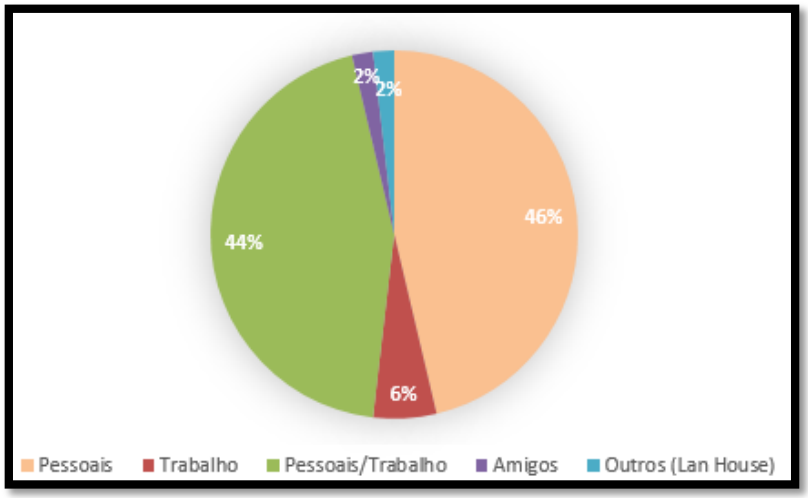
Quando questionado aos usuário sobre a confiança depositada ao informar/inserir informações pessoais em páginas da internet, 76% das pessoas informaram confiam Parcialmente, assim como representando no Gráfico 4.

Gráfico 4: Nível de confiança ao inserir dados pessoais em sites da internet



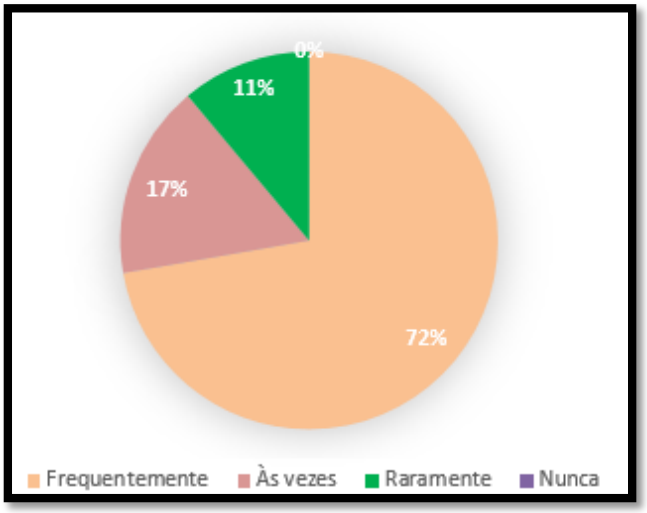
Com relação aos equipamentos usados para realizar acesso à internet, 46% informaram que realizam acesso apenas através de equipamentos Pessoais. Contudo, 44% das pessoas informaram que seus acessos na rede são por meio de equipamentos Pessoais e de Trabalho, conforme demonstrado no Gráfico 5.

Gráfico 5: Meios de acesso à internet



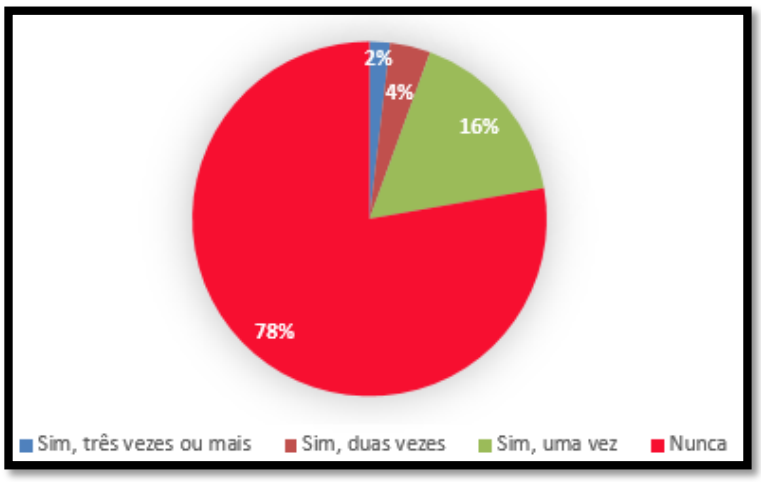
Com relação a atualização do Sistema Operacional e softwares como Antivírus atualizados, 72% das pessoas informaram que fazem a atualização Frequentemente (Gráfico 6).

