UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DE NEGÓCIOS FINANCEIROS

Cristiano Reicher

SEGURANÇA DA INFORMAÇÃO NO ACESSO AO INTERNET BANKING

Porto Alegre
2011

Cristiano Reicher

SEGURANÇA DA INFORMAÇÃO NO ACESSO AO INTERNET BANKING

Trabalho de conclusão de curso de Especialização apresentado ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Especialista em Gestão de Negócios Financeiros.

Orientadora: Profª. Drª. Ângela Freitag Brodbeck

Porto Alegre

2011

Cristiano Reicher

SEGURANÇA DA INFORMAÇÃO NO ACESSO AO INTERNET BANKING

Trabalho de conclusão de curso de Especialização apresentado ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Especialista em Gestão de Negócios Financeiros.

Aprovado em ___ de novembro de 2011.

BANCA EXAMINADORA:

_____

Prof.

_____

Prof.

Dedico este trabalho primeiramente a Deus, que nos dá força para seguir em nossos objetivos. Aos meus pais Udo e Marlene, pela dedicação e educação, e em especial a minha esposa Charlene que sempre esteve me apoiando e incentivando a chegar até aqui.

AGRADECIMENTOS

Agradeço a toda minha família, e em especial minha esposa Charlene Brunel Serafim Reicher, pela força e paciência.

A todos os professores que por todo esse tempo estiveram dispostos a repassar seus conhecimentos, e em especial ao apoio prestado durante a realização deste Trabalho de Conclusão de Curso.

Ao Banco do Brasil S.A. e a Universidade Federal do Rio Grande do Sul pela oportunidade de realização deste curso.

RESUMO

As inovações tecnológicas e o grande avanço que a internet teve nas últimas décadas revolucionaram o sistema financeiro, os investimentos em tecnologia geram redução de custos, vantagem competitiva e consequentemente maiores lucros. O objetivo das Instituições Financeiras é cada vez mais atrair seus clientes ao ambiente virtual, o Internet Banking, eliminando em muitos momentos a presença física nas agências. Junto com esta tendência vêm a preocupação com a segurança da informação nas transações realizadas, manter seguro e em sigilo os dados de pessoas e empresas é fundamental para que este processo se mantenha em crescimento. Assim, este estudo tem por objetivo principal identificar a percepção dos clientes bancários que realizam transações financeiras através do Internet Banking quanto à sua importância e responsabilidade para garantia de um acesso seguro e confiável. Para o levantamento de dados foi utilizada a estratégia de pesquisa qualitativa, através do método de estudo de caso. Diante dos resultados obtidos durante a pesquisa, chegou-se ao objetivo proposto, constatando os compromissos e a percepção dos clientes quanto a sua importância para a segurança no acesso ao Internet Banking.

Palavras-chave:

Internet Banking, Segurança da Informação, Instituição Financeira

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

As mudanças tecnológicas proporcionadas pela evolução da internet nas últimas décadas trouxeram para os clientes dos bancos muito mais facilidade e praticidade na realização de suas transações bancárias. O uso da internet para tais transações vem sendo aperfeiçoado e aprimorado a cada dia. Segundo pesquisa realizada pela Federação Brasileira dos Bancos FEBRABAN (2011), em 2010, os gastos com tecnologia pelas instituições financeiras avançaram 15% em relação a 2009, totalizando R$ 22 bilhões. O número de adeptos ao seu uso também aumentou na mesma velocidade, o mesmo levantamento aponta um aumento em quase 20% ao ano do uso do Internet Banking, aproximadamente 23% do total das operações bancárias já são realizadas por este canal, totalizando cerca de 56 bilhões de operações em 2010. A frequência também é alta, cerca de 50% dos usuários fazem uso deste serviço de uma a duas vezes por semana.

Através do Internet Banking, como é chamado o canal de acesso dos clientes às informações bancárias pelo site das instituições financeiras, são realizadas diversas transações, como transferir valores entre contas correntes, efetuar pagamentos, realizar aplicações financeiras, obter extratos e empréstimos, dentre outros, tudo de forma on-line. O uso deste canal traz diversos benefícios a quem o utiliza, permite ganho de tempo e comodidade, realizando suas tarefas bancárias de qualquer lugar com acesso a internet e em horários flexíveis. Uma preocupação que acompanha esta tendência é a segurança da informação na internet, principal questão de estudo deste trabalho. A segurança dos dados utilizados nas transações, sua confiabilidade e privacidade são preocupações que devem ser alvo de constantes atualizações por parte de quem presta o serviço e, principalmente, do usuário, que deve adotar uma série de providências e cuidados para que seus dados não sejam violados.

Diagnosticando todas as facilidades e benefícios trazidos pelo uso do Internet Banking, o esforço e os investimentos dos bancos na melhoria da segurança neste canal alternativo e acompanhando diretamente o comportamento e as transações realizadas pelos clientes bancários, no dia a dia das agências, percebe-se que grande parte deles não têm ciência da sua importância quanto às providências e cuidados necessários para um acesso seguro e confiável.

Diante dos fatos verificados, a questão de pesquisa centra-se no seguinte aspecto: **Qual a percepção dos clientes pessoa jurídica da cidade de Joinville/SC quanto à sua responsabilidade perante a segurança no acesso ao Internet Banking?**

1.1 OBJETIVOS

O objetivo geral deste estudo é identificar a percepção dos clientes pessoa jurídica que realizam transações financeiras através do Internet Banking quanto à importância e sua responsabilidade para garantia de um acesso seguro e confiável em agências bancárias da cidade de Joinville/SC.

Já os objetivos específicos são os seguintes:

1. Classificar os métodos mais utilizados por terceiros para ataques e invasões de informações bancárias;
2. Descrever e comparar os mecanismos de segurança adotados pelos bancos para viabilizarem um acesso seguro aos seus clientes;
3. Relacionar os métodos e procedimentos necessários para que os clientes bancários realizem seus acessos com total segurança.
4. Verificar o perfil dos usuários deste serviço, perfil da empresa por qual faz o acesso e a frequência com que é realizada;
5. Identificar o nível de conhecimento dos clientes que utilizam o Internet Banking quanto aos procedimentos de segurança e se faz uso das medidas indicadas.

1.2 JUSTIFICATIVA

A importância desta pesquisa se dá pelo fato de que a adoção de cuidados específicos em relação à segurança da informação é importante e fundamental para que o acesso ao Internet Banking seja seguro e confiável, evitando danos negativos aos clientes e ao bancos. As instituições financeiras investem constantemente em mecanismos, aplicativos e atualizações para proporcionar esta segurança. Mas esta função não é somente deles, depende

muito do conhecimento e comportamento dos clientes perante suas ações no acesso a internet e ao canal de atendimento a sua conta.

Além disso, o estímulo ao uso deste canal alternativo é de suma importância para o Sistema Bancário, pois através dele, os clientes podem efetuar todas as suas transações bancárias, tudo de forma on-line. Desta forma, o atendimento presencial realizado nas agências torna-se menor nos aspectos operacionais, diminuindo custos e direcionando sua estrutura e mão-de-obra para os negócios. Também trazendo uma comodidade e praticidade aos clientes.

Outro aspecto que torna relevante a questão de pesquisa é o fato de existirem poucas publicações a respeito dos métodos e providências que os usuários do Internet Banking devem tomar para usufruírem deste serviço com segurança as suas informações e transações. Podendo desta forma mostrar que através de alguns cuidados essenciais, o seu uso é tão seguro como os meios tradicionais. Demonstrando como funciona e seus meios de segurança, o número de clientes adeptos ao uso deste serviço tende a crescer cada vez mais.

Visando atingir os objetivos propostos, a estratégia de pesquisa utilizada será a qualitativa, através do método de estudo de caso.

1.3 ESTRUTURA DO TRABALHO

O trabalho está estruturado da seguinte forma, após este capítulo de introdução são apresentados os principais conceitos em relação ao tema estudado. No capítulo 3 são apresentados os itens relacionados ao método de pesquisa utilizado, forma de coleta de dados, amostra e análise dos dados. Na sequência são apresentadas as análises destes dados. E, por fim, no capítulo 5, são feitas as considerações finais do trabalho e indicações para pesquisas futuras, bem como das limitações desta pesquisa.

2 SEGURANÇA DA INFORMAÇÃO NO ACESSO AO INTERNET BANKING

Este capítulo tem como finalidade fornecer base teórica necessário ao bom entendimento do tema proposto, incluindo os aspectos gerais de segurança da informação, segurança de computadores, Internet Banking e métodos de ataque pela internet. São apresentados também os métodos de segurança utilizados pelos bancos e os cuidados que os usuários devem tomar para tornar seu acesso financeiro na internet seguro.

