5CONTECSI June 04 - 06, 2008 São Paulo, Brazil

5th International Conference on Information Systems and Technology Management
5º Congresso Internacional de Gestão da Tecnologia e Sistema de Informação
De 04 a 06 de Junho de 2008 - São Paulo - Brasil

PS-910

RISK PERCEPTION IN INFORMATION SECURITY ON E-COMMERCE TRANSACTIONS: A STRATEGIC APPROACH

Fabiano Ribeiro Lima (Federal University of Lavras, MG, Brazil) – frlimabh@gmail.com
Pedro Calixto Alves de Lima (Federal University of Lavras, MG, Brazil) – pedrocalixto@hotmail.com

This work approaches aspects of safety in the transactions made through Internet, as well the tools more used by the sites of e-commerce to guarantee your own safety, as well as the one of your customers. It treats of aspects considered important, of the users' of e-commerce point of view, in the moment of deciding for using or not the Internet to make a purchase. An exploratory research was accomplished through questionnaire on the risks found in the purchases accomplished by the internet, 71 people that work in a company of Telecom in the area of Information Technology participated in this research. Most of the participants answered to consider among medium and very loud the risk of improper collection through credit card and of interception of financial data in the purchases accomplished by the internet. The great majority of the interviewees (93%) it marked that would accomplish their purchases for the internet there were not been risks during those transactions.

Keywords: E-commerce, Internet, Security Information, Cryptography, Strategy

PERCEPÇÃO DOS RISCOS EM SEGURANÇA DA INFORMAÇÃO NAS TRANSAÇÕES EM E-COMMERCE: UMA ABORDAGEM ESTRATÉGICA

Introdução

O comércio eletrônico (e-commerce) constitui um novo modelo de negócios gerado a partir do crescimento vertiginoso da Internet nos anos 90. No modelo tradicional, as empresas em geral, e as de manufatura e de venda direta ao consumidor em especial, realizam negócios utilizando lojas, shopping centers, catálogos e vendedores de porta. Esse modelo de negócios concentra a venda em determinadas regiões e nichos econômicos (Filho, 2000)

A Internet é um ambiente de mídia interativo, não linear e que possui uma cultura peculiar. Kiani (1998) afirma que devido a estas diferenças, estão ocorrendo profundas variações na maneira como os usuários compram produtos e serviços. É sabido que um dos pontos mais desafiados para melhoria e confiabilidade para a realização de transações eletrônicas via internet é a segurança. Para Lasch (1998) um dos anseios identificados na compra pela Internet é por uma maior segurança, devido ao fato de que muitos consumidores ainda não estão conduzindo transações pela rede por conta dos riscos percebidos envolvidos na compra nesse meio.

O sucesso do comércio eletrônico depende da sua credibilidade, pois, nos mercados cada vez mais dinâmicos e competitivos, as empresas que têm maior probabilidade de sobreviver são, justamente, as que se preocupam com as expectativas, desejos e necessidades do cliente e que se equipam melhor que seus concorrentes para satisfazê- las (Giglio, 1996).

A segurança na internet é considerada uma das maiores barreiras para o desenvolvimento do comercio eletrônico. Temos hoje, virtualmente, uma gama enorme de negócios que possui seu próprio *web site*, por conseguinte, o número de indivíduos e empresas com acesso à internet tem se expandido rapidamente e o entusiasmo sobre as facilidades do comercio eletrônico na *web* são resultados desses fatos, porem a realidade mostra que a internet é extremamente vulnerável (Stallings, 1999).

A conjuntura atual enfrentada pela Internet, em especial pelo e-commerce, demonstra a existência de desafios que precisam ser transpostos uma vez que se pretende continuar com as atuais taxas de crescimentos (Filho, 2000). As empresas que pretenderem entrar no setor de comércio eletrônico devem comprovar aos seus consumidores em potencial, que seus *sites* são confiáveis, pois, de acordo com Engel *et al.* (1995), o risco percebido pode influenciar como os clientes irão satisfazer as expectativas das empresas de e-commerce. As freqüentes notícias de invasões em sistemas informatizados por meio da Internet transmitem uma imagem negativa para o leigo (Filho, 2000), o que pode ser um fator significativo na tomada de decisão e determinar o volume de transações pela Internet. Neste contexto, um dos desafios é reduzir os riscos voltados para segurança da informação percebidos pelos consumidores nas compras efetuadas via Internet e aumentar o volume de negociações no comercio eletrônico.

A principal preocupação que norteia este trabalho é identificar os riscos percebidos pelo usuário nas interceptações de dados em realizar compras via Internet e apresentar estratégias de segurança para eliminar tais riscos. Identificar tal preocupação é

importante na elaboração de estratégias em e-commerce, uma vez que influenciam no processo de decisão de compra. A elaboração de estratégias visa o aumento da segurança da informação e com isso a redução dos riscos de interceptação dos dados nas compras realizadas através da Internet o que possibilitaria um aumento de adeptos ao comércio eletrônico e ascensão das empresas do meio.

Atualmente as principais ferramentas estratégicas para minimizar os riscos em segurança da informação nas transações em e-commerce são: criptografia de dados, protocolo de autenticação, certificado digital, selo digital, assinatura digital e firewall.

O objetivo no presente estudo foi verificar quais os riscos percebidos pelo usuário com relação à segurança da informação em e-commerce e apresentar estratégias para eliminar estes riscos, identificar os riscos em segurança da informação em e-commerce percebidos por indivíduos que realizam, ou não, compras pela Internet, apresentar modelos utilizados para a segurança da informação que visam reduzir os riscos nas interceptações de dados no e-commerce também apresentar ferramentas de segurança da informação como meio estratégico para a redução do risco, por conseguinte, o aumento do volume de compras via Internet.

Referencial Teórico

Internet como meio de compra

O ambiente comercial da Internet possui características únicas que o distingue das formas tradicionais de comércio, trazendo um novo paradigma. A Internet é um ambiente de mídia interativo, não linear e que possui uma cultura peculiar. Kiani (1998) afirma que devido a estas diferenças, estão ocorrendo profundas variações na maneira como os usuários compram produtos e serviços.

Para Lasch (1998) um dos anseios identificados na compra pela Internet é por uma maior segurança, devido ao fato de que muitos consumidores ainda não estão conduzindo transações pela rede por conta dos riscos percebidos envolvidos na compra nesse meio. Os consumidores estão preocupados com a segurança do número do cartão de crédito e outras informações confidenciais transmitidas quando compram produtos e serviços na Internet. Existe também a preocupação sobre a legitimidade das empresas que vendem pela rede. De acordo com Lasch (1998), os consumidores estão corretamente preocupados com as questões de segurança no comércio pela Internet.

Risco percebido nas compras Via Internet

O risco percebido, segundo Solomon (1998), é a crença de que a compra de um produto ou serviço venha a ter conseqüências negativas. O risco percebido pode também ser considerado como uma característica das decisões nas quais exista a incerteza sobre as conseqüências significantes que possam acontecer.

Em uma análise dos diversos tipos de riscos percebidos encontrados na literatura supõe-se que as compras pela Internet podem desencadear alguns novos tipos de risco, como por exemplo, o risco da privacidade e segurança das informações transmitidas (Kovacs, 2004).

Em uma pesquisa realizada por Rohm e Milne (1998), os resultados indicaram que grande parte dos usuários da Internet, tanto os que efetuam compras por esse meio bem como os que nunca compraram, têm uma série de preocupações quanto à privacidade das informações, incluindo a aquisição e sua disseminação pelas empresas.

Ao enviar dados pessoais pela Internet o consumidor fica exposto, também, ao comércio desses dados pelas próprias empresas, desencadeando, assim, o receio do fim da privacidade, podendo surgir o risco social, em que a privacidade seja invadida sem o devido conhecimento e consentimento prévio.

No Brasil, segundo pesquisa realizada por Gonçalves et al. (1998), verificou-se que 66,67% dos internautas não confiam nas compras realizadas na Internet. As principais razões para essa falta de confiança foram: possibilidade do número de cartão de crédito ser utilizado por outros, pagamento adiantado sem garantia de recebimento da mercadoria e falta de informação em geral. Na mesma pesquisa foi indagado ao respondente se compraria na Internet caso esta oferecesse total segurança nas informações transmitidas, e verificou-se que 91,4% realizariam compras. A segurança na transmissão dos dados então surge como o grande desafio para um crescimento efetivo das transações comerciais na rede (Gonçalves et al., 1998)

Aspectos de segurança na web

Com o crescimento da grande rede e com o avanço tecnológico, a exploração comercial do meio teve início. Foi uma grande revolução quando as pessoas puderam à distância, sem contato verbal explícito, comprar os mais variados itens, ou então efetuar movimentações financeiras em suas contas bancárias (Ferro, 2003).

A Web foi projetada sem muita preocupação, ou quase nenhuma, com segurança. O objetivo principal era disponibilizar informações de uma forma mais amigável que os recursos disponíveis na época. Com o rápido crescimento da Web e com a diversificação de sua utilização, a segurança se tornou um ponto de importância crucial, principalmente para quem tem a Web como um dos principais apelos comerciais. (Figueiredo, 1999)

O uso da Internet para a indústria financeira foi extremamente modesto, mas desde então surgia uma preocupação que se tornaria ponto central e fator crítico para o sucesso dos negócios baseados nessa tecnologia: A segurança. (Ferro, 2003)

Segundo Turban *et al* (1999), Albertin (2000), Kosiur (1997) e Santos (2001), são variáveis importantes para a implantação de qualquer comércio eletrônico, a autenticidade, a integridade, a confidencialidade dos dados e transações Turban *et al* (1999), Albertin (2000), Kosiur (1997) e Santos (2001). Stallings (1999) acrescenta ainda, as variáveis de não repudio, controle de acesso (permissão), disponibilidade e tempestividade.

Autenticidade – deve provar que o transmissor ou receptor da mensagem é quem ele realmente quem ele diz ser. Para Albertin (2000), "ambas as partes tem de se sentir confortáveis e crentes que estão comunicando-se com aquela a qual estão fazendo negócios". Filho (2000) sugere ainda que o processo de autenticação de usuário é responsável por determinar com quem se está comunicando, antes de se revelar dados confidenciais ou se fechar qualquer negócio.

A primeira etapa é a autenticação, que assegura que o usuário é quem afirma ser. A segunda etapa é a autorização, que concede a um usuário acesso a recursos de uma rede com base na sua identidade (Filho, 2000).

No caso de uma interação em tempo real, como a conexão de um computador com outro, pode-se considerar dois aspectos, o primeiro no momento da inicialização da conexão, este serviço deve garantir que as duas entidades são autenticas, ou seja que são quem alegam ser. Em segundo lugar, o serviço deve garantir que a comunicação deve ocorrer de forma que não seja possível a uma terceira parte se disfarçar e se passar por

uma das partes já autenticadas na inicialização da conexão para conseguir transmitir e receber mensagens de forma autorizada (Curti, 2004).