Gráfico 6: Preocupação com atualizações do SO e antivírus



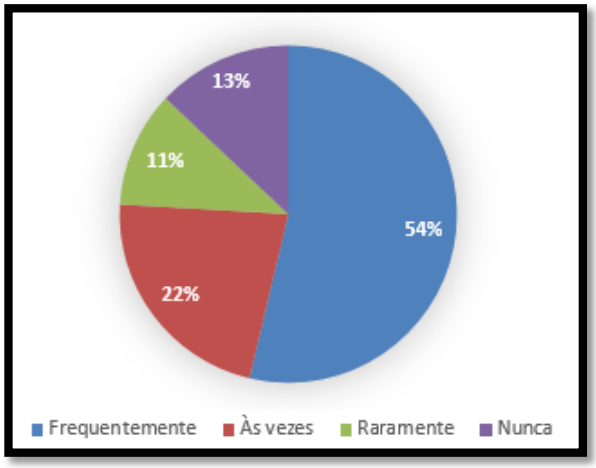
Quando questionado sobre ser alvos de ataques/invasões na internet (Ex: perfil de rede social ou e-mail hackeado), 78% das pessoas informaram que Nunca foram alvo de invasores(Gráfico 7).

Gráfico 7: Índice de ataques sofridos na internet



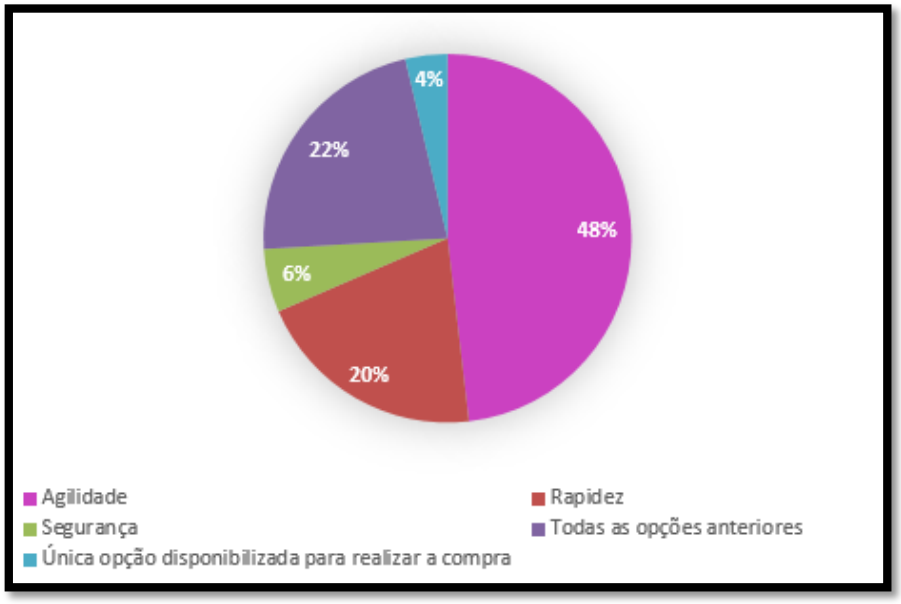
Sobre o uso de cartões de crédito para realizar transações na internet, 54% informaram que utilizam cartões Frequentemente, assim como representado pelo Gráfico 8.

Gráfico 8: Frequência de uso do Cartão de Crédito na internet



Quando indagado aos usuário de cartão de crédito, sobre o motivo que os levaram a escolher este meio para pagamento, 46% das pessoas informaram que o uso era devido a Agilidade que o mesmo oferece (Gráfico 9).