2.1 CONCEITO DE SEGURANÇA DA INFORMAÇÃO

Diariamente, no mundo inteiro, redes de computadores, servidores e computadores pessoais estão sendo invadidos. A qualidade e o nível de sofisticação destes ataques variam amplamente; enquanto geralmente acredita-se que a maioria das invasões tem sucesso devido às senhas fracas ou um descuido do usuário, há ainda um grande número de ataques que usam técnicas cada vez mais avançadas. No Brasil, diversos sites oficiais do governo federal sofreram invasões. No decorrer do ano de 2011, foram alvos de ataques os endereços da Presidência da República, do Ministério dos Esportes, Receita Federal, Petrobrás, entre outros.

A Segurança da Informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto as pessoais, segundo Clesio, (2008). Ela tem como finalidade garantir a disponibilidade, sigilo, integridade, autenticidade e controle de acesso das informações, como cita Sêmola, (2003). A Segurança da Informação dá a garantia de que a mesma estará disponível para acesso no momento desejado. Ela tem como objetivo a preservação de três princípios básicos:

> **Confidencialidade**: toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso de apenas às pessoas para quem elas são destinadas.
> **Integridade**: toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
> **Disponibilidade**: toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade (SÊMOLA, 2003).

Deve-se ter a consciência de que não existe sistema seguro em todos os aspectos. De acordo com Oliveira (2001): “o único sistema totalmente seguro é aquele que não possui nenhuma forma de acesso externo, está trancado em uma sala totalmente lacrada” Todo e qualquer sistema que tenha algum acesso ou informação externa está vulnerável a algum tipo de ameaça a sua segurança.

De acordo com Cunha (2005), são definidos como ameaças os agentes ou condições que venham a causar incidentes que comprometam as informações por meio da exploração de vulnerabilidade, podendo assim provocar perdas de confidencialidade, integridade e disponibilidade, como consequência, causando impactos aos negócios de uma organização. Tais ameaças podem ser classificadas quanto a sua intencionalidade, sendo divididas nos seguintes grupos:

a) **Naturais** – ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc;
b) **Involuntárias** – ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, etc;
c) **Voluntárias** – ameaças propositais causadas por agentes humanos como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Segundo Oliveira (2001), “o risco sempre vai existir, assim como existe na nossa vida fora dos bits e bytes. A questão é trazer o “grau de risco” a um nível aceitável, de modo que possamos evoluir na utilização da tecnologia até um patamar mais confiável e, consequentemente, mais eficaz”.

2.2 SEGURANÇA DE COMPUTADORES

De acordo com CERT.BR (2006) podemos dizer que um computador é seguro quando ele atende a três requisitos básicos da segurança da informação. Como exemplos de violações para cada um destes requisitos podemos citar:

a) Confidencialidade: alguém tem acesso a seu computador, sem sua autorização e lê informações confidenciais de sua declaração de imposto de renda, por exemplo.

b) Integridade: alguém tem acesso a seu computador, sem sua autorização e altera informações da sua declaração de imposto de renda, por exemplo.
c) Disponibilidade: seu provedor acaba sofrendo uma grande sobrecarga de dados ou algum ataque de navegação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de imposto de renda.

Segundo Oliveira (2001), os principais atentados a segurança que podemos sofrer usando nosso computador pessoal são os ataques à privacidade, quando temos os nossos dados pessoais, como documentos e fotos visualizados por um hacker; destruição, quando temos nossos dados gravados no computador destruídos por um hacker, ou por um ataque de vírus ou programas com função semelhante; ou ainda, obtenção de vantagens: é o mais comum e preocupante, acontece quando são tiradas vantagens financeiras através de um ataque a computadores pessoais.

Deve-se ter uma preocupação bastante grande com a segurança dos computadores, pois estes são utilizados para realizar inúmeras tarefas, como comunicação: através de e-mails ou mensagens instantâneas; armazenamento de dados, sejam eles pessoais ou comerciais; e principalmente transações financeiras, sejam estas transações bancárias ou compra de produtos e serviços pela internet.

Esta preocupação e cuidado são importantes para que não se tenha senhas e números de cartões de crédito furtadas e utilizadas por terceiros, conta de acesso a internet utilizada por alguém não autorizado, dados pessoais ou comercias alterados ou destruídos, transações bancárias realizadas indevidamente ou até com o computador deixando de funcionais, por ter sido comprometido e arquivos essenciais terem sido apagados. (CERT.BR, 2006)

Como citado por Wikipedia (2011), para evitar as ameaças de invasões existem alguns mecanismos de segurança que garantem o sigilo e proteção as informações, elas podem ser classificadas em controles físicos, que são barreiras que tem por objetivo limitar o acesso ou contato direto a informação e em controles lógicos que são barreiras que procuram impedir ou limitar o acesso a informação por meio eletrônico.

Como exemplos de mecanismos de controles físicos podemos citar: portas, paredes, trancas, blindagens, etc. E como exemplos de mecanismos de controles lógicos: Mecanismos de criptogtafia, assinatura digital, mecanismos de controle de acesso, protocolos de segurança, etc.

Todo usuário de computador com acesso a internet, seja com fim pessoal ou profissional, deve estar atendo ao seu uso correto para evitar a exposição de dados pessoais ou

danos financeiros, utilizando de forma consciente e verificando os mecanismos de segurança existentes.

2.3 INTERNET BANKING

O investimento em tecnologia pelos bancos, no Brasil, traz um aumento na sua gama de produtos e serviços, também traz diversificação aos pontos de contato com o cliente. O Internet Banking é um destes canais de contato, sendo o que mais cresce dentre os canais eletrônicos de auto-atendimento. (D‟ANDRÉA et al, 2000). Banco Eletrônico, como também são conhecidos os canais de auto-atendimento são compostos pelo caixa eletrônico, atendimento telefônico, home e office Banking e Internet Banking. Souza (2000) traz a sua definição:

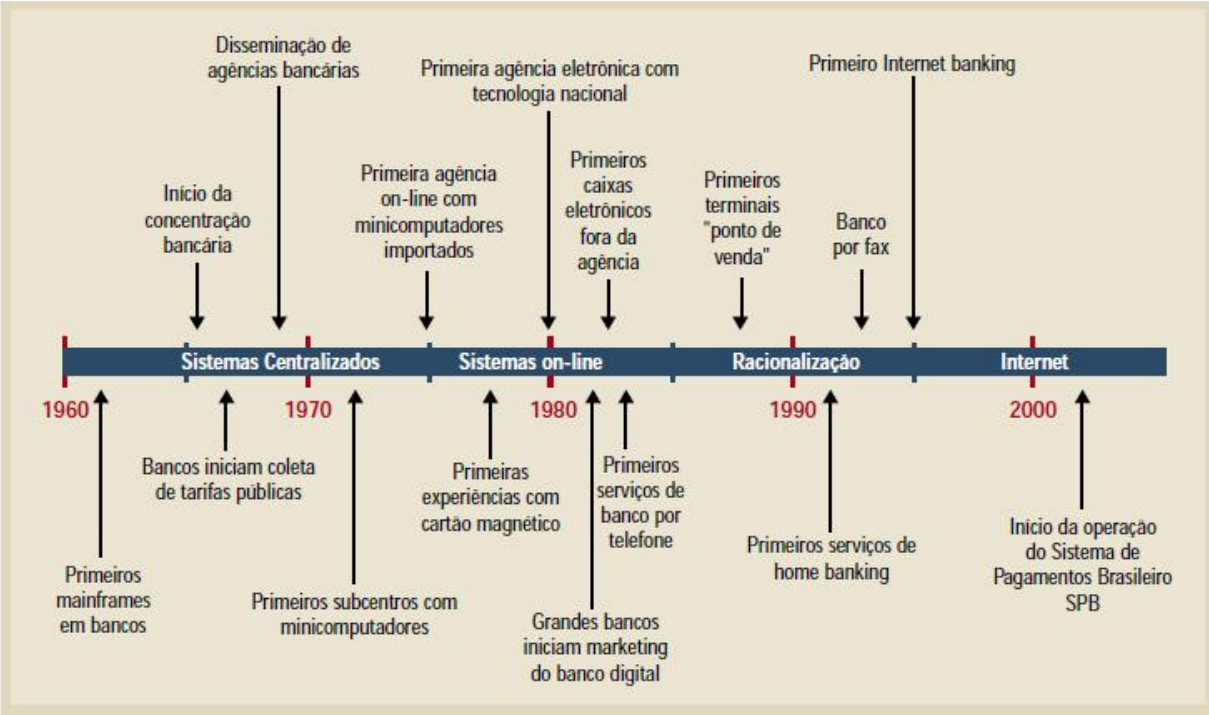
> "O Banco Eletrônico é um conjunto de produtos e serviços suportado por modernas ferramentas tecnológicas e realizado com baixa interferência humana. Restrito inicialmente aos caixas eletrônicos, cresce a cada dia pela implementação de produtos como o home, o office e o Internet Banking, a ponto de não haver mais sentido pretender-se delinear suas fronteiras com o que alguns chamam de 'banco tradicional'". (SOUZA, 2000, p. 5).

Ao longo dos avanços tecnológicos ocorridos a partir de 1965, as instituições financeiras se transformaram, foram impulsionadas pela reforma bancária, decretada pelo governo militar brasileiro, com esta reforma, o Estado pretendia ajusta o sistema financeiro ao mesmo estádio de desenvolvimento que já era observado na indústria (DINIZ, 1994).