Integridade – impedir que o conteúdo da mensagem seja modificado, intencionalmente ou acidentalmente, desde a sua origem até o seu destino e os dados não sejam modificados quando armazenados (Menezes, 2003).

O serviço de integridade pode ser aplicado a todo um fluxo de mensagens de uma conexão, a uma única mensagem ou a determinados campos desta mensagem. Uma conexão que tenha este princípio implantado garante que as mensagens serão recebidas como foram enviadas, sem duplicação, inserção indevida, modificações, sem reordenação ou repetições (Curti, 2004).

Sempre que se quer que uma mensagem não seja alterada. Refere-se portanto à integridade da informação que pode ser comprometida acidentalmente (erros humanos quando os dados são inseridos, erros de transmissão entre um computador e outro, vírus, bugs, etc.). Contudo, no comércio eletrônico, as situações a serem evitadas são aquelas em que pessoas mal intencionadas (ex.: hackers) comprometam deliberadamente a integridade das mensagens, por benefício próprio, para lesar alguém, ou simplesmente para se promoverem (Filho, 2000).

Confidencialidade – Garantir que o conteúdo da mensagem seja secreto e somente conhecido pelo transmissor e seu receptor, tornando-se um componente essencial para a privacidade do usuário (Menezes, 2003).

A confidencialidade é a proteção das informações contra ataques passivos e análise de mensagens, quando em trânsito nas redes ou contra a divulgação indevida da informação, quando sob guarda (Curti, 2004).

Com respeito à utilização indevida de conteúdos de mensagens, pode-se identificar diversos níveis de proteção para cada tipo de informação identificado. Podem ser definidos diversas formas para este serviços, incluindo a proteção de mensagens individuais ou até mesmo de campos dentro desta mensagem. Este processo de identificação e refinamento daquilo que realmente deve ser protegido é bastante complexo e se reflete em toda a estrutura de segurança adotada (Curti, 2004).

Não Repudiação – Garantir meios para provar a participação de todas as partes envolvidas na negociação após sua conclusão, evitando, assim, a negação ou repudiação por algumas das partes (Menezes, 2003).

Para Filho (2000) o não repudio serve para provar (por meio de assinaturas digitais) que, por exemplo, um consumidor pediu a um fornecedor, X artigos a um preço Y por cada. Mesmo que mais tarde o consumidor afirme, no ato da entrega, que encomendou menos artigos que a quantidade X, ou que cada artigo tinha um preço inferior a Y, o fornecedor serve-se dessa prova para que o consumidor não recuse a encomenda. (Curti, 2004)

Disponibilidade – prover meios para garantir a disponibilidade do sistema de Comercio Eletrônico (Menezes, 2003).

Uma grande variedade de ataques pode resultar na perda ou redução da disponibilidade da informação. Alguns desses ataques são compensados através de medidas automatizadas, como a autenticação e a criptografia, ao passo que já outros requerem algum tipo de ação física para a prevenção ou recuperação das perdas de disponibilidade de elementos de um sistema distribuído

Permissão de Acesso – Ter a habilidade de limitar e controlar o acesso a sistemas e aplicações através dos *links* de comunicação (Menezes, 2003).

Tempestividade – Permitir que todas as transações sejam datadas com dia e a hora da negociação e devem impedir alterações nas datas já gravadas (Menezes, 2003).

Santos (2001) diz que, para entender os requisitos de segurança em Comercio Eletrônico, é preciso entender que as ameaças podem existir com relação aos meios de comunicação.

Stallings (1999) classifica estas etapas em quatro categorias: Interrupção, Intercepcão, modificação e fabricação:

Interrupção – Representa um ataque sobre a disponibilidade do sistema, destruindo ou indisponibilizando um ou mais recursos do sistema.

Intercepção – Fere a confidencialidade do sistema permitindo que uma entidade não autorizada ganhe acesso às informações dos dados trafegados.

Modificação – Destrói a integridade do sistema, dando condições a uma entidade não só a obtenção de acesso, como permitindo a alteração de recursos e informações no sistema.

Fabricação – Ataca a autenticidade do sistema viabilizando a inserção, por parte de uma entidade a objetos no sistema.

Stallings (1999) ainda divide os ataques a sistema de segurança que envolve a *Web* em dois tipos: ativos e passivos. Os ataques passivos estão relacionados à "escuta" pelo atacante, dos dados trafegados entre o navegador e o servidor *Web* e a obtenção de informações que deveriam ser restritas (intercepção). Os ataques ativos incluem a representação ou imitação de outros usuários (fabricação), a alteração de mensagens em transito entre clientes e servidores (modificação), e a alteração de informação no *Web site* (modificação).

Ataques conhecidos como negação de serviço (DoS – Denial of Service) são exemplos de interrupções em sistema de segurança (Menezes,2003)

Os principais mecanismos de proteção hoje existentes são: criptografia, protocolos de autenticação, certificado digital, assinatura digital, selos digitais e firewall.

Criptografia de dados

Até alguns anos atrás, face à impossibilidade de inverter a função de ciframento das senhas e principalmente devido ao limitado desempenho dos computadores, o que inviabilizava buscas exaustivas de senhas, este mecanismo de criptografia e armazenamento de senhas era seguro. (Filho, 2000)

Atualmente, o grande desempenho dos novos microprocessadores e as redes de computadores permite que vários deles possam estar interagindo na busca de senhas. Assim, o sistema que apenas utiliza-se do mecanismo convencional de senhas tornou-se vulnerável, sendo um sério risco à segurança do sistema. .(Filho, 2000)

Os dois mais conhecidos programas de domínio público, que têm por objetivo quebrar senhas, são o "Crack" e o "John the Ripper". Ambos atuam de forma similar, exaustivamente buscando por palavras de dicionário, ou ainda cadeias de dígitos/letras que, cifrados, coincidam com alguma das senhas armazenadas no arquivo password. Quando isto ocorre, significa que a senha de algum usuário foi encontrada. Este tipo de busca normalmente primeiro encontra as senhas tidas como triviais (palavras e datas) para em seguida, após alguns dias de processamento, também encontrar senhas algo mais complexas.(Filho, 2000)

Para Kosiur (1997), as técnicas de criptografia utilizadas atualmente oferecem, ao Comercio Eletrônico, autenticidade, não repudiação e privacidade.Resumidamente o termo criptografia pode ser considerado como uma técnica que converte dados em um código complexo, difícil de ser quebrado. Este termo tem suas origens nas palavras

gregas *kryptós* e *grafos*, que significa escondido ou oculto, e grafia ou escrita, respectivamente (Menezes, 2003)

Albertin (2000) define a criptografia como ” a arte ou a ciência de escrever em cifra ou em código, ou ainda, como o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que somente o destinatário a decifre e a compreenda”.

Encriptação consiste no modo como são convertidos mensagens e dados para um formato ilegível e secreto com o escopo de proteger o seu conteúdo. Apenas quem possuir o algoritmo de encriptação e a chave secreta poderá fazer a decifragem. Por vezes, é possível decifrar. Contudo, as técnicas modernas de encriptação são virtualmente "inquebráveis". Exemplos de encriptação são a proteção de mensagens mail, informação de cartões de crédito e dados de empresas. Existem dois tipos principais de encriptação: chave única (usa apenas uma única chave que ambos, o emissor e o receptor, possuem) e chave pública (que usa uma chave pública conhecida por todos e uma chave privada que apenas quem recebe a mensagem encriptada conhece), aplicando-se a cada um dos métodos algoritmos próprios (Ahuja, 1997).

Criptografia de chave única ou privada.

A criptografia de chave privada envolve a utilização de uma única chave que serve tanto para cifrar como para decifrar o texto. Isto gera problemas na distribuição das chaves entre o transmissor e receptor, devendo-se utilizar um meio seguro para o envio dessa chave, o que pode ser incomodo em grandes redes de comunicação (ALBERTIN 2000)

Também designada de encriptação tradicional ou encriptação simétrica, utiliza a mesma chave tanto para a codificação como para a decodificação. As mensagens (X), ou dados, são transformados num formato (Y), codificado por meio de uma função matemática (método de encriptação), parametrizada pela chave (W). Para que o receptor consiga decifrar a mensagem ou ter acesso a dados, há que possuir a chave (W) (Filho, 2000). O processo pode ser visualizado na figura 1.

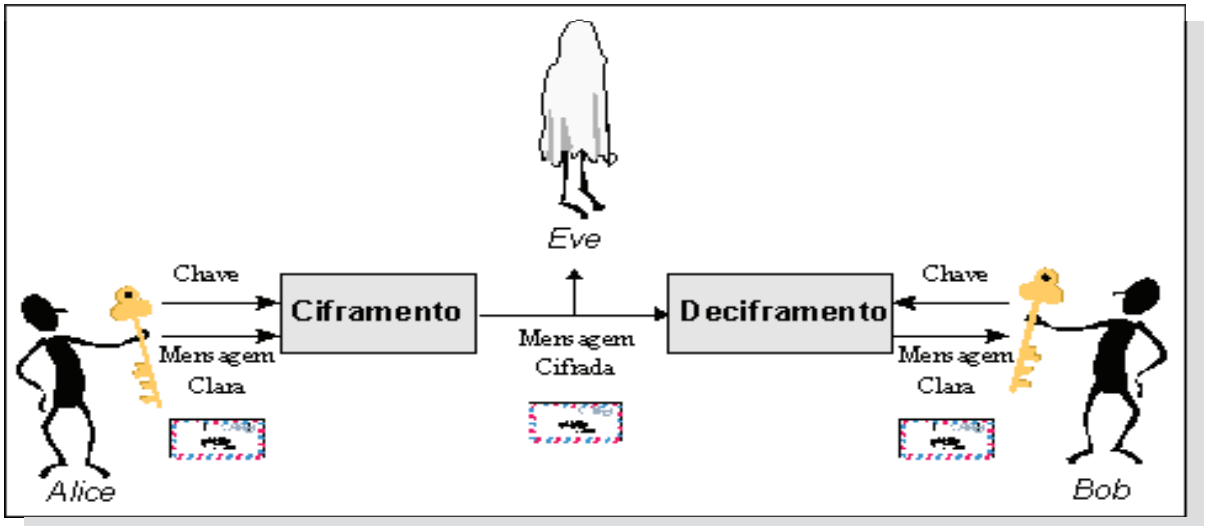

Figura 1 - Modelo de Criptografia de Chave única

A criptografia de chave pública ou assimétrica evita este problema, porque a chave pública pode ser distribuída num meio não seguro, contudo a chave privada nunca é transmitida. (Filho, 2000)

Criptografia de chave pública e alguns algoritmos

Historicamente, a distribuição da chave num sistema de criptografia de chave única sempre foi, e continua a ser, o ponto mais vulnerável deste processo. Se algum invasor puder subtrair a chave, o mais perfeito sistema de encriptação de chave única torna-se inútil. As chaves precisam ser distribuídas a todos os usuários de um sistema, caso contrário não podem ter acesso a mensagens ou dados que lhes são destinados. (Filho, 2000)

Para eliminar o problema, surgiram em 1976 dois investigadores da Universidade de Stanford, Diffie e Hellman, que propuseram um sistema radical de um novo sistema de criptografia em que as chaves de encriptação (chave pública, conhecida por todos) era diferente da chave de decifragem (chave privada, conhecida apenas pelo destinatário da mensagem) e que a chave de decifragem não poderia ser derivada através da chave de encriptação.(Filho, 2000)

Em sua proposta, o sistema de criptografia tinha que atender a três requisitos: 1º) se aplicarmos um algoritmo decifração chaveado (X) a uma mensagem cifrada por um algoritmo decifração chaveado (Y), obteremos a mensagem de texto simples ou plano original (W); 2º) é excessivamente difícil deduzir (X) de (Y); 3º) Não pode ser decifrado através de ataque de texto plano escolhido. (TANENBAUM, 1997).