Gráfico 9: Razão pela qual faz uso do Cartão



CONCLUSÃO

Com base nas pesquisa realizadas e no conhecimento adquirido ao longo deste projeto, conclui-se que:

Como toda operação realizada pela *internet* tem os seus ricos, e alguns perceptivos, é claro que, grande parte da população ainda tem receio de fornecerem dados pessoais em web sites e até mesmo dados de cartões de créditos. A insegurança que prevalece sobre o pensamento do usuário, é um dos grandes desafios que as instituições precisam vencer para alavancar as transações *online* para assim acompanhar o crescimento de atividades que são realizadas. Muitos riscos são percebidos, ao efetuar qualquer envio de informação para um destino conhecido ou desconhecido e não ter a certeza de que as mesmas são de fato verdadeiras. Para isso foram criadas tecnologias inovadoras para assim interligar um canal de segurança entre o remetente e o receptor.

Contudo, o maior desafio das instituições atualmente é garantir a segurança das informações. Neste caso, é imprescindível a utilização de mecanismos de segurança para manter a integridade dos dados(próprios) e das organizações relacionadas, pois necessitam de políticas e sistemas de segurança para obter uma gestão satisfatória.

Deve-se ter consciência de que o elo mais fraco no processo de envio e recebimento de dados na internet são as pessoas. Assim como há inúmeras empresas em busca de melhorar a segurança e garantir maior integridade para os dados trafegados, há várias outras pessoas interessadas em fazer mal uso do conteúdo trafegado na rede.

REFERÊNCIAS

ARAÚJO, Márcio Tadeu; FERREIRA, Fernando Nicolau Freitas. **Política de Segurança da Informação: Guia Prático para Elaboração e Implementação**. 2ª Ed. Rio de Janeiro. Editora Ciência Moderna, 2008.

Arte de Pesquisar. **Fontes de Informação**. Disponível em: http://artedepesquisar.blogspot.com.br/2009/05/fontes-de-informacao.html, 06 de Maio 2009. Acessado em: Outubro/2013.

BALTZAN, Paige; PHILLIPS, Amy. **Sistemas de Informação**. Porto Alegre. Bookman, 2012.

BERNARDI, Fábio. **Segurança da Informação - Conscientização**, 2013. Disponível em: http://www.bluminformatica.com.br/SegurancadaInformacaoConscientizacao.html. Acessado em: Outubro/2013.

Blog do Professor José Artur Teixeira Gonçalves.**Como fazer uma monografia**. Disponível em: http://metodologiadapesquisa.blogspot.com.br/2008/11/objetivos-gerais-e-especficos.html, 11 de Novembro 2008. Acesso em: maio/2013.

BOLZANI, C. A. M. **Residências Inteligentes: Redes de Dados, Computação Pervasiva, Automação residenciais**. 1º Ed. São Paulo. 2004.

BURNETT, Steve; PAINE, Stephen. **Criptografia e Segurança: O Guia Oficial RSA**. Rio de Janeiro. Campus, 2002.

CARLSON, Jacob; GREEN, Ken; SCHETINA, Erik. **Sites Seguros: Aprenda a desenvolver e construir**. Rio de Janeiro: Campus, 2002.

Central de Proteção e Segurança. 6 regras para transações financeiras *online* mais seguras, 2012. Disponível em: http://www.microsoft.com/pt-br/security/online-privacy/finances-rules.aspx, Acessado em: Junho/2013.

eDestinos. **Segurança nas Transações**, 2012. Disponível em: http://www.edestinos.com.br/seguranca. Acessado em: Maio/2013.

FECOMERCIOSP. **Evolução dos meios de pagamento no Brasil**, 2013. Disponível em: http://www.fecomercio.com.br/blog/2013/09/17/evolucao-dos-meios-de-pagamento-no-brasil/. Acessado em: Agosto/2013.

FINKELSTEIN, Maria Eugênia. **Direito do Comércio Eletrônico**. 2ª Ed. Rio de Janeiro: Campus, 2011.