Conforme Diniz (2004), na década de 70, o desenvolvimento tecnológico do país teve um papel importante dos bancos, tais instituições investiram bastante em desenvolvimento de sua área de informática. Os clientes bancários desta década até a metade da década de 80 demandavam eficiência e rapidez do sistema financeiro nacional. Mais recentemente, as transformações que ocorreram foram denominadas de Economia Digital, um novo modelo de atuação bancária, no qual a internet tem um papel fundamental na evolução de novas formas de atuação e relacionamento com o cliente. O primeiro Internet Banking surgiu no ano de 1995, com a internet ainda no modo discado. Com o avanço da tecnologia, hoje com conexões extremamente mais rápidas, os sistemas de acesso evoluem a cada dia.

O mesmo autor traz em sua publicação uma ilustração desta evolução bancária brasileira, demonstrada na figura abaixo.

Figura 1 – Fase de automação bancária no Brasil



Fonte: DINIZ (2004)

O termo Internet Banking pode ser considerado novo e até mesmo desconhecidos para uma parte da população. Trata-se do nome dado ao serviço disponibilizado pelas Instituições Financeiras para que seus clientes possam realizar suas transações bancárias através da internet. De acordo com Lau (2006), "é uma opção adicional aos clientes de bancos que buscam realizar transações bancárias em qualquer localidade, onde se dispõe de um computador e conectividade com a internet".

A comodidade e a tranquilidade na realização das transações bancárias, têm atraído cada vez mais clientes a utilização deste serviço, pois esta ferramenta permite realizar diversas transações através de um computador pessoal, sem sair de casa, bastando estar conectado a internet. Dentre as transações que podem ser realizadas seguem alguns exemplos: transferência de valores entre contas correntes, efetuar pagamentos, emitir DOC/TEC, realizar aplicações financeiras, obter empréstimos e extratos, dentre outros.

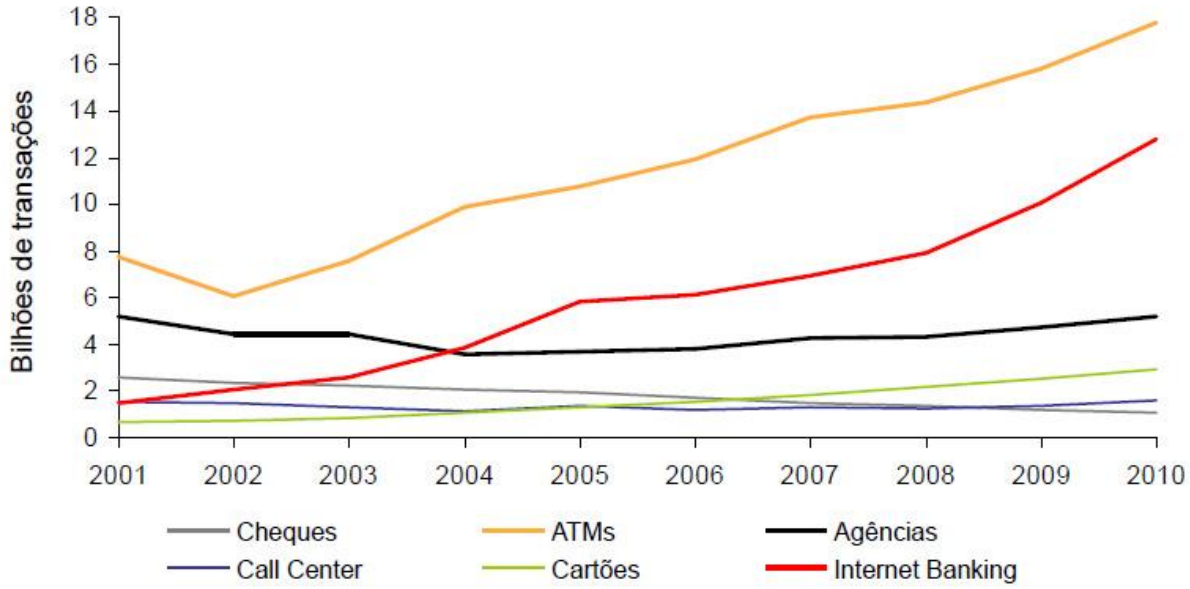
Os bancos têm investido muitos recursos em tecnologia, seja para ampliar a área geográfica de atendimento, para diminuir os seus custos ou ainda para proporcionar conveniência a seus clientes. (DINIZ, 2000).

Informações da Federação Brasileira de Bancos FEBRABAN (2011) dão conta de que as pessoas estão cada vez mais usando os sites dos bancos para realizar suas transações bancárias, pelo menos uma em cada quatro transações já são feitas pela internet. São cerca de

23% do total de transações realizadas, que é de 56 milhões. Os investimentos feitos com tecnologia da informação pelos bancos em seus sites também são altos, passaram dos 22 bilhões de reais no último ano.

Destaca-se abaixo um comparativo da FEBRABAN (2011) com a evolução do número de transações bancárias por cada canal de origem do atendimento.

Figura 2 – Transações bancárias por origem



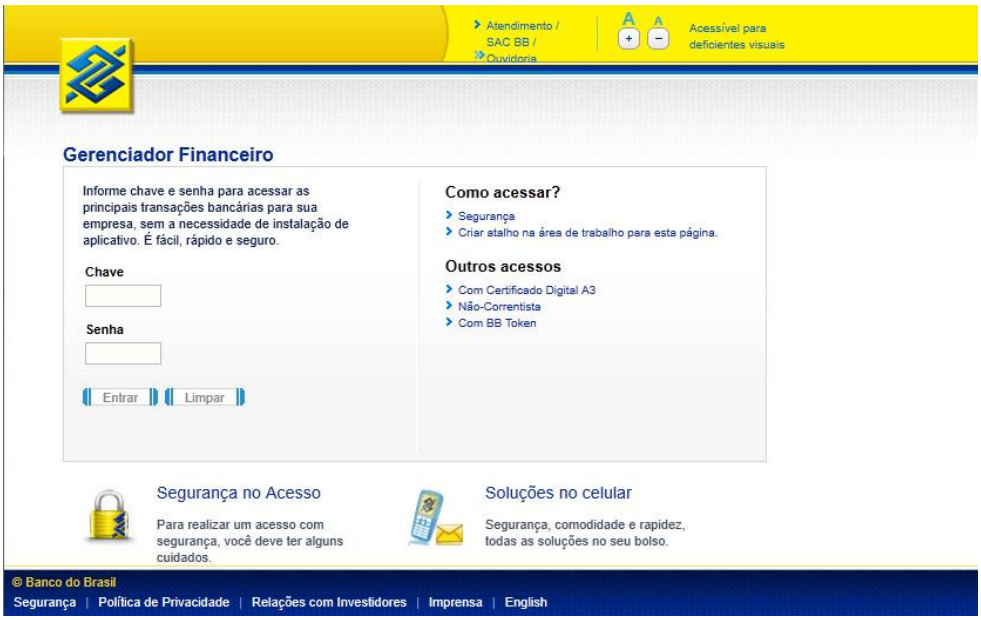
Fonte: FEBRABAN (2011)

O comparativo nos mostra que o Internet Banking ultrapassou o atendimento pelas agências em número de transações, em meados de 2004, e vem crescendo constantemente nos últimos anos. Dados da FEBRABAN (2011) indicam que com o ritmo de crescimento do internet banking este será o meio mais utilizado para transações bancárias em um futuro próximo.

A mesma pesquisa da FEBRABAN (2011), traz dados interessantes sobre a evolução da utilização do Internet Banking, informa que os clientes que utilizam a internet como canal de atendimento têm crescido mais rápido do que o número de contas correntes.

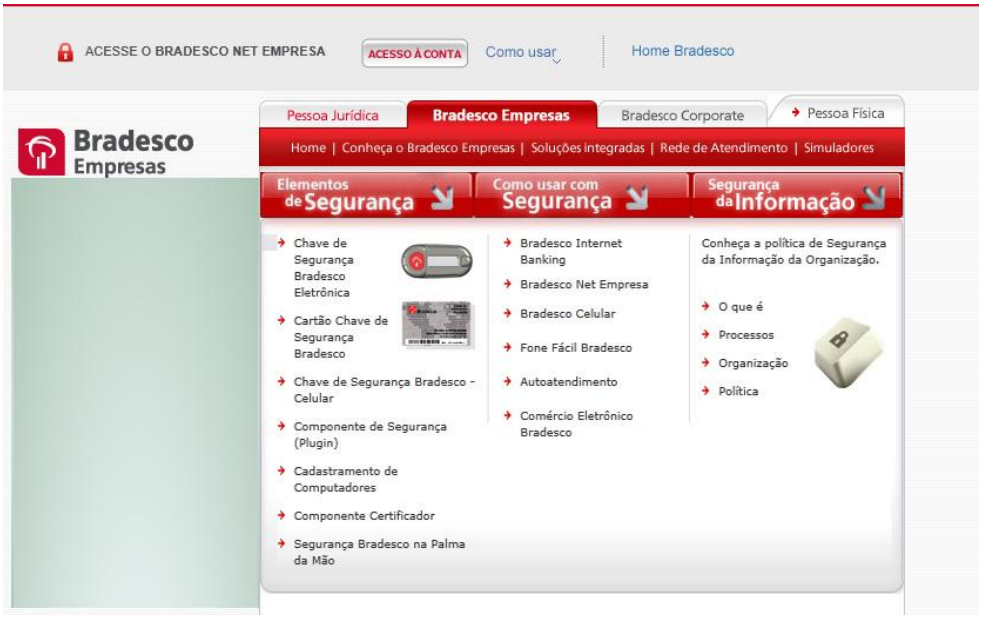
É relacionado em seguida imagens com o modelo da página de acesso do Internet Banking para clientes pessoa jurídica, utilizados atualmente por dois dos maiores bancos brasileiros.