Neste sistema as chaves existem aos pares, em que uma delas serve para codificar a mensagem e a outra para a respectiva decodificação. Deste modo, cada interveniente numa transação, normalmente o cliente e o servidor, tem cada qual associado um par de chaves únicas. Uma dessas chaves é chamada de chave pública, chave esta utilizada para codificar as mensagens e largamente distribuída. A outra chave, designada por chave privada, está cuidadosamente guardada e é utilizada para decodificar mensagens recebidas. Um interveniente que necessite enviar uma mensagem a outro irá encriptar a mensagem recorrendo ao algoritmo público do destinatário. Deste modo, a mensagem só pode ser unicamente decodificada por meio da chave privada do destinatário, ficando assim livre de interceptações. (Filho, 2000)

Protocolos de autenticação

Conforme antes dito, a autenticação é a forma de ser verificada a identidade de uma pessoa (ou usuário, neste contexto) ser aquela que afirma ser. Assim, no caso de um impostor tentar assumir uma identidade falsa, o protocolo de autenticação deve ser capaz, no mínimo, de ignorá-lo e de preferência tomar algumas precauções defensivas. Existem no mercado alguns protocolos que têm como objetivo a realização de trocas seguras de dados em redes tipicamente abertas, como a Internet. Os três mais utilizados, ou pelo menos mais conhecidos são o SSL, o S-http, SET, S/MIME, Ipsec, etc. (Filho, 2000)

Assinaturas digitais

As assinaturas digitais têm uma importância crucial para a sedimentação e o crescimento do comércio eletrônico, vez que na seara dos negócios, como no mundo dos

relacionamentos outros, exige-se que o ambiente de atuação possua um nível de segurança aceitável pelas partes intervenientes (Filho, 2000).

Tal como as assinaturas escritas, o propósito de uma assinatura digital é garantir que um indivíduo que envie uma mensagem realmente seja quem afirma ser. Resume-se a um código que pode ser enviado juntamente com uma mensagem que identifica de forma única o emissor da mensagem (Filho, 2000).

No modelo de assinatura convencional, a assinatura faz fisicamente parte do documento que está sendo assinado, enquanto que uma assinatura digital não está fisicamente junto da mensagem a ser assinada. A assinatura convencional pode ser verificada comparando-se dois documentos que contêm a mesma assinatura, enquanto que a assinatura digital, por outro lado, pode ser verificada utilizando-se um algoritmo de verificação público (Menezes 2003).

Outra diferença fundamental entre assinatura convencional e digital está no fato de que a "cópia" de uma assinatura em uma mensagem digital é idêntica à original, enquanto que uma assinatura em papel pode comumente ser diferente da original. Essa última característica mostra que cuidados devem ser tomados para evitar que uma mensagem assinada digitalmente seja reusada, portanto, deve-se acrescentar informações, como data à mensagem. Um esquema de assinatura consiste em dois componentes: um algoritmo de assinatura e um algoritmo de verificação (STINSON, 1995).

Na assinatura digital, o receptor (X) sempre utilizará a chave publica da origem (Y) para decifrá-la, para garantir a autenticidade de chaves publicas foram criados os certificados digitais (Menezes, 2003)

Num sistema com chave pública, qualquer pessoa pode cifrar uma mensagem, mas somente o destinatário da mensagem pode decifrá-la. Vê-se que, ao revés, uma pessoa pode fazer uso de uma só chave para cifrar determinada mensagem, e a decifragem ser realizada por outrem que tenha a chave pública do emissor, obtendo-se assim uma personalização do documento, tal qual uma assinatura. A um processo desse tipo denomina-se assinatura digital (Filho, 2000).

Exemplificadamente, X personaliza uma mensagem, codificando-a com sua chave secreta, e a envia para o destinatário Y. Y, possuidor da chave pública de X, tem a faculdade de decodificar a mensagem – a mensagem pode ser decodificada por qualquer um que tenha a chave pública de X. A chave secreta de X é a prova de que este realmente é o emissor do documento (Filho, 2000).

Uma assinatura digital deve possuir as seguintes propriedades (Pistelli, 1999):

1 - a assinatura há que ser autêntica: quando um usuário usa a chave pública de X para decifrar uma mensagem, ele confirma que foi X e somente X quem enviou a mensagem;

2 - a assinatura não pode ser forjada: somente X conhece sua chave secreta;

3 - o documento assinado não pode ser alterado : se houver qualquer alteração no texto criptografado, este não poderá ser restaurado com o uso da chave pública de X;

4 - a assinatura não é reutilizável: a assinatura é uma função do documento e não pode ser transferida para outro documento;

5 - a assinatura não pode ser repudiada: o usuário Y não precisa de nenhuma ajuda de X para reconhecer sua assinatura e X não pode negar ter assinado o documento.

Então, o uso de assinaturas digitais envolve dois processos: um realizado pelo usuário remetente, que assina o documento; o outro, pelo destinatário da assinatura digital, que a autentica (Filho, 2000).

Selos Digitais

Serve para gerar chancelas cronológicas que associam data e hora a um documento digital sob a forma de criptografia forte. Futuramente, terá grande aplicação para fazer prova da existência de certo documento eletrônico em determinada data. Concretamente, como exemplo, um pesquisador pode descrever seu achado científico em documento e selá-lo com selo eletrônico digital. Posteriormente, poderá comprovar a antecedência de sua idéia, a despeito de publicação inédita por parte de outros pesquisadores (Filho, 2000).

Firewall

Um sistema pode oferecer múltiplos métodos de autenticação para controlar o acesso a dados, particularmente porque os hackers são muitas vezes persistentes e geniais nos seus esforços de obterem acesso não autorizado. Um método de defesa poderá ser uma Firewall, um dispositivo (ex.: um computador) inserido entre a rede de uma organização e o resto da Internet (ver figura 2) (Filho, 2000).

Figura 2 - *Firewall* como uma barreira física protetora de uma Intranet.

Firewall é um componente, ou conjunto de componentes (*software* e *hardware*), que pretende forçar a aplicação de políticas de segurança estabelecidas entre uma rede privada e o mundo exterior. Também chamado de barreira de fogo, o *firewall* determina que serviços internos podem ser acessados pelo meio exterior ao perímetro de segurança, quem pode acessá-los, quais serviços externos podem acessados a partir do meio interno da rede e quem pode acessá-los internamente. Para funcionar efetivamente, um *firewall* deve posicionar-se estrategicamente na rede, de forma que todo o trafego interno para internet, é vice e versa, deva passar por ele a fim de ser inspecionado, permitindo apenas que trafego autorizado ultrapasse a área de segurança (Tanenbaum, 1997)

Esta barreira monitoriza e controla todo o tráfego entre a Internet e a rede interna organizacional. O seu propósito é restringir o acesso de estranhos à Intranet. Uma Firewall está normalmente localizada no ponto onde a rede interna (intranet) é ligada à Internet, contudo também é praticável ter Firewalls dentro da própria Intranet para limitar ainda mais o acesso a dados (neste caso, a certos usuários da Intranet) (Filho, 2000).

O uso de Firewalls limita o acesso, e como tal, certas operações como publicidade e compra/venda de produtos poderão não ser feitas ou então serem minimizadas (Filho, 2000).

Para mitigar estas desvantagens, opta-se por implementar uma Firewall simples com poucas regras de restrição de acesso quando uma organização pretende fazer publicidade de produtos ou serviços ou outro tipo de operações comerciais. Quando uma

organização pretende partilhar dados confidenciais unicamente a um conjunto selecionado de clientes, então é aconselhável instalar um Firewall mais complexa de modo a oferecer um grau de segurança elevado (Filho, 2000).

Ameaças na Web

Atualmente, a Web enfrenta diferentes formas de ameaça que foram surgindo ao longo de sua evolução. A Web não introduziu muito mais ameaças de segurança do que já existia na Internet. A Internet funciona para a Web como seu mecanismo de transporte e, portanto herda suas vulnerabilidades de segurança. Devido à pressa na construção de novas funcionalidades em todo o ambiente, projetistas não consideraram o impacto em segurança que esta nova tecnologia causaria, deixaram de ver importantes pontos de possíveis ataques e vulnerabilidades. A Web não demorou muito em caminhar da comunidade científica para o mundo comercial. Neste ponto, as ameaças tornaram-se mais sérias. Uma nova tecnologia encontrava-se disponível e muito atrativa para os atacantes. Figueiredo (1999)

A tabela a seguir apresenta uma comparação das principais formas de ameaças em segurança encontrada em transações pela Internet (Figueiredo, 1999)

A maioria dos ataques a aplicativos da Web solicitam a transmissão de entradas mal–intencionadas por meio de solicitações HTTP. O objetivo geral é coagir o aplicativo a executar operações não autorizadas ou interromper suas operações normais.

	Integridade	Confidenciabilidade	Negação de Serviço	Autenticação
Ameaças	- modificação de dados do usuário - browser cavalo de Tróia - modificação de memória - modificação de mensagens em trânsito	- eavesdropping - roubo de info/dado do servidor/cliente - info da configuração da rede/máquinas... - info de qual cliente "conversa" com servidor em trânsito	- bloqueio da conexão - inundação da máquina com solicitações bogus - isolamento máquina por ataques a DNS	- personificação de usuários legítimos - falsificação de dados
Consequências	- perda de info - compromete a máquina - vulnerabilidade para outras ameaças	- perda de informação - perda de privacidade	- interrupção - aborrecimento - impedir usuário realizar seu trabalho	- má representação do usuário - crença que informação falsa é verdadeira
Medidas	- checksums criptográfico	- encriptação, Web proxy	- difícil prevenir	- técnicas criptográficas

Tabela 1 : Comparação das principais formas de ameaças em segurança encontrados em transações pela Internet

É por isso que uma validação de entradas abrangente é uma contramedida essencial para vários ataques, devendo ser uma prioridade no desenvolvimento de páginas da Web e controles ASP.NET (Microsoft, 2006). A Figura 3 realça as ameaças mais comuns a aplicativos da Web.