FONSECA, Willian. **O que é token?** 2009. Disponível em: http://www.tecmundo.com.br/senha/3077-o-que-e-token-.htm. Acessado em: Setembro/2013.

FONTES, Edison. **Praticando a Segurança da Informação: Orientações práticas alinhadas com Norma NBR ISSO/IEC 27002 – Norma NBR ISSO/IEC 27001 – Norma NBR 15999-1 – COBIT – ITIL**. Rio de Janeiro: Brasport, 2008.

GOOGLE, 2013. Disponível em: https://www.google.com.br/. Acessado em: Setembro/2013.

HAMANN, Renan. **Como funciona o cartão de crédito - Entenda quais são as tecnologias empregadas nos pagamentos realizados com cartões de crédito**, 2011. Disponível em: http://www.tecmundo.com.br/infografico/8058-como-funciona-o-cartao-de-credito.htm. Acessado em: Outubro/2013

Informação em Mídias Digitais?. Convergência das mídias, cultural e informacional. Disponível em: http://infmdiasdigitais.blogspot.com.br/2011/07/convergencia-das-midias-cultural-e.html, 03 de Julho de 2011. Acessado em Outubro/2013.

Instituto Nacional de Tecnologia da Informação. **Certificado Digital**. Disponível em: http://www.iti.gov.br/certificacao-digital. Acessado em: Outubro de 2013.

ITI. **Certificado Digital**, 2013. Disponível em: http://www.iti.gov.br/certificacao-digital. Acessado em: Outubri/2013.

MARAKAS, George M.; O'BRIEN, James A. **Administração de Sistemas de Informação**. Porto Alegre. Bookman, 2013.

MASTERCARD. **Como funciona a MasterCard - Compreendendo o processe de transação e como você se encaixa**, 2013. Disponível em:

http://www.mastercard.com/br/merchant/pt/how_works/index.html. Acessado em: Agosto/2013.

MONTREAL. Biometria - **A Montreal está no topo do segmento no Brasil**, 2013. Disponível em: http://www.montreal.com.br/HttpHandlers/FileHandler.ashx?id=17&menuid=37. Acessado em: Novembro/2013.

NAKAMURA, E; GEUS, P. L. **Segurança em redes em ambientes cooperativos**. Rio de Janeiro : Editora Novatec , 2007 .

Oficio Eletrônico. **Cartilha de Certificação Digital**, 2012. Disponível em: https://www.oficioeletronico.com.br/Downloads/CartilhaCertificacaoDigital.pdf. Acessado em Junho/2013.

OLHAR DIGITAL. **Método de criptografia usado mundialmente apresenta falha**. Disponível em: http://olhardigital.uol.com.br/produtos/seguranca/noticias/metodo-de-criptografia-usado-mundialmente-apresenta-falha,-segundo-pesquisa, 15 de Fevereiro de 2012. Acessado em: Junho/2013.

PEREIRA, Lucas; BATISTA, Thais. **Segurança em Redes de Computadores. Aula 2 - Introdução aos Mecanismos de Defesa**, 2013. Disponível em: http://www.metropoledigital.ufrn.br/aulas_avancado/web/disciplinas/seg_redes/aula_02.html. Acessado em: Novembro/2013.

PINHEIRO, José Maurício. **Biometria nos Sistemas Computacionais Você é a Senha**. Rio de Janeiro. Editora Ciência Moderna, 2008.

POTTER, Richard E; RAINER, R. Kelly; TURBAN, Efraim. **Introdução a Sistemas de Informação: Uma abordagem Gerencial**. Rio de Janeiro: Campus, 2007.

SATANDER. **O que fazemos por sua segurança - Cartões de Segurança On-line**, 2013. Disponível em: http://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=6736. Acessado em: Setembro/2013.

SCHNEIER, Bruce. **Segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2008.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e práticas**. São Paulo. Pearson, 2008.

SOBRAL, Fábio. **Certificação Digital**, 2012. Disponível em: http://biblioo.info/certificacao-digital/. Acessado em: Novembro/2013.