Figura 3 – Acesso ao Internet Banking Banco do Brasil



Fonte: https://aapj.bb.com.br/aapj/loginpfe.bb

Figura 4 – Acesso ao Internet Banking Banco Bradesco



Fonte: http://www.bradescopessoajuridica.com.br/SitePJ/default.aspx

Este benefício e comodidade necessitam de cuidados específicos quanto à segurança nas transações, que será exemplificado a seguir. Podemos notar que em ambas as páginas de acesso, os bancos trazem informações quanto à segurança no acesso, mostrando o compromisso e a preocupação das instituições quanto ao assunto.

2.4 SEGURANÇA NO USO DO INTERNET BANKING

A principal preocupação dos bancos e dos clientes quanto ao acesso e utilização de suas transações bancárias através do Internet Banking são a segurança de seus dados e movimentações financeiras.

Esta preocupação tem um fundamento. Segundo Weber (1999), a Internet foi projetada visando fornecer conectividade entre computadores para uma comunidade restrita de usuários que confiavam mutuamente entre si, ela não foi projetada para um ambiente comercial, para tráfego de informações valiosas ou sensíveis, ou para resistir a ataques mal-intencionados.

A Federação Brasileira dos Bancos FEBRABAN (2011) afirma que os bancos brasileiros investem valores expressivos em segurança. De acordo com informações divulgadas pela Federação, R$9,4 bilhões é o valor gasto anualmente tanto em sistemas de segurança física quanto em segurança eletrônica. Ela destaca também que as instituições financeiras atuam em estreita parceria com governos, as polícias e também com o Judiciário, para evitar e combater crimes. A FEBRABAN possui uma equipe especializada em segurança, trata-se da Comissão de Segurança Bancária, que afirma propor, constantemente, novos padrões de proteção aos usuários e funcionários.

Os bancos seguem, rigorosamente, as leis e sua regulamentação, como por exemplo, a obrigatoriedade de haver um plano de segurança, submetido à Polícia Federal, em todos os postos de atendimento e agências.

Mesmo com todo este investimento e preocupação, os casos de tentativas e sucessos em fraudes pela internet acontecem frequentemente. Percebendo qualquer vulnerabilidade nos sistemas, os *crackers*, realizam invasões em servidores de empresas e computadores pessoais, podendo se apropriar de informações sigilosas ou progredir para uma ação de roubo financeiro via internet.

De acordo com RODRIGUES (2010), pesquisa realizada pela FEBRABAN revelou que golpes online causaram prejuízos de 900 milhões de reais em 2009. No primeiro semestre de 2010, esse número foi de 450 milhões de reais. Considerando a proporcionalidade com 2009, nota-se que este número não tem aumentado, isto é importante, pois o número de acessos cresce a cada ano. Cerca de apenas 0,001% dão algum problema, incluindo fraudes, afirma a FEBRABAN.

2.5 FRAUDES NO INTERNET BANKING

A fraude na internet pode ser definida como a distorção intencional da verdade de um fato, visando a obtenção de lucro ilícito, utilizando os serviços da rede, tais como, mensagens eletrônicas, salas de bate papo e sites disponíveis na internet. (LAU, 2006).

Com o desenvolvimento avançado do ambiente da internet, surgiram diversas pessoas especializadas em ataques às informações em trânsito ou armazenadas por organizações ou usuários. Os mais conhecidos são os *hackers* e *crackers*, que utilizam de vários métodos e tipos de ataques para atingirem seus objetivos, sejam eles apenas de informações sigilosas ou financeiros.

De acordo com Garcia (2011), os ataques a sites de serviços de bancos pela internet aumentaram 45% entre julho e setembro de 2011, na comparação com igual período de 2010. Os números indicam que o golpe do phishing (roubo de senhas bancárias e de cartão) avança, exige cautela redobrada do usuário do serviço e provoca transtornos e prejuízos para empresas. Notificações sobre Cavalos de Troia (expediente usado para furtar informações e credenciais) respondem por 43% dos registros de tentativa de fraude. Essa categoria teve queda de 9% de junho a setembro em relação ao trimestre anterior, mas sofreu aumento de 18% se comparada a igual período de 2010.

2.5.1 Métodos de Ataques

Os métodos de ataque considerados mais comuns utilizados atualmente são a engenharia social e a utilização de *spans.*

De acordo com o CERT.BR (2006), nos ataques de engenharia social, normalmente, o atacante se faz passar por outra pessoa e utiliza meios, como uma ligação telefônica ou e-mail, para persuadir o usuário a fornecer informações ou realizar determinadas ações, muitas vezes abusando da ingenuidade ou confiança do usuário.

O termo *spam*, segundo ANTISPAM.BR (2011), é usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *Unsolicited Commercial E-mail*).

2.5.2 Tipos de Ataques

Existem dois tipos básicos de ataques na tentativa de fraudar os clientes dos bancos que utilizam a internet para suas transações, são eles: *scam* e *phishing*.

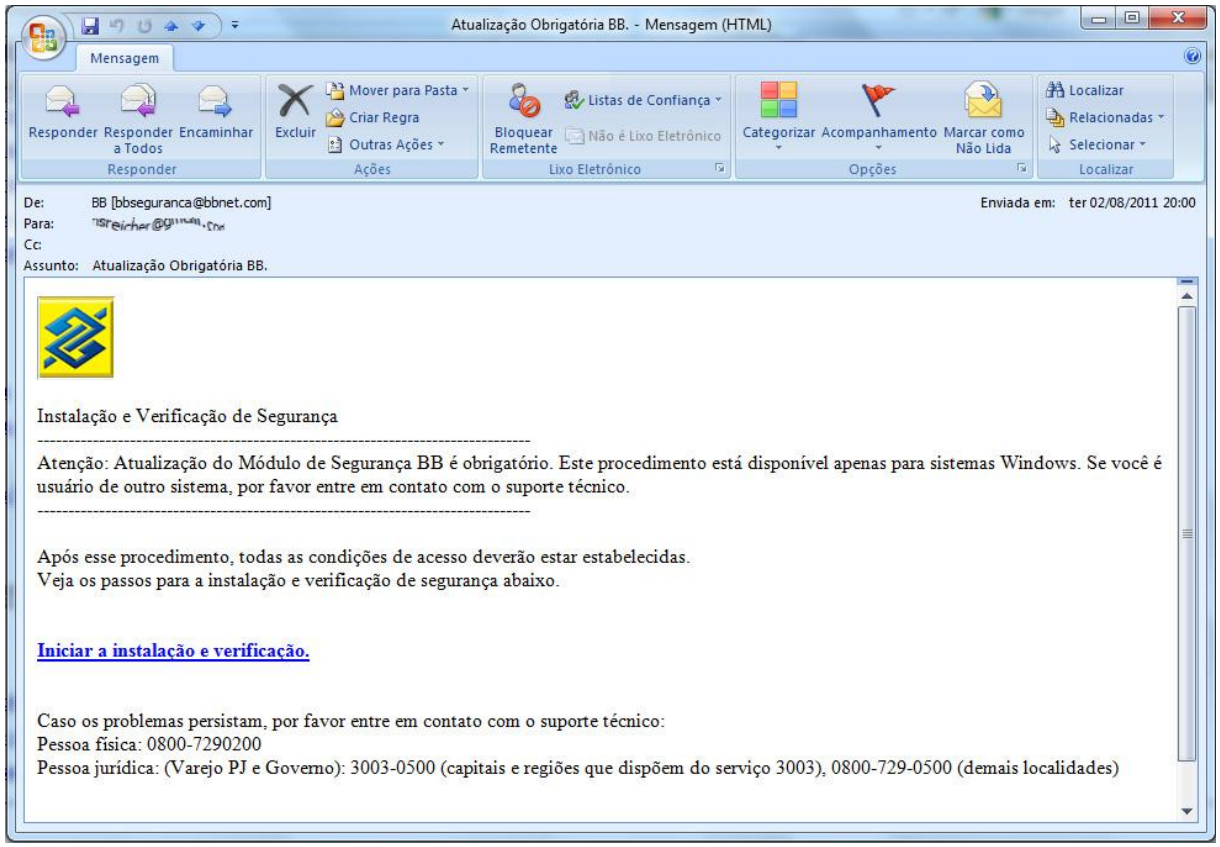
O *scam* é considerado qualquer esquema ou ação fraudulenta ou enganosa que tem como finalidade obter algum tipo de vantagem financeira. O mais comum é o recebimento de e-mails de produtos com preços bem atrativos, no qual o usuário faz a compra e recebe um produto que não condiz com o qual ele adquiriu e na maioria dos casos nem recebe. (CERT.BR, 2006).