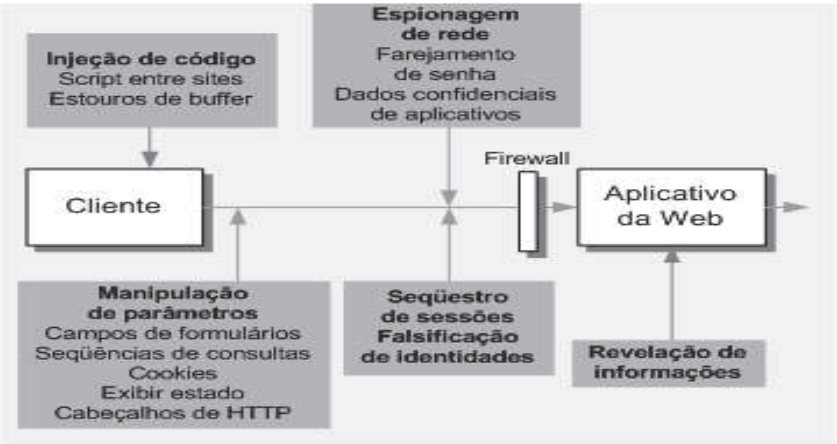

Figura 3: Ameaças comuns a páginas da Web e controles ASP.NET

Incidentes de segurança no Brasil

O CERT.br mantém estatísticas sobre notificações de incidentes a ele reportados. Estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os notificaram ao CERT.br

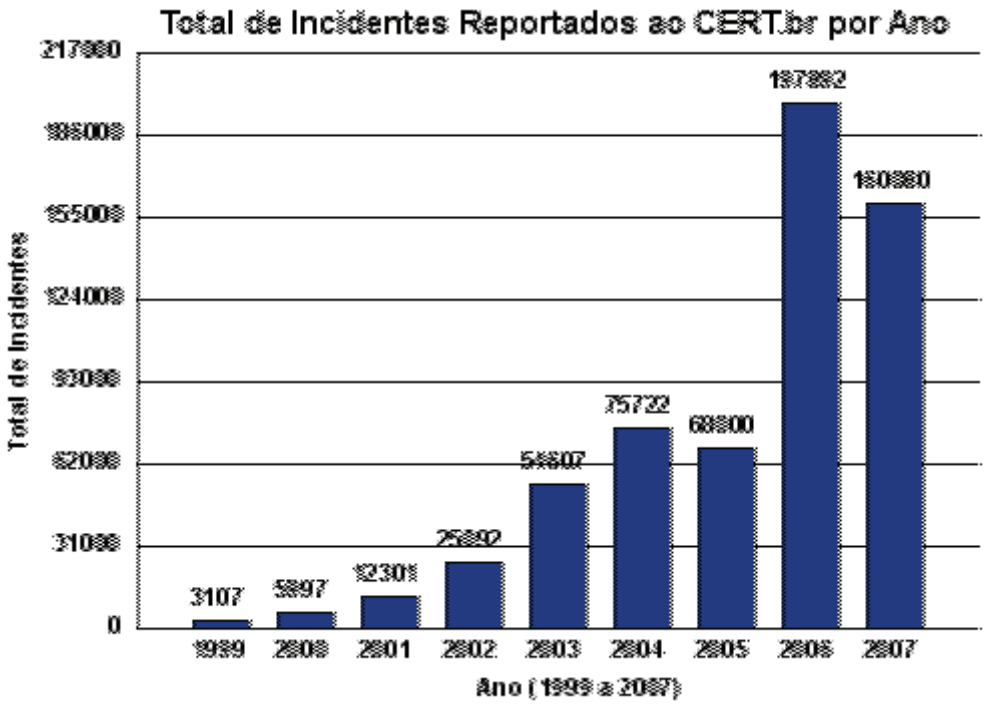

Figura 4 : Incidentes Reportados ao CERT.br – Jan. a Dez. de 2007

A Figura 4 chama a atenção para o crescimento no número de incidentes reportados ao CERT.br, certamente pelo aumento concomitante do número de usuários.

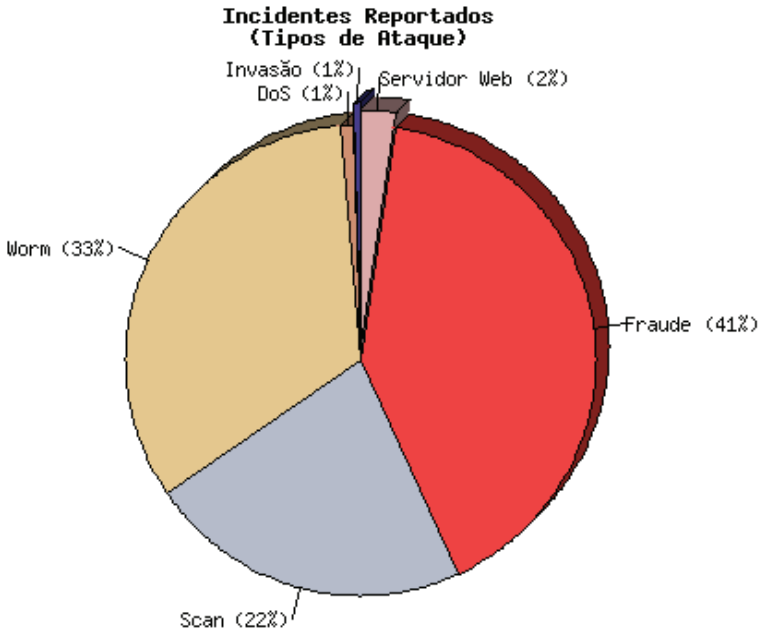

Figura 5: Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2007

A Figura 5 apresenta os tipos de incidentes de denunciados, enfatizando as fraudes (41%), worms (33%) e scans (22%) que totalizam 96% dos tipos de ataques relatados ao CERT.

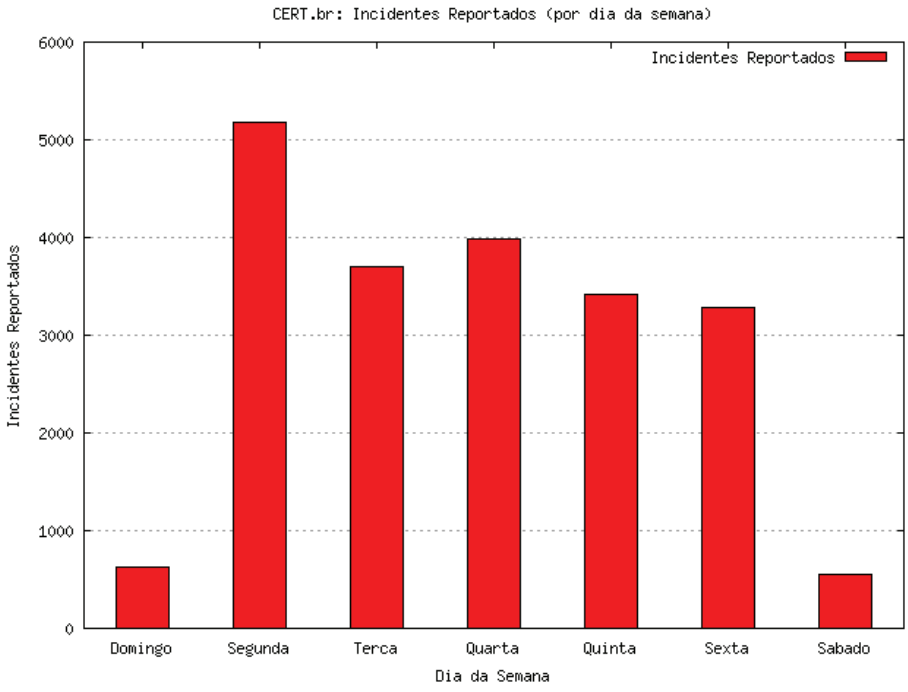

Figura 6: Incidentes Reportados ao CERT.br de acordo com os dias da semana

A Figura 6 expõe os ataques nos diferentes dias da semana. A segunda feira é retratada como o dia de maior número de ataques a rede que totalizam quase 5000 incidentes em todo Brasil.

O aspecto da segurança no ambiente Internet abre cada vez mais horizontes e oportunidades de negócios para empresas que trabalham com e-commerce.

O mundo digital é uma realidade da qual não se pode fugir, pois os que são contrários a esses avanços tecnológicos, acabam sendo levados pela grande massa que adota as inovações oferecidas, considerando o universo de pessoas que atualmente acessam a rede e que têm potencial de efetuar transações por ela.

Metodologia

Pelo objetivo proposto, este estudo é de caráter exploratório-descritivo. Exploratório devido à temática e ao número de casos analisados, contudo descritivo, uma vez que o método descritivo tem como objetivo principal descrever características de determinada população ou fenômeno e estabelecer relações entre as variáveis (Bickman, Rog e Hedrick, 1997).

Os dados coletados foram essencialmente primários, ou seja, obtidos especialmente para atender às necessidades da pesquisa (Bickman, Rog E Hedrick, 1997). Esta pesquisa foi do tipo corte-transversal, uma vez que os dados foram coletados em um único período de tempo sem a intenção de traçar a evolução ou identificar mudanças ao longo do tempo (Sieber, 1997). Não foram analisadas as determinantes interpessoais (fatores culturais e sociais) nem as psicológicas (motivação, percepção, atitude, aprendizagem e outras), somente as características que influenciam no processo de compra como: idade, sexo e grau de escolaridade.

O primeiro passo desse trabalho foi um levantamento teórico do material disponível sobre segurança da informação voltado para o comercio eletrônico e as reações provocadas pela a falta da mesma no consumidor neste segmento, tendo como foco o risco percebido nas interceptações dos dados nas compras realizadas por meio da internet. A literatura investigada para a revisão teórica compreendeu pesquisa em periódicos, dissertações, revistas indexadas, livros e web sites nas áreas de administração, tecnologia de informação e e-commerce.

Instrumento de coleta de dados

O instrumento de coleta de dados foi um questionário auto-explicativo preenchido individualmente, contendo 17 perguntas. Foi utilizada uma escala de cinco pontos, permitindo aos respondentes atribuir graus crescente aos riscos identificados na hora de realizar uma compra via internet, através de uma escala artificial de pontos que variam de 1 a 5, em que: 1 muito baixo, 2 baixo, 3 médio, 4 alto e 5 muito alto. (Kovacs e Salomão, 2004)

Amostra

A amostra que constituiu esta pesquisa foi composta de 71 participantes que trabalham em uma empresa de telecomunicações no departamento de TI (Tecnologia da Informação), portanto com suficiente conhecimento ao acesso à internet. Os critérios de inclusão na pesquisa foram: ter acesso regular à internet, trabalhar na empresa a pelo menos 3 meses, visando assim obter uma amostra mais homogênea com um domínio

suficiente sobre as ferramentas de segurança de informação e ter idade superior a 20 anos (teoricamente tendo maior poder de compra e acesso a cartões de crédito).