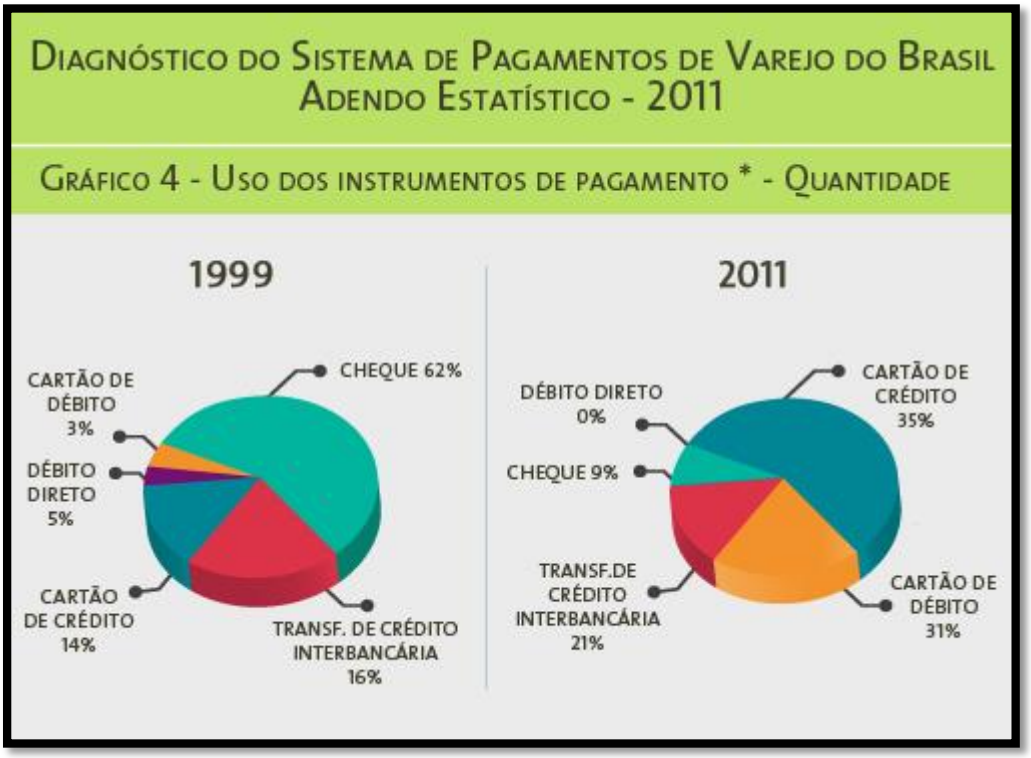
TAKATA, Roberto. **Quanta informação aqui, lá, em todo lugar?** 2011. Disponível em:http://quipronat.wordpress.com/2011/02/16/quanta-informacao-aqui-la-em-todo-lugar. Acessado em: Outubro 2013

Tec Mundo. **O que é token**, 2009. Disponível em: http://www.tecmundo.com.br/senha/3077-o-que-e-token-.htm. Acessado em: Junho/2013

VENEZIANO, Wilson Henrique. **Organizações e Sistemas de Informação**. Brasília: Desenvolvido em Atendimento Ao Plano de Trabalho do Programa de Formação de Especialistas Para A Elaboração da Metodologia Brasileira de Gestão de Segurança da Informação e Comunicações – Cegsic 2009-2011.

ANEXO I: DIAGNÓTICO DO SISTEMA DE PAGAMENTOS DE VEREJO NO BRASIL SOBRE OS INSTRUMENTOS DE PAGAMENTOS USADOS DESDE 1999 ATÉ 2011.

Gráfico 10: Diagnóstico do Sistema de Pagamento de Verejo do Brasil. Adendo Estático - 2011



Fonte: FECOMERCIOSP, 2013

ANEXO II: O QUE SIGNIFICA OS DADOS CONTIDOS NO CARTÃO DE CRÉDITO

Figura 16: Significado dos itens que são apresentados em Cartão de Crédito

Fonte: HAMANN, 2011