Phishing, também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários. O termo também é usado para se referir a mensagens que procuram induzir o usuário a instalação de códigos maliciosos ou mensagens que no próprio conteúdo apresentam formulários para o preenchimento e envio de dados pessoais. (CERT.BR, 2006). São listados abaixo alguns exemplos *phishing:*

a) Cartões e Mensagens;
b) Notificações Financeiras e Cadastrais;
c) Informações/Notícias Bombásticas e Apelos Dramáticos;
d) Download de Programas;
e) Prêmios, Promoções e Campanhas;
f) Temas Adultos e Erotismo;
g) Governo e Serviços Públicos;
h) Telecomunicações;
i) Bancos e Crédito;
j) Comércio eletrônico;
k) Mensagem Internacional.

A figura apresentada a seguir representa um *phishing* recebido em nome do Banco do Brasil, via e-mail, com o título: Atualização Obrigatória BB, solicitando uma instalação e verificação de Segurança através da atualização do Módulo de Segurança BB.

Figura 5 – Exemplo de mensagem de *phishing* enviada em nome do Banco do Brasil



Fonte: Autor

É interessante verificar a utilização do nome, marca e centrais de atendimentos, todos verdadeiros, a diferença é que os bancos não encaminham e-mails deste tipo, e verificando o link relacionado para ser clicado e o remetente da mensagem, ambos não tem relação alguma com a página do banco.

2.5.3 Códigos maliciosos *(malware)*

De acordo com Wendel (2011), *malwares* são programas de computadores criados com a intenção de infiltrar ou roubar dados e/ou espionar e/ou danificar e/ou esconder evidências em um sistema computacional. Vírus, *Worms, Spywares, Keyloggers, Rootkits, Backdoors, Trojan Horses*, etc, são considerados *malwares*.

Como o próprio nome sugere, a palavra **Malware** foi criada a partir da junção de duas palavras em inglês ”***Mal****icious” e “Soft****ware***”, ou seja, programa malicioso.

2.6 MEDIDAS DE SEGURANÇA APLICÁVEIS AOS BANCOS

Os bancos vêm aperfeiçoando e investindo cada vez mais nos aspectos de segurança necessários para um acesso seguro.

Como um dos principais podemos considerar o certificação digiral SSL (Secure Sockets Layer) é uma tecnologia de segurança que é utilizada para codificar os dados trafegados entre o computador do usuário e um Website, em conjunto. O protocolo SSL, através de um processo de criptografia dos dados, previne que os dados trafegados possam ser capturados, ou mesmo alterados no seu curso entre o navegador do usuário e o site com o qual ele está se relacionando, garantindo desta forma informações sigilosas como os dados de cartão de crédito, da conta corrente e de transações financeiras. (LANYWAY, 2011).

Dentre outras medidas adotadas são citadas as seguintes:

a) Cadastramento de senha específica para a internet;
b) Cadastramento e identificação do computador a ser utilizado;
c) Créditos para favorecidos previamente cadastrados;
d) Limites máximos diários para pagamentos e transferências;
e) Encerramento da sessão, dentre outros.

As características específicas dos principais mecanismos de segurança são abordados no capítulo de análise de resultados, onde é feito um comparativo entre três dos maiores bancos brasileiros.

2.7 MEDIDAS DE SEGURANÇA APLICÁVEIS AOS USUÁRIOS

Além das medidas adotadas pelos bancos para garantir a segurança nos acessos as contas via internet, os usuários também possuem uma série de cuidados a serem tomados. Podemos considerar essas medidas tão ou mais importantes do que as tomadas pelos bancos, um acesso indevido a uma conta, quase em sua totalidade, parte de um descuido ou atitude tomada pelo usuário. Assim como o número de acessos crescem, pessoas mal intencionadas também aparecem com mais frequência buscando levar vantagem em alguma transação.

Conforme Delgado (2006), a Federação Brasileira dos Bancos explica que o esforço das equipes de Tecnologia da Informação em desenvolver sistemas mais seguros se perde quando o usuário deixa senhas anotadas na mesa, usa internet banking em computadores compartilhados ou mesmo quando aceita baixar fotos e arquivos anexos de remetentes desconhecidos.

Os principais cuidados que devem ser tomados para um acesso seguro e confiável indicados pela FEBRABAN (2011) são relacionados abaixo:

a) Nunca emprestar o cartão bancário para ninguém nem permitir que estranhos o examinem sob qualquer pretexto. Pode haver troca do cartão, sem que seja percebido;
b) Não deixar o cartão sem assinatura;
c) Digitar a senha nos pagamentos com cartão de crédito e débito com bastante atenção. Conferindo se o campo de digitação da senha é mesmo destinado para ela. Ao efetuar pagamentos com cartão, não deixar que ele fique longe do controle e tomar cuidado para que ninguém observe a digitação da senha. Ao receber de volta o cartão verificar se é o mesmo que foi entregue;
d) Se for preciso anotar a senha, guardar em lugar diferente do cartão, reduzindo seus riscos em caso de roubo ou perda;
e) Em caso de cartão roubado, perdido ou extraviado, comunicar o fato imediatamente à Central de Atendimento do banco emissor, pedindo o cancelamento. Em caso de assalto, também registrar a ocorrência na delegacia mais próxima;
f) Em caso de retenção do cartão no caixa automático, apertar as teclas “ANULA” ou “CANCELA” e comunicar imediatamente com o banco. Tentar utilizar o telefone da cabine para comunicar o fato. Se ele não estiver funcionando, pode tratar-se de tentativa de golpe. Nesses casos nunca aceitar ajuda de desconhecidos, mesmo que digam trabalhar no banco, nem aceitar usar celular emprestado, nem digitar senha alguma na máquina ou qualquer aparelho mesmo que seja celular;
g) Tomar especial cuidado com esbarrões ou encontros acidentais, que possam levar a perder de vista, temporariamente, o cartão magnético. Se isso ocorrer, verificar se o cartão que está em poder é realmente o do portador. Em caso negativo, comunicar o fato imediatamente ao banco;
h) Solicitar sempre a via do comprovante da operação e, antes de assiná-lo, conferir o valor declarado da compra;

i) Ao sair, levar cartões e talões de cheques de forma segura, sem deixá-los a mostra.

j) Em viagem não deixar bolsa ou carteira em locais de trânsito de pessoas;

k) Ao efetuar compras com cartão pela Internet, procurar, antes, saber se o site é confiável e se tem sistema de segurança para garantia das transações;

l) Evitar expor o cartão a campo magnético (rádio, alarme de veículo, vídeo, celular, etc.) ou ao calor. Ambos podem prejudicar os registros da tarja magnética do cartão, impedindo sua leitura pelas máquinas;

m) Manter atenção com e-mails de origem desconhecida, que aguçam a curiosidade ou que contenham mensagens como “Você está sendo traído”; “Seu nome está na lista de devedores do Serasa (ou do SPC)”; “Confira: fotos picantes”. Esses e-mails costumam ser a porta de entrada para programas espiões que roubam as senhas do usuário e dão origem às fraudes. Na dúvida, deletar o e-mail antes mesmo de abri-lo;

n) Manter o sistema operacional e programas antivírus atualizados;

o) Evitar acessar sua conta por meio de sites de bancos (Internet-banking) se estiver utilizando computadores instalados em locais de grande circulação de pessoas, como cyber cafés, lan-houses e outros computadores, mesmo que pessoais, em local de trabalho ou estudo que são compartilhados com outras pessoas;

p) Trocar periodicamente a senha utilizada para acessar seu banco na Internet;

q) Manter em local seguro e fora da vista de terceiros os dispositivos de segurança do banco de acesso, como cartões de senhas e tokens;

r) Em caso de dúvida em relação à segurança de algum procedimento no Internet Banking, entrar em contato com o banco. Prevenção é a melhor forma de segurança;

s) Acompanhar os lançamentos em conta corrente. Em caso de constatação de qualquer crédito ou débito irregular, entrar imediatamente em contato com o banco;

t) Na desconfiança do acesso à página do Internet Banking, clicar na barra superior do navegador e movimentar a janela, caso algum conteúdo existente na página não acompanhe a movimentação pode ser o indício de um programa espião no computador.