Os participantes foram abordados de forma aleatória e neste momento eram esclarecidos dos objetivos e da finalidade exclusiva na utilização dos dados para fins de pesquisa.

Técnicas estatísticas para análise dos dados

Para mensuração dos dados obtidos por meio do questionário proposto será utilizado o programa Microsoft Office Excel 2003.

Este programa permite a tabulação das informações e sua representação sob a forma de gráficos e tabelas o que possibilita uma melhor interpretação e entendimento dos dados.

Resultados

Toda pesquisa utiliza dados qualitativos e quantitativos, em dosagens variadas. Quando uma pesquisa se apóia completamente, ou quase completamente em dados quantitativos, ela é chamada de pesquisa quantitativa; de forma distinta, quando ela se firma em textos ou outras variedades de dados qualitativos, ela é chamada de pesquisa qualitativa. Enquanto a pesquisa quantitativa utiliza a estatística como ferramenta básica de organização e análise dos dados, a pesquisa qualitativa utiliza ferramentas lógicas e de observação (Moreira, 2002).

A pesquisa qualitativa identifica a presença ou ausência de algo, enquanto a quantitativa procura medir o grau em que este algo está presente. Na quantitativa, os dados são obtidos de um grande número de respondentes. Usando-se escalas são submetidos a análises estatísticas formais Na qualitativa, os dados são colhidos através de perguntas abertas através de questionários ou entrevistas em grupos ou individuais ou ainda em profundidade (Cruz & Ribeiro, 2003)

> No caso desta pesquisa, pode-se dizer que ela se orientou por um estudo de campo quantitativo, tendo em vista o objetivo colocado de verificar a percepção do risco quanto à segurança da informação nas compras pela Internet.

Dessa forma, a coleta de dados enfatizou números (ou informações conversíveis em números) que permitiram verificar relações entre graus diferenciados dos riscos percebidos tendo o e-commerce como meio de compra.

O primeiro passo desse trabalho foi um levantamento teórico do material disponível sobre segurança da informação voltado para o comercio eletrônico e as reações provocadas pela a falta da mesma no consumidor neste segmento, tendo como foco o risco percebido nas interceptações dos dados nas compras realizadas via internet. A literatura investigada para a revisão teórica compreendeu pesquisa em periódicos, dissertações, revistas indexadas, livros e web sites nas áreas de Administração, Tecnologia de Informação e e-Commerce.

A esta revisão seguiu-se uma pesquisa qualitativa, que buscou subsídios complementares à literatura para o entendimento do objeto de estudo e construção do questionário para o *survey* pela Internet.

Instrumento de coleta

O questionário auto-explicativo foi composto por 17 itens sobre os riscos percebidos em segurança da informação percebidos pelos entrevistados ao se realizar compras via Internet. Foram elaboradas frases em que os respondentes indicavam o quanto concordavam ou discordavam da existência destes riscos de comprar pela Internet.

Foi utilizada uma escala de cinco pontos, permitindo aos respondentes atribuir graus crescente aos riscos identificados na hora de realizar uma compra via internet, através de uma escala artificial de pontos que variam de 1 a 5, em que: 1 muito baixo, 2 baixo, 3 médio, 4 alto e 5 muito alto. (Kovacs e Salomão, 2004)

PESQUISA DE ANÁLISE DE RISCO UTILIZANDO E-COMMERCE

Você já realizou alguma compra na Internet?
( ) sim ( ) não

Idade: ( ) 20-30 anos ( ) 30-40 anos
( ) 40-50 anos ( ) acima de 50 anos

Escolaridade: ( ) 1º Grau ( ) 2º Grau
( ) 3º Grau ( ) Pós-Graduado

Sexo ( ) M ( ) F

Marque a intensidade do risco na hora de realizar uma compra via internet, de acordo com a tabela abaixo.

1	Muito Baixo
2	Baixo
3	Médio
4	Alto
5	Muito Alto

01. Transporte inadequado da mercadoria

1	**2**	**3**	**4**	**5**

02. Intercepção dos dados financeiros

1	**2**	**3**	**4**	**5**

03. Descumprimento do prazo de entrega da mercadoria

1	**2**	**3**	**4**	**5**

04. Não ficar satisfeito com a mercadoria

1	**2**	**3**	**4**	**5**

05. Encontrar um outro produto com preço inferior ao comprado

1	**2**	**3**	**4**	**5**

06. Divulgação dos dados pessoais

1	**2**	**3**	**4**	**5**

07. Cobrança indevida através de cartão de crédito

1	2	3	4	5

08. Demora/dificuldade em realizar trocas

1	2	3	4	5

09. Garantia do produto

1	2	3	4	5

10. Facilidade na negociação de preços

1	2	3	4	5

11. Empresa não efetue todas as etapas do processo de compra (idoneidade da empresa)

1	2	3	4	5

12, Demora/dificuldade em realizar compra (complexidade do site)

1	2	3	4	5

Se não houvesse risco nas transações via internet, você utilizaria o meio para efetuar suas compras? ( ) sim ( ) não

Amostra

A amostragem é um campo da estatística bastante sofisticado que estuda técnicas de planejamento de pesquisa para possibilitar inferências sobre um universo a partir do estudo de uma pequena parte de seus componentes, uma amostra (Lee, 2006)

A amostra que constituiu esta pesquisa foi de natureza não probabilística (amostragem restrita aos elementos que se tem acesso) e teve como critérios de inclusão: ter nacionalidade brasileira, trabalhar na empresa a pelo menos 3 meses, visando assim obter uma amostra mais homogênea com um domínio suficiente sobre as ferramentas de segurança de informação e ter idade superior a 20 anos, teoricamente tendo maior poder de compra e acesso a cartões de crédito.

Antes da aplicação dos questionários os participantes foram esclarecidos dos objetivos e da finalidade exclusiva na utilização dos dados pra fins de pesquisa e utilização dos dados. Os respondentes foram abordados de forma aleatória durante seu horário de trabalho.

Técnicas estatísticas para análise dos dados

Os dados foram condensados em um banco de dados, de modo a cumprir os objetivos propostos.

A mensuração dos dados obtidos através do questionário proposto e a confecção nos gráficos foram realizadas no programa Microsoft Office Excel 2003 e demonstradas em percentuais para facilitar a compreensão e promover comparação com o total amostral.

Análise dos Resultados

A pesquisa foi realizada no departamento de TI – Tecnologia de Informação de uma empresa de Telecomunicações com o quadro de colaboradores composto de 480 pessoas, sendo 73% do sexo masculino. O questionário aplicado abrangeu este público

para que fosse possível detectar a sensibilidade de risco em segurança da informação ao optar por comprar ou não utilizando o e-commerce. Esta população foi escolhida por possuir conhecimento específico na área de tecnologia de informação, meio disseminação do e-commerce.

Caracterização da Amostra

A amostra foi composta de 71 participantes, destes 50 (70,4%) responderam já ter utilizado a internet para realizar compras e 21 (29,6%) não realizam compras através da Internet, dados apresentados no gráfico 01.

Gráfico 01: Realização de compras pela Internet

A faixa etária entre 20 e 30 anos compreendeu 56,3% dos respondentes, 32,4% encontravam-se entre 31 e 40 anos, 8,4% entre 41 e 50 anos e 2,8 % acima de 51 anos de acordo com o gráfico 02.

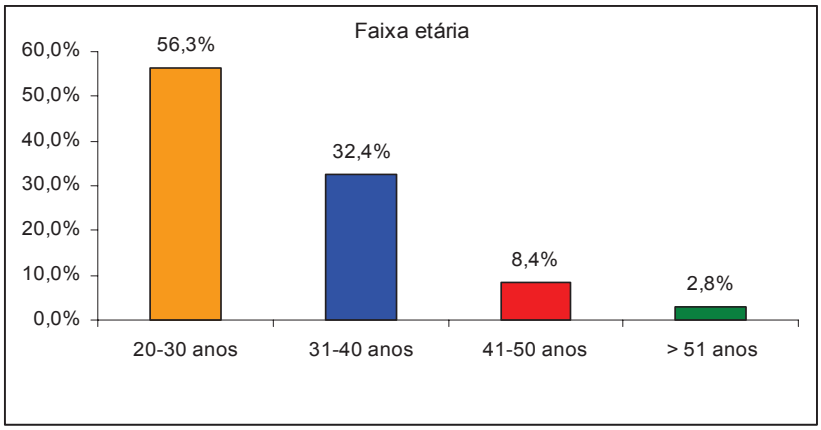

Gráfico 02: Faixa Etária da amostra estudada.

A maior parte dos participantes possuía 3º grau completo (88,7%) e destes 80% declararam ter curso de pós-graduação. Este resultado era esperado uma vez que a empresa pesquisa exige profissionais com maior grau de instrução

Análise dos Riscos Percebidos

Para todas as perguntas foi utilizada uma escala artificial de pontos respondidas de acordo com a seguinte instrução: “Marque a intensidade do risco na hora de realizar uma compra via internet, de acordo com a tabela abaixo.”

1	Muito Baixo
2	Baixo
3	Médio
4	Alto
5	Muito Alto

Os resultados apresentados é a exposição dos dados obtidos por meio do questionário aplicado.

Pergunta 01: Transporte inadequado da mercadoria

De acordo com o gráfico 03, observa-se que a maioria dos respondentes opinou entre muito baixo e médio o risco de transporte inadequado das mercadorias compradas pela internet.

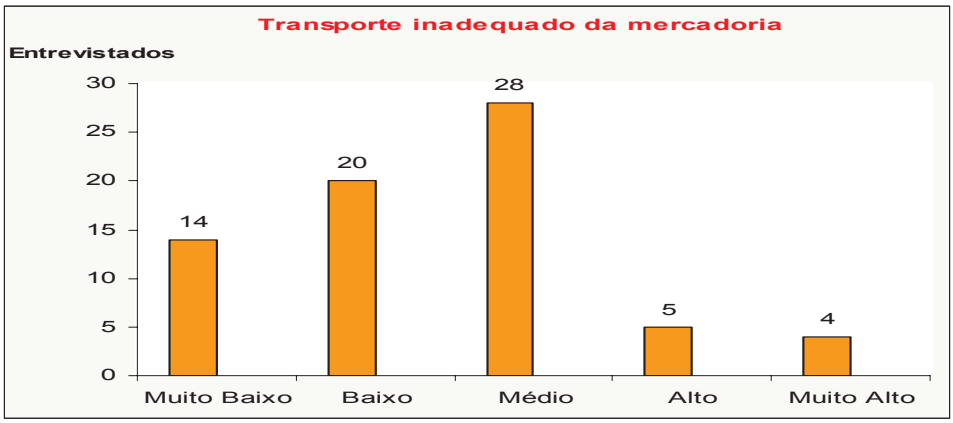

Gráfico 03: transporte inadequado das mercadorias

Pergunta 02: Interceptação dos dados financeiros

O gráfico 04 apresenta a insegurança dos entrevistados quanto a interceptação dos dados financeiros, 90,1% dos entrevistados, ou seja 64 participantes, afirmaram considerar entre médio e muito alto o risco de ter suas informações interceptadas.