A escolha de um local adequado, a confiança no sistema de segurança dos bancos e a adoção dos cuidados relacionados, fazem do acesso ao Internet Banking uma tarefa

corriqueira sem demais preocupações ou complicações, trazendo muita comodidade e praticidade para os clientes e bancos.

Os cuidados específicos indicados pelos principais bancos brasileiros, são relacionados no capítulo de apresentação e análise dos resultados.

3 MÉTODO

É apresentado a seguir os procedimentos metodológicos utilizados para a obtenção dos resultados do problema proposto pelo projeto.

3.1 MÉTODO ESCOLHIDO E JUSTIFICATIVA

A pesquisa foi realizada através do método de pesquisa qualitativo de estudo de caso. O método de estudo de caso foi escolhido por trazer a oportunidade de analisar o problema proposto em mais de uma organização, trabalhando com diferentes fontes de pesquisa e evidências, possibilitando assim uma visão sistêmica da análise.

3.2 INSTRUMENTOS DE COLETA DE DADOS

A primeira e a segunda parte do levantamento de dados foram realizados através de pesquisas junto às Instituições Financeiras, a partir das suas páginas de acesso ao Internet Banking, dados fornecidos por tais instituições, livros e revistas especializadas, artigos e cartilhas publicados na internet. Uma delas a fim de levantar quais os procedimentos e recursos são utilizados pelos principais bancos brasileiros para garantir a segurança da informação no acesso de seus clientes a este serviço. A outra com o objetivo de relacionar as principais ações que os clientes adotem para tornar seu acesso e realizações de tarefas pelo Internet Banking seguro. As instituições pesquisadas nestas duas primeiras etapas foram o Banco Amarelo, Banco Vermelho, Banco Laranja, classificadas entre os três maiores bancos do Brasil pelo lucro líquido realizado em junho de 2011, de acordo com o Banco Central do Brasil. Tais instituições são responsáveis por cerca de 80% do mercado nacional.

A terceira parte foi realizada através do levantamento de informações, aplicado através de questionário, buscando verificar o perfil dos usuários do Internet Banking, perfil da empresa por qual faz o acesso, frequência com que é realizada e qual o percentual destes

clientes tem o conhecimento dos procedimentos de segurança, faz uso das medidas indicadas pelos bancos e tem a percepção quanto a sua importância na adoção destas ações. A entrevista foi direcionada através de questões fechadas e abertas.

O objeto de pesquisa desta etapa foram os clientes pessoa jurídica da agência do Banco Amarelo, localizado na Rua Dr. João Colin, na cidade de Joinville SC. A cidade está situada na região nordeste do estado de Santa Catarina, possui cerca de 515.250 habitantes e conta com a presença de mais de dez Instituições Financeiras, totalizando cerca de 55 agências instaladas na cidade. O Banco Amarelo possui na cidade 13 agências em funcionamento.

Os clientes pessoa jurídica da agência pesquisada estão divididos em três carteiras, classificados de acordo com o seu faturamento. Uma carteira de clientes com faturamento acima de dois milhões e quatrocentos mil reais, com cerca de 75 empresas. E outras duas carteiras de clientes com faturamento até dois milhões e quatrocentos mil reais, cada uma destas carteiras possui cerca de 110 empresas, totalizando um universo de 295 clientes. O público alvo de clientes empresas foi escolhido devido a facilidade de contato, complexidade e quantidade das transações realizadas através da internet.

3.3 APLICAÇÃO DO INSTRUMENTO DE PESQUISA

A aplicação do instrumento de pesquisa junto aos clientes pessoa jurídica do Banco Amarelo foi realizado através de questionário enviado via e-mail para os administradores ou responsáveis pelo departamento financeiro de cada empresa, ou seja, a pessoa responsável pela utilização do Internet Banking.

Foram encaminhados cerca de 120 e-mails, em sua maioria, quase em totalidade para uma das carteiras com 110 clientes, devido a facilidade de contato. A taxa de retorno foi de 46,66%, ou seja, 56 questionários respondidos, equivalente a 18,98% do total da população em questão. Muitos clientes ficaram receosos quanto à veracidade do e-mail encaminhado, mesmo com a indicação da finalidade e com a identificação do funcionário da agência. Esta dúvida foi tratada através de contato pessoal, aumentando assim significativamente o número de questionários respondidos.

3.4 ANÁLISE DOS DADOS

A análise dos dados foi realizada de forma descritiva e comparativa, apresentando os resultados obtidos pela pesquisa. Serão descritos os aspectos de segurança utilizados pelos bancos e pelos clientes, em seguida comparando-os para identificar um conjunto que possa ser considerado o mais seguro.

Relacionando as três etapas do levantamento de dados, buscou-se apresentar uma situação ideal entre bancos e clientes para um acesso seguro. Esta relação está descrita no final do capítulo de apresentação e análise dos resultados.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Neste capítulo será apresentada a análise e interpretação dos resultados das pesquisas realizadas e questionários aplicados. A análise dos resultados foi dividida em três etapas, relacionando primeiramente os mecanismos de segurança utilizados por 3 principais bancos brasileiros para o acesso a transações financeiras pela Internet, em seguida com a apresentação dos cuidados que cada banco indica a seu usuário para o acesso seguro, posteriormente demonstrando a percepção dos clientes pessoa jurídica da população pesquisada quanto à importância do seu conhecimento quanto ao assunto e do seu comportamento para garantir a segurança no acesso bancário na internet.

4.1 MECANISMOS DE SEGURANÇA ADOTADOS PELOS BANCOS

Será relacionado a seguir os mecanismos de segurança adotados pelos 3 principais bancos brasileiros para a garantia de um acesso seguro ao seu Internet Banking para clientes empresariais, os bancos pesquisados não serão identificados, sendo a partir de agora chamados como: Banco Amarelo, Banco Vermelho, Banco Laranja.

4.1.1 Protocolo de Segurança

Os três bancos pesquisados utilizam o protocolo de segurança SSL – *Secure Socket Layer*, que é um protocolo de segurança que criptografa todos os dados trafegados entre o computador do cliente e o do banco, ou seja, transforma informação sigilosa em código secreto. O Banco Amarelo e o Banco Laranja utilizam como certificador de segurança para esta funcionalidade o CertiSign, empresa responsável pela garantia de acesso a site seguro das principais instituições financeiras do mundo. O Banco Vermelho não cita seu certificador.

4.1.2 Chave de Acesso

Cada usuário do Internet Banking do Banco Amarelo possui um identificador, chamado de “chave de acesso”, vinculado a cada empresa com a qual tenha relacionamento. Desta forma, todas as ações do usuário são facilmente identificadas através da consulta ao histórico de transações. A chave de acesso é também conhecida como Chave J, pois é composta pela letra J seguida de sete números. A permissão de acesso é estabelecida de acordo com os poderes vigentes no contrato social de cada empresa, no qual é designado o administrador da mesma.

O Banco Vermelho também trabalha com a representação no sistema por usuários, devidamente certificados no seu Internet Banking, que têm as suas responsabilidades definidas, de acordo com níveis pré-estabelecidos. O acesso é feito através de um arquivo de certificação digital com as informações do usuário, fornecido pelo banco.

Já o Banco Laranja disponibiliza o acesso aos seus clientes pessoa jurídica através do chamado cartão PJ, com ele, seus responsáveis legais e funcionários movimentam a conta da empresa utilizando os mais modernos recursos eletrônicos. O responsável pela empresa determina qual tipo de cartão cada funcionário deve ter de acordo com suas responsabilidades e funções, definindo o número de cartões que a empresa irá precisar, quais tipos de cartões e os limites diário e semanal.

4.1.3 Senhas

O Banco Amarelo trabalha com a senha de acesso e senha da conta. A senha de acesso é formada por um código alfanumérico de oito dígitos, que deve conter em sua composição pelo menos três letras e um numeral. Gerada juntamente com a chave do usuário (a Chave J), a senha é alterada pelo usuário no primeiro acesso. A senha da conta é necessária para confirmar transações de movimentação em conta corrente e para realização de consultas. É formada por um código de oito dígitos numéricos, utilizado para acessar as transações que envolvam a conta corrente do cliente.

Os bancos Vermelho e Laranja trabalham de forma diferente do Banco Amarelo e semelhante entre si. Eles utilizam uma chave de segurança eletrônica (Token), um dispositivo

eletrônico físico, que gera um código temporário e aleatório, de uso único, que é utilizado no acesso e nas transações realizadas pelo Internet Banking.

4.1.4 Componente de Segurança

Os bancos Amarelo e Vermelho utilizam um componente de segurança auxiliar, um software acoplado ao navegador de acesso, para ampliar as funções de segurança na realização de transações contábeis nos seus canais de acesso ao Internet Banking. Este componente tem por finalidade atuar na detecção/inibição de softwares maliciosos, a exemplo do vírus cavalo de troia, usados para capturar as informações inseridas por meio do teclado do computador convencional e virtual, bloqueando o acesso a conta no caso de alguma possível violação.