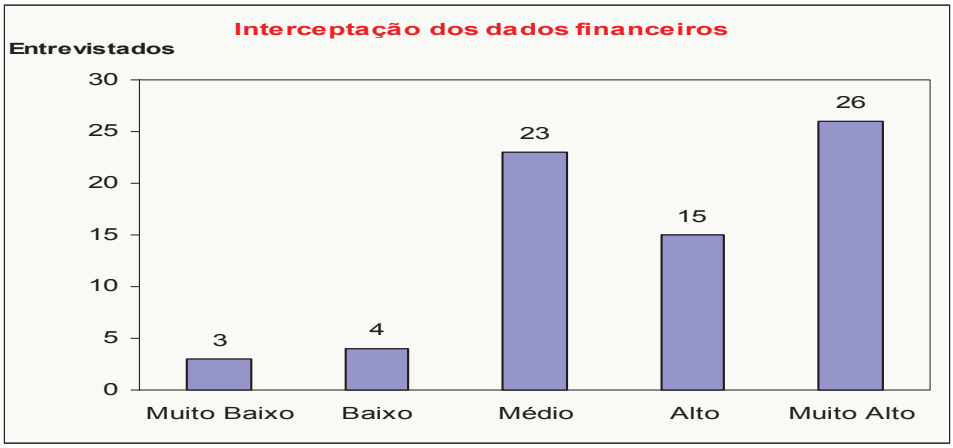

Gráfico 04: Interceptação dos dados financeiros

Pergunta 03: Descumprimento do prazo de entrega da mercadoria

Constatou-se que os 38% dos entrevistados (27 participantes) opinaram considerar médio risco de descumprimento do prazo de entrega da mercadoria e 32,4% (23 participantes) como alto ou muito alto como mostra a gráfico 05.

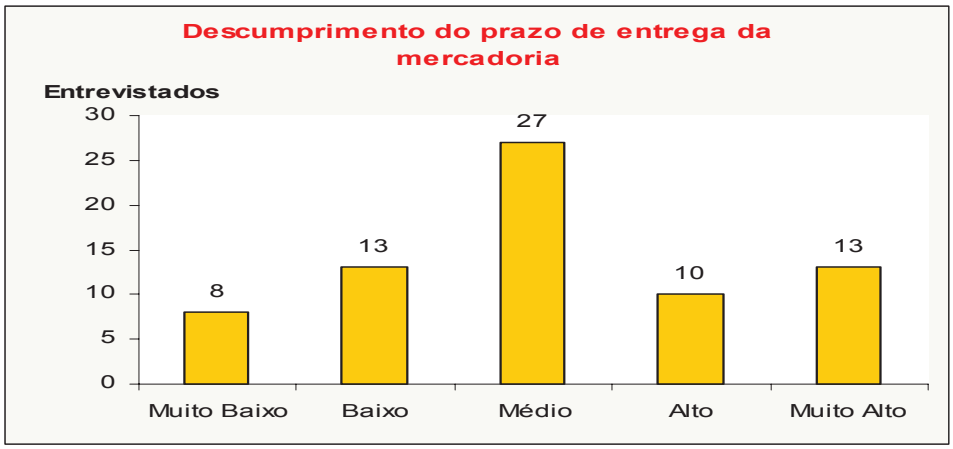

Gráfico 05: Descumprimento do prazo de entrega da mercadoria comprada via internet

Pergunta 04: Não ficar satisfeito com a mercadoria

Para esta pergunta, 69% (49 participantes) assinalaram entre muito baixo e médio o risco de não ficar satisfeito com a mercadoria, e 31% (22 participantes) entre alto e muito alto. O gráfico 06 apresenta esses dados.

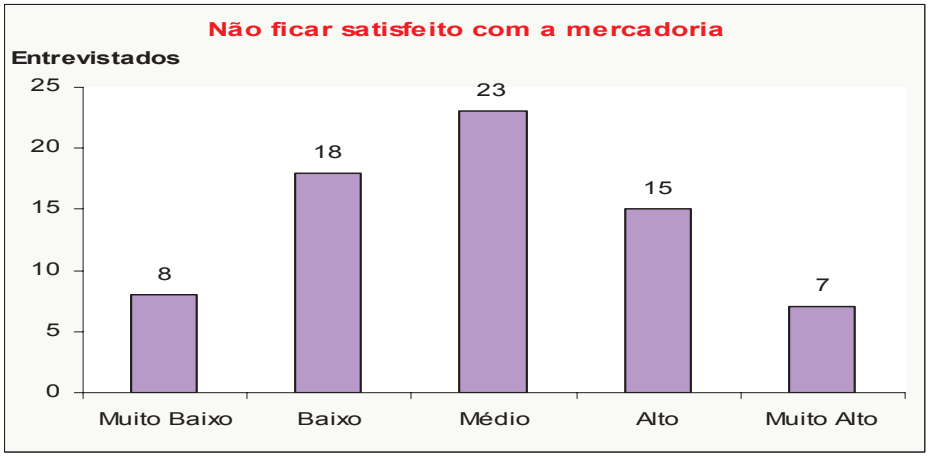

Gráfico 06: Não ficar satisfeito com a mercadoria

Pergunta 05: Encontrar um outro produto com o preço inferior ao comprado

Como confirma o gráfico 07, o maior percentual de risco em encontrar um outro produto com o preço inferior ao comprado ficou entre muito baixo e médio, que corresponde a 71,8% dos respondentes (51 participantes).

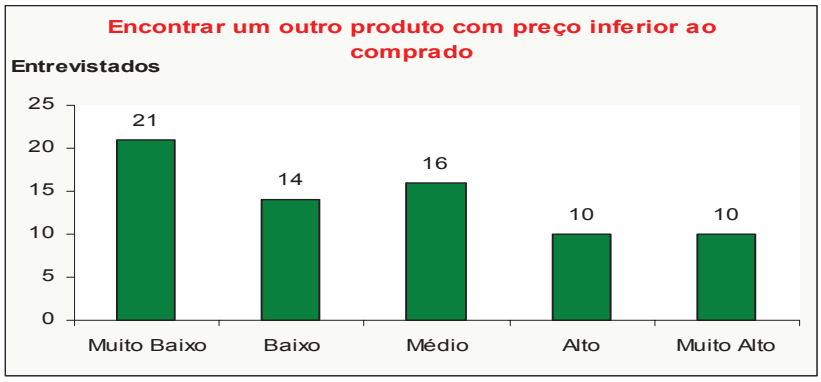

Gráfico 07: Encontrar um outro produto com o preço inferior ao comprado

Pergunta 06: Divulgação dos dados pessoais

A grande maioria, 90, 1% dos entrevistados foram enfáticos em demonstrar a insegurança em disponibilizar dados pessoais na internet. O gráfico 08 exibe estes dados. 64 participantes declararam considerar de médio a muito alto o risco de divulgação de seus dados pessoais.

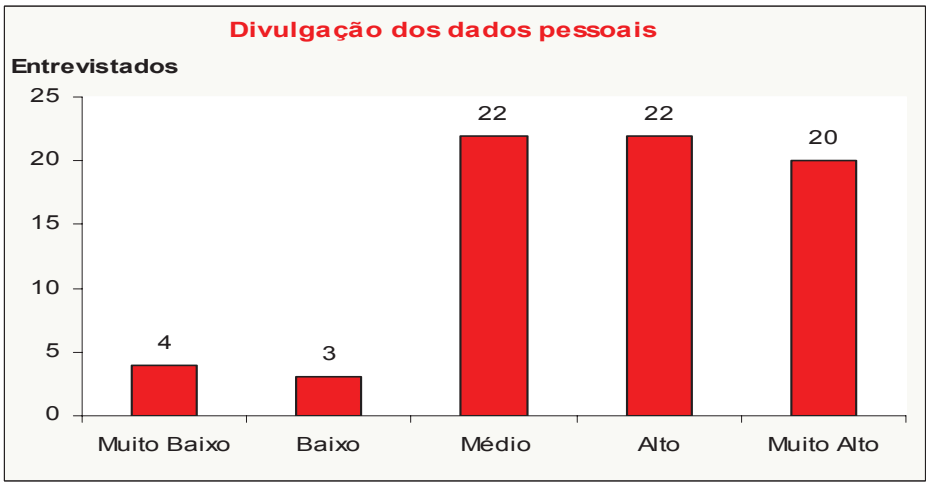

Gráfico 08: Divulgação dos dados pessoais

Pergunta 07: Cobrança indevida através de cartão de crédito

Dos entrevistados que participaram desta pesquisa, 69% (49 participantes) consideraram como risco de médio a muito alto a cobrança indevida através de cartão de crédito. O cenário abordado é apresentado no gráfico 09

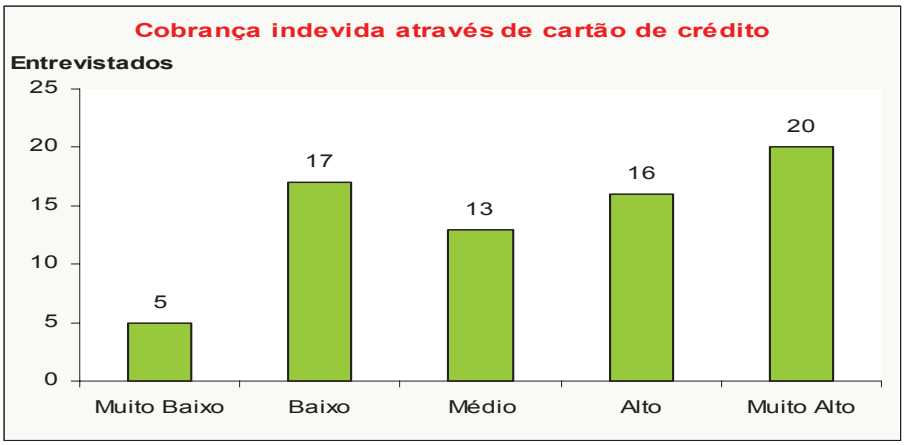

Gráfico 09: Cobrança indevida através de cartão de crédito

Pergunta 08: Demora/Dificuldade em realizar trocas

Outro ponto abordado pela pesquisa e que demonstrou bastante preocupação dos entrevistados é o risco da demora/dificuldade em realizar trocas,uma vez que 88,7% (63 participantes) das pessoas responderam entre médio e muito alto.