Outro ponto positivo da utilização deste sistema é que a agência de relacionamento do cliente recebe um aviso quase que instantâneo quando da ocorrência de um bloqueio de chave, podendo acompanhar a conta do cliente, verificando possíveis alterações ou violações. O Banco Laranja não utiliza este componente auxiliar.

4.1.5 Mecanismos de Segurança Complementares

Há, ainda, alguns mecanismos de segurança complementares utilizados pelos bancos analisados:

a) Teclado Virtual;
b) Encerramento de sessão automático;
c) Cadastramento de computadores;
d) Bloqueio de horários;
e) Cadastramento de favorecidos de crédito;
f) Limites para transferências e pagamentos;
g) Imagem de Identificação – Captcha.

4.2 CUIDADOS DE SEGURANÇA POR PARTE DOS USUÁRIOS

Os cuidados principais com a segurança que os usuários do Internet Banking devem tomar, indicados pela FEBRABAN, foram citados no capítulo de revisão bibliográfica. Os bancos analisados também indicam aos seus clientes alguns cuidados para que possam garantir essa segurança. É apresentada a relação que cada um disponibiliza, para fazermos uma comparação e identificarmos quais delas são mais lembradas, considerando assim como as mais importantes.

O Banco Amarelo cita em sua página na internet que disponibiliza ferramentas que proporcionam ao cliente maior segurança para realizar suas operações financeiras pela Internet. Mas, para que essas ferramentas tenham real eficácia, o cliente deve tomar alguns cuidados, que segue:

a) Nunca informar o número do cartão ou o código de segurança ao utilizar o autoatendimento pela Internet;
b) Certificar-se de que está na área segura do portal;
c) Evitar atalhos para acessar o site do banco;
d) Procurar sempre acessar o site do banco no início da conexão ao provedor;
e) Evitar realizar operações em equipamentos de uso público;
f) Evitar abrir e-mail de origem desconhecida;
g) Evitar também executar programas ou abrir arquivos anexados, sem verificá-los com antivírus atualizado;
h) Utilizar somente provedores com boa reputação no mercado e *browsers* e antivírus mais atualizados.
i) Certifique-se também de que as demais pessoas que utilizam o seu computador tenham conhecimento e sigam as orientações de segurança;
j) Confirmar quando foi o último acesso;

O Banco Vermelho cita em sua página na internet que para realizar transações financeiras e obter informações por computador pela internet, os clientes devem conhecer os riscos a que podem estar sujeitos e devem estar cientes das medidas preventivas que devem adotar para evitá-los. Serão relacionados abaixo as medidas indicadas pelo banco.

a) Manter sempre o antivírus atualizado e instalado no computador que utiliza;
b) Não executar aplicações, nem abrir arquivos de origem desconhecida.

c) Em casos de contaminação, a única maneira de garantir a "limpeza", é a formatação da máquina.
d) Só utilizar equipamento efetivamente confiável.
e) Não usar programas piratas ou de origem desconhecida;
f) Evitar sites arriscados e só fazer *downloads* de sites que conheça e saiba que são confiáveis;
g) Utilizar sempre as versões de navegadores mais atualizadas;
h) Usar somente provedores confiáveis;
i) Em caso de dúvida sobre a segurança de algum procedimento, entrar em contato com o Banco;

O Banco Laranja também faz menção da importância do usuário quanto a segurança no acesso as transações financeiras pela internet, ele cita em sua página que no dia a dia do cliente é importante navegar na internet com segurança. Para tanto, o banco oferece dicas importantes. São relacionados a seguir.

a) Verificar se o certificado SSL realmente existe na página que está sendo acessada e se ele foi gerado pelo Banco. Verificando se o cadeado de segurança está ativo no navegador;
b) Deixar o antivírus sempre ativo e atualizado;
c) Passar o antivírus em todos os arquivos baixados pela Internet;
d) Passar o antivírus em todos os anexos recebidos por e-mail;
e) Ao baixar arquivos da Internet é preciso ter muito cuidado. Quando o download de um arquivo é feito, ele tem a possibilidade de interagir com grande parte do computador, deixando-o suscetível a modificações que podem ser prejudiciais.

Todas as medidas de segurança indicadas pelos bancos pesquisados são de suma importância para a garantia de um acesso seguro. Os itens mais lembrados entre os três bancos são relativos à utilização e atualização de antivírus e abertura de e-mails e arquivos desconhecidos, questões relacionadas a estas medidas foram colocadas com relevância no questionário aplicado aos clientes, analisado a seguir.

4.3 ANÁLISE DO QUESTIONÁRIO APLICADO

A seguir são apresentados a sistematização dos dados, análise e interpretação do questionário aplicado junto aos clientes pessoa jurídica do Banco Amarelo, localizado na Rua Dr. João Colin em Joinville/SC, abordados nesta pesquisa. Foram selecionados apenas clientes de um banco para esta parte da pesquisa devido à facilidade de contato com os mesmos.

Foram analisados 56 questionários nesta etapa, correspondente a 18,98% do total de clientes pessoa jurídica da agência do Banco Amarelo mencionada.

O instrumento de coleta de dados compões-se de quatro grupos de questões: caracterização da empresa, caracterização do respondente, questões objetivas a respeito do conhecimento e uso das medidas de segurança por parte do usuário do Internet Banking e questões abertas sobre a percepção pessoal quanto ao uso e a segurança neste acesso.

O roteiro da análise de dados foi definido com base nestes grupos de questões, ou seja, nos perfis da amostra e nos aspectos ligados diretamente a segurança no acesso ao Internet Banking.

4.3.1 Caracterização da Empresa

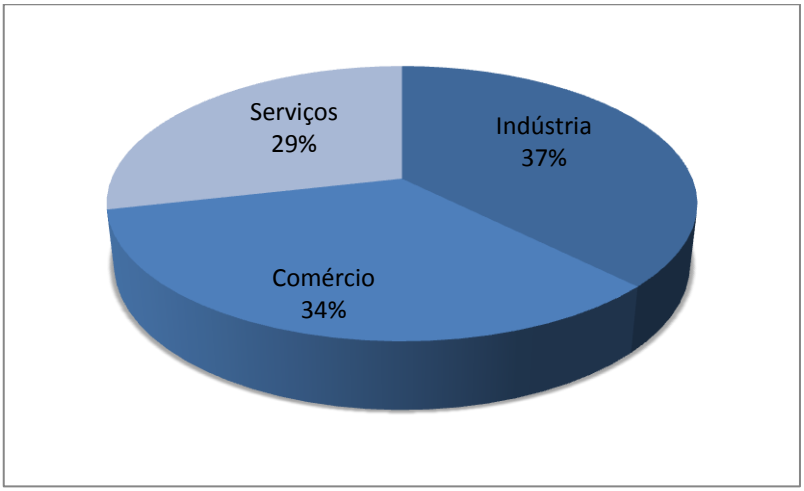
A seguir são apresentados os dados coletados que caracterizam o perfil das empresas da amostra estudada. As características em questão são o ramo de atividade, tempo de atuação no mercado e porte da empresa.

Tabela 1 – Ramo de atividade da empresa

Ramo Empresa	Frequência	Percentual
Indústria	21	37%
Comércio	19	34%
Serviços	16	29%
Total	**56**	**100%**

Na sequência será apresentado o gráfico para ilustrar a informação apresentada na tabela 1.

Gráfico 1 – Percentual do ramo de atividade da emp resa



Analisando os resultados obtidos, percebe-se que o ramo de atividade das empresas pesquisadas são bem divididos entre indústria, comércio e serviços, mostrando que independente da atuação da empresa para que ela busque realizar suas transações pela internet.

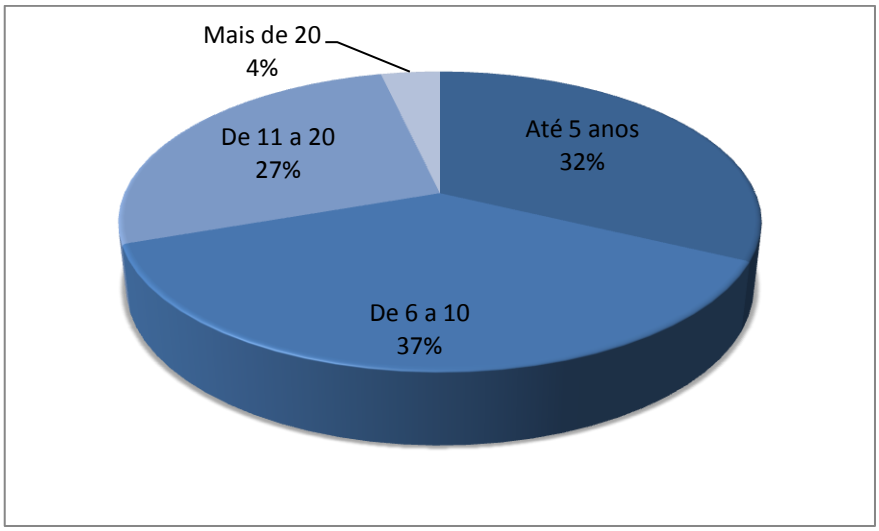
São relacionados a seguir os dados referentes ao tempo de atuação no mercado das empresas pesquisadas.