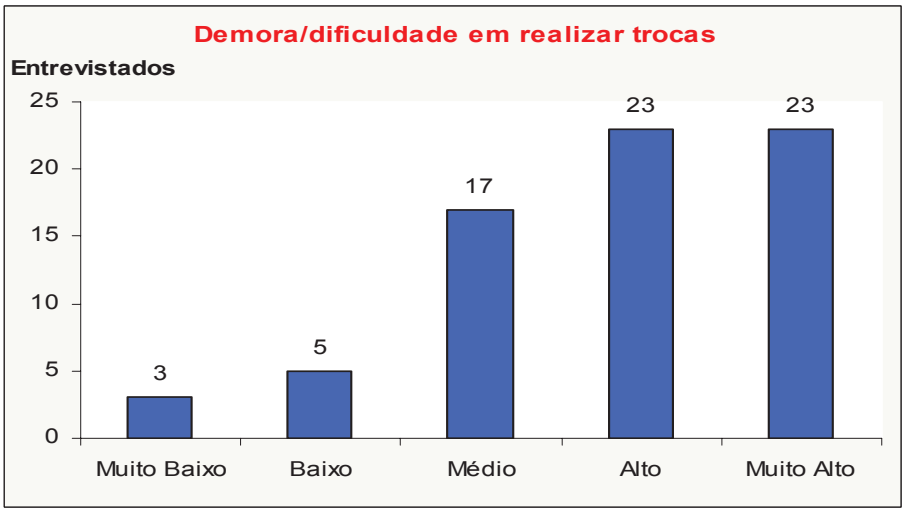

Gráfico 10: Demora/ Dificuldade em realizar trocas

Pergunta 09: Garantia do produto

O gráfico10 mostra a opinião dos entrevistados quanto a garantia do produto, 67,6% (48 participantes) consideraram como muito baixo a médio o risco do produto não ser o mesmo idealizado no momento da compra.

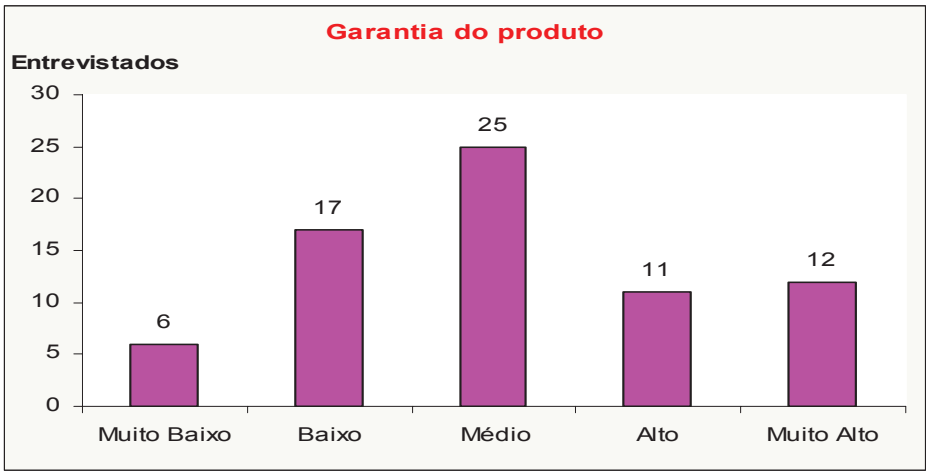

Gráfico 10: Garantia do produto

Pergunta 10: Não conseguir negociar o preço

Na pergunta sobre negociação do preço, 69% (49 paticipantes)dos entrevistados ficaram propensos a médio e muito alto como relata o gráfico 11.

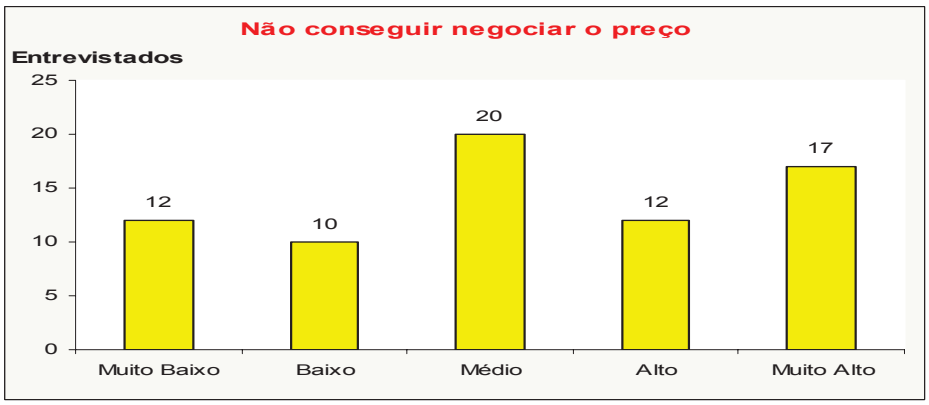

Gráfico 11: Não conseguir negociar o preço

Pergunta 11: Empresa não efetue todas as etapas do processo de compra

Quando abordados quanto a idoneidade da empresa fornecedora do produto via internet, foi constatado que 69% (49 participantes) dos entrevistados assinalaram entre médio e muito alto o risco de a empresa não seja idoneamente correta.

O gráfico 12 apresenta mais claramente os dados expostos.

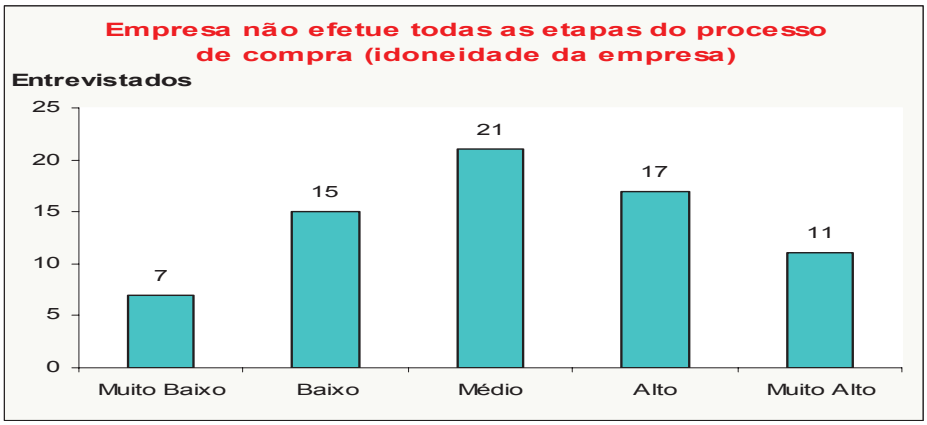

Gráfico 12: Empresa não efetue todas as etapas do processo de compra

Pergunta 12: Demora/Dificuldade em realizar compras

Conclui-se ao analisar o gráfico 13 e levando em consideração que o público pesquisado tem facilidades em navegar na internet, a complexidade do site não foi um agravante para realizar compras pela internet, 71,8% deste público (51 participantes) opinaram entre muito baixo e médio sobre a dificuldade em navegar em um site de e-commerce.

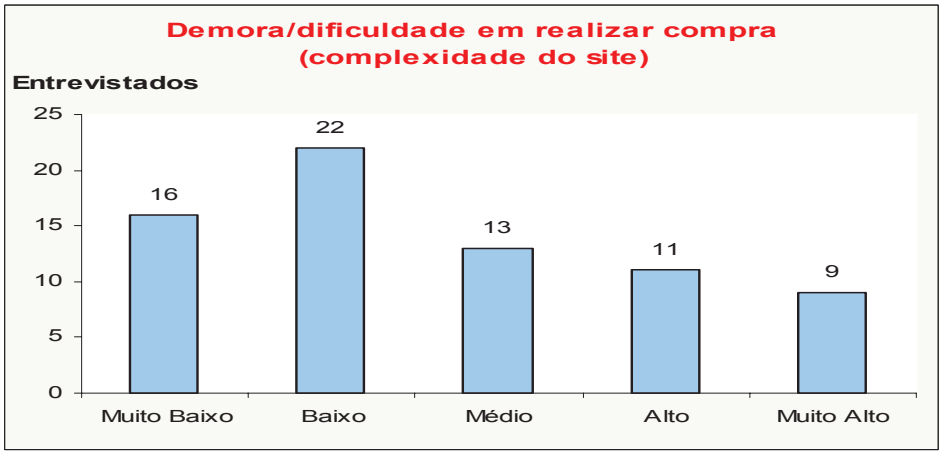

Gráfico 13: Demora/Dificuldade em realizar compras

Pergunta 13: Se não houvesse risco nas transações via internet, você utilizaria a internet para realizar suas compras?

Quando a hipótese da maximização da segurança foi abordada, os entrevistados mostraram-se interessados em continuar/realizar compras via internet. A confirmação desta explanação foi que 93% marcaram "sim" e somente 7% marcaram "não" quanto perguntados sobre tal hipótese, como apresentado no gráfico 14.

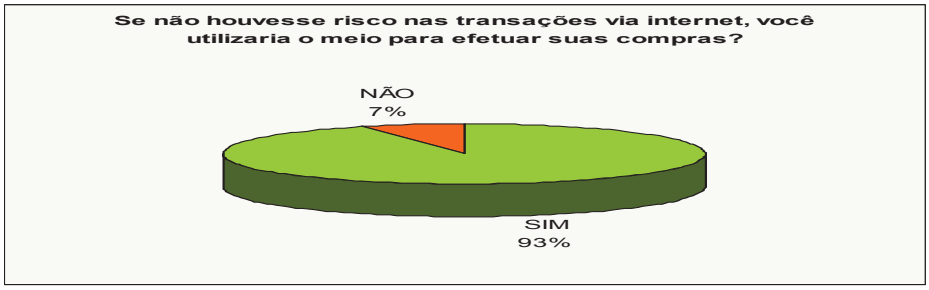

Gráfico 14: Se não houvesse risco nas transações via internet, você utilizaria a internet para realizar suas compras.

De forma geral, o público entrevistado já demonstrava interesse em utilizar o e-commerce como meio de compras, o que validou a pesquisa para a obtenção de resultados reais e mais confiáveis.

Como esperado, os resultados indicaram uma tendência a ressalvas quanto a utilização da internet devido a aspectos de segurança, demonstrados nos gráficos 6 e 7, em que os riscos sentidos pelos entrevistados foram na maioria de médio a muito alto

Da mesma forma, o gráfico 14 demonstra que se as empresas de e-commerce se adequarem às exigências do mercado buscando meios de promoverem maior segurança, tanto para o cliente quanto para o fornecedor durante as transações eletrônicas, um maior número de pessoas continuará e/ou começará a utilizar o meio, como forma de aquisição de bens de consumo viabilizando uma maior adesão das empresas físicas ao meio virtual.

Conclusão

O questionário utilizado para levantamento de dados abordou não somente questões sobre segurança da informação, mas também, marketing, fidelização de clientes, logística, navegação no site e gerenciamento de produtos. Estes tópicos serviram como indicadores, mostrando um cenário de integração da segurança da informação a estes outros tópicos, são pontos relevantes na tomada de decisões em realizar uma transação comercial via e-commerce.