Tabela 2 - Tempo de atuação da empresa no mercado

Tempo atuação	Frequência	Percentual
Até 5 anos	18	32%
De 6 a 10	21	37%
De 11 a 20	15	27%
Mais de 20	2	4%
Total	**56**	**100%**

Na sequência será apresentado o gráfico para ilustrar a informação apresentada na tabela 2.

Gráfico 2 – Percentual do tempo de atuação da empresa no mercado



O tempo de atuação também apresentou-se bem dividido, com certa diferença para empresas de 6 a 10 anos, com 37% das respostas. Já empresas com mais de 20 anos no mercado corresponde a apenas 4% da amostra, demonstrando que empresas mais tradicionais, tendem a ter uma certa restrição a introdução de novas ferramentas e tecnologias.

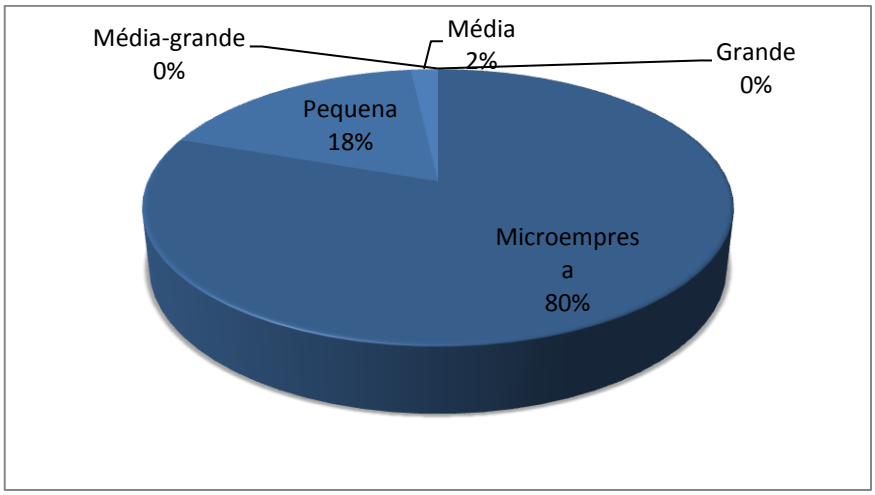
A classificação das empresas quanto ao seu faturamento seguem as seguintes referências: Microempresa - Menor ou igual a R$ 2,4 milhões; Pequena Empresa - Maior que R$ 2,4 milhões e menor ou igual a R$ 16 milhões; Média Empresa - Maior que R$ 16 milhões e menor ou igual a R$ 90 milhões; Média-grande Empresa - Maior que 90 milhões e menor ou igual a R$ 300 milhões; Grande Empresa - Faturamento maior que R$ 300 milhões.

Tabela 3 - Porte da empresa por faturamento anual

Porte Empresa	Faturamento	Frequência	Percentual
Microempresa	≤ R$ 2,4 milhões	45	80%
Pequena	> R$ 2,4 milhões e ≤ R$ 16 milhões	10	18%
Média	> R$ 16 milhões e ≤ R$ 90 milhões	1	2%
Média-grande	> 90 milhões e ≤ R$ 300 milhões	0	0%
Grande	> R$ 300 milhões	0	0%
Total		**56**	**100%**

Na sequência será apresentado o gráfico para ilustrar a informação apresentada na tabela 3.

Gráfico 3 – Percentual do porte da empresa por faturamento anual



Em relação ao porte das empresas, nota-se que quase em sua totalidade estão classificadas como micro-empresas, esta característica está relacionada ao modelo de atuação da agência e da carteira de clientes com maior direcionamento na pesquisa.

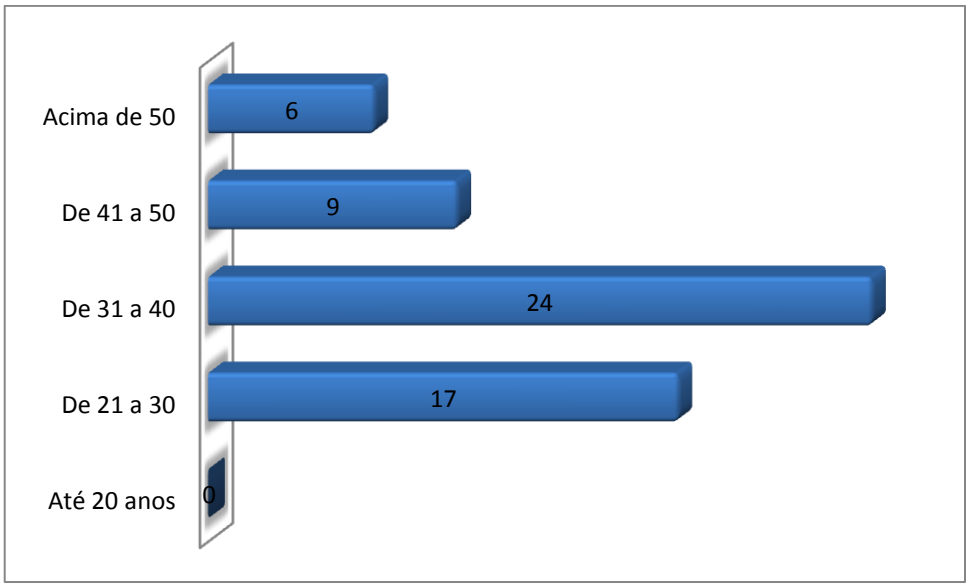
4.3.2 Caracterização do Respondente

Em seguida são apresentados os dados coletados que caracterizam o perfil dos usuários do Internet Banking, pessoa responsável na empresa por realizar as transações financeiras por meio eletrônico e que respondeu o questionário enviado. A segurança dos dados e transações das empresas dependem do conhecimento e comprometimento destas pessoas. As características em questão são: faixa etária, escolaridade, cargo que ocupa, tempo de trabalho na empresa, se utiliza o Internet Banking do Banco Amarelo, com qual frequência, há quanto tempo e se utiliza o acesso a conta pela internet de outro banco.

Tabela 4 – Faixa etária.

Faixa etária	Frequência	Percentual
Até 20 anos	0	0%
De 21 a 30	17	30%
De 31 a 40	24	43%
De 41 a 50	9	16%
Acima de 50	6	11%
Total	**56**	**100%**

Gráfico 4 – Comparativo da faixa etária



Pode-se perceber através dos dados pessoais do respondente, coletados através do questionário de pesquisa, que a pessoa responsável pelas transações financeiras das empresas tem uma faixa etária que varia de 21 até acima de 50 anos, a maioria está relacionada na idade entre 31 a 40 anos, com 43%. Abaixo de 20 anos não é apontado nenhum respondente.

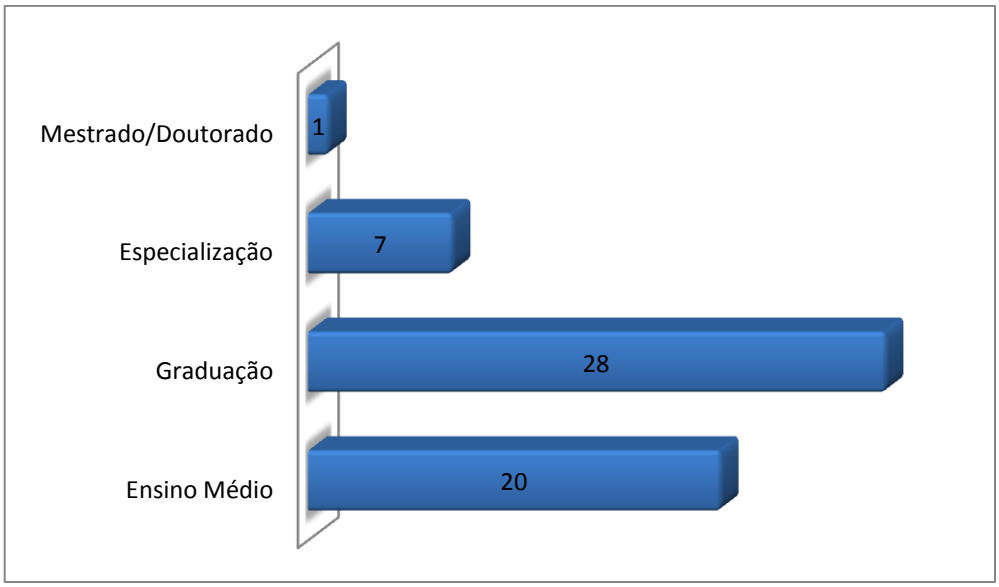
Esta faixa de idade nos mostra que a empresa tem uma pessoa com experiência na área financeira ou administrativa, mas com idade mediana, pois pessoas com idade um pouco mais avançada, costumam ter certa restrição a utilização de novas ferramentas e tecnologias e pessoas muito novas ainda não têm a visão de responsabilidade da função ou o