O objetivo deste trabalho foi levantar o risco em segurança da informação nas transações de e-commerce e propor como estratégia a melhoria da segurança através de mecanismos como: criptografia de dados, certificação digital, selo digital, assinatura digital e firewall, estes, capazes de garantir uma maior confiabilidade aos dados trafegados nas redes.

A segurança parece ser um fator chave. Surge assim, a necessidade da adoção de medidas que garantam cada vez mais a proteção de todos os procedimentos de um pedido eletrônico, desde a transmissão até o armazenamento dos dados.

As empresas de e-commerce estão evoluindo e criando novas tendências para atender a demanda de mercado, porém o conhecimento do ambiente de comunicação e suas particularidades como segurança da informação, são fatores fundamentais para o sucesso e sobrevivência destas, neste meio.

Por sua vez, os riscos físicos e da proteção da informação devem ser analisados para a criação de estratégias de redução de risco tanto para os que compram, bem como para os que ainda não compraram através do e-commerce. Os resultados indicam que os riscos influenciam a decisão de adquirir produtos e serviços pela rede, havendo uma relação inversamente proporcional entre risco percebido e a predisposição para a compra por esse meio.

Tendo em vista as informações analisadas por este trabalho, e pelos dados apresentados em relação aos entrevistados, pode-se perceber que o usuário de Internet, que transaciona pela rede, preocupa-se em não disponibilizar suas informações, principalmente quando são financeiras.

A sobrevivência de uma empresa de e-commerce depende uma grande capacidade de inovação, o que exige olhar para o futuro com objetivos traçados, compreender como são as forças sociais, econômicas e tecnológicas que interagem, além de saber articular as competências necessárias. É preciso refletir os desejos do consumidor atual e futuro.

Sintetizo a estratégia em segurança da informação, utilizando ferramentas de proteção da informação transacionada pela rede da internet, como meio para viabilizar a adesão ao e-commerce, as novas tecnologias são uma arma da qual o e-commerce não pode abrir mão.

Referencias Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE PROVEDORES DE INTERNET. **História da Internet.** São Paulo, 2005. Disponível em: http://www.abranet.org.br /historiadainternet/brasil.htm . Acesso em 29/01/2006

AHUJA, V. **Secure Commerce on the Internet**. Academic Press, 1997

ALBERTN, A. L. **Comercio Eletrônico: Modelo , Aspectos, Contribuições de sua aplicação**. 2. ed. São Paulo: Editora Atlas, 2000. *apud* Menezes, H.. **Comercio Eletrônico Para Pequenas Empresas**. 1ª ed.. Florianopolis: BookStore, 2003,p26.

ALMEIDA, L.C.P. **O comércio, a internet e os organismos internacionais: construindo a estrutura do comercio eletrônico**. Rio de Janeiro: CNC, 1999.

BICKMAN, L., ROG, D. J., and HEDRICK, T. E. *Applied* **Research design: a practical approach**. apud: BICKMAN, L.; ROG, D. J. (Ed.). **Handbook of applied social research methods.** Thousand Oaks: Sage Publications, 1997. p.05-37

CASTILHO Filho, A. F. F. **Avaliação do uso de novas tecnologias de informação nas empresas: Internet, Intranet e Extranet. Estudo de casos.** 1998. Dissertação de metrado. São Paulo: Universidade de São Paulo, 1998.

CERT CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTOS EM INCIDENTES EM SEGURANÇA NO BRASIL.**Cartilha de segurança para a internet.** Disponível em: http://cartilha.cert.br/ . Acesso em 10/03/2008

CORRÊA, J B. **E-COMMERCE: Principais Características que Influenciam no Processo de Decisão de Compra Via Internet.** Florianópolis, 2002. 96f. Dissertação (Mestrado em Engenharia da Produção) – Programa de Pós-graduaçâo em Engenharia da Produção, UFSC, 2002

CRUZ, C.; RIBEIRO, U. **Metodologia Científica – Teoria e Prática**. 1ª ed. Rio de Janeiro: Axcel Books 2003. 218p

Curti, J. C, **Análise de segurança em aplicações que utilizam plataformas UNIX e MS-Windows como Clientes e Servidores**. Instituto de Computação
Universidade Estadual de Campinas, 2004.

ENGEL, J. F.; BLACKWELL, R. D. e MINIARD, P. W. **Consumer Behavior**. 8. ed. Orlando: The Dryden Press, 1995. 951 p. Bibliografia: p. 441- 442. ISBN: 0030984645.

FERRO, W. R. **Comércio Eletrônico e a Segurança da Rede: Uma Visão Tecnológica.** VI Semead - Seminários em Administração FEA-USP 11 e 12 de
Agosto de 2003.Disponível em:http://www.ead.fea.usp.br/Semead/6semead/index.htm.
Acesso em : 16/01/2006.

FIGUEIREDO, A., **Administração de Sistemas e Segurança**. Revista Unicamp, nº 6, Setembro de 1999. Disponível na Internet pelo endereço http://www.revista.unicamp.br/infotec/admsis/admsis6-1.html. Acesso em 16/01/2006.

Filho, A. A. S. **Comércio Eletrônico: Marketing, Segurança, Aspectos Legais e Logística**. Mosoró, 2000.225p. Dissertação para obtenção do Título de Mestre em Engenharia da Produção - Universidade Federal de Santa Catarina, SC

GIGLIO, E. **O comportamento do consumidor e a gerência de marketing**. São Paulo: Pioneira, 1996.

Gonçalves, C F; SOARES, F C; ALBERTO, C et al. Comércio **Eletrônico na Internet: Uma Pesquisa Exploratória no Mercado Consumidor**. Encontro Nacional da ANPAD, 1998. Anais... CD- ROM.

Gonçalves, A., BARROS, A. C., RIBEIRO, D., COSTA,L.. **Comércio Electrónico**. Universidade do Minho, 1999.

Kiani, G. **Marketing opportunities in the digital world**. *Internet Research*, v. 8, p. 185-194, 1998.

KOTLER, P. **Administração de Marketing**. 10ª ed. São Paulo: Pearson. 2004. p 681

KOSIUR, D. **Understanding Electronic Commerce: How Online Transations Can Grow Your Business**. Washington. Microsoft Press, 1997. *apud*

Kovacs, M. H., SALOMÃO A. F. **Dimensões de riscos percebidos nas compras pela Internet.** RAE-eletrônica, v. 3, n. 2, Art. 15, jul./dez. 2004.
Disponível em:
http://www.rae.com.br/eletronica/index.cfm?FuseAction=Artigo&ID=1807&Secao=MERCADO&Volume =3&Numero=2&Ano=2004. Acesso em 10/01/2006

Lasch, Erin. **Do you trust the web?** Ohio CPA Journal, Columbus, v.57, n.4, p.8-11, oct./dec. 1998. ISSN: 07498284

LEE – Laboratório de epidemiologia e estatistica. **Pesquisa** Disponível em: http://www.lee.dante.br/pesquisa/amostragem/que_amostragem.html. Acesso em: 20/01/2005.

MARCIO, A. **A Internet e os Hackers. Ataques e Defesas.** 5ª ed. São paulo: Editora Chantal, 2000. 195p. ISBN: 8587173049

Menezes, H. **Comercio Eletrônico Para Pequenas Empresas**. 1ª ed.. Florianópolis: BookStore, 2003,192p.

MICROSOFT. **Páginas e Controles ASP.NET Seguros.** Disponível em: www.microsoft.com/.../ devsec/secmod83.mspx. Acesso em 29/01/2006

PEREIRA, M. A. **Internet: Introdução e Conceitos**. Disponível em: http://www.marco.eng.br/matematica/Aula%201_arquivos/frame.htm . Acesso em: 29/01/2006

PISTELLI, D. **Criptografia.** UFRJ, 1999. Artigo disponível em: http://www.nucc.pucsp.br/novo/cripto/cripto.html

Rohm, A. J. e Milne, G. R. Emerging **marketing and policy issues in electronic commerce: attitudes and beliefs of Internet users**. Marketing and Public Policy Proceedings, v.8, p. 73-79, 1998, *apud*: Kovacs, M. H., SALOMÃO A. F. **Dimensões de riscos percebidos nas compras pela Internet.** RAE-eletrônica, v. 3, n. 2, Art. 15, jul./dez. 2004. Disponível em: http://www.rae.com.br/eletronica/index.cfm?FuseAction=Artigo&ID=1807&Secao=MERCADO&Volume =3&Numero=2&Ano=2004. Acesso em 10/01/2006

SANTOS, S. C. dos. **Introdução ao Comercio Eletrônico**. *apud* Menezes, H. Comercio Eletrônico Para Pequenas Empresas.1ª ed.. Florianópolis: Editora BookStore, 2003. p.26.

SIEBER, J. E. **Planning ethically responsible research**. *apud*: BICKMAN, L.; ROG, D. J. (Ed.). **Handbook of applied social research methods**. Thousand Oaks: Sage Publications, 1997. p.127-159.

SPECTOR, R. **Amazon.com: como crescer da noite para o dia: os bastidores da empresa que mudou o mundo.** 1ª ed. Rio de Janeiro: Editora Campus, 2000. 234p.

STALLINGS, W. **Cryptography and Network Security: Principles and Practice.** 2. ed. New Jersey: Prentice Hall, 1999.

STINSON, D. R. Cryptography: Theory and Practice. Florida: CRC Press LLC, 1995. *apud* Menezes, H. Comercio Eletrônico Para Pequenas Empresas.1. ed.. Florianópoli: BookStore, 2003. p.35-36.

Solomon, M. R., **Consumer behavior: buying, having and being**. 4. ed. New Jersey: Prentice Hall, 1998. 640 p. Bibliografia: p. 280-281 ISBN:0137957254. *apud*: Kovacs, M. H., SALOMÃO A. F. **Dimensões de riscos percebidos nas compras pela Internet.** RAE-eletrônica, v. 3, n. 2, Art. 15, jul./dez. 2004. Disponível em: http://www.rae.com.br/eletronica/index.cfm?FuseAction=Artigo&ID=1807&Secao=MERCADO&Volume=3&Numero=2&Ano=2004. Acesso em 10/03/2008

TANENBAUM, A.S. **Redes de Computadores**. 4. ed. Rio de Janeiro: Campus, 1997.

TELECO – INFORMAÇÃO EM TELECOMUNICAÇÕES. **Usuários de Banda Larga e Internet no Brasil**. Disponível em: http://www.teleco.com.br/comentario/com94.asp Acesso em 10/03/2008

TURBAN, E., et al. **Eletronic Commerce: a managerial Perspective**. New Jersey: PHI, 1999. *apud* Menezes, H. **Comercio Eletrônico Para Pequenas Empresas.**1. ed.. Florianópolis: BookStore, 2003. p.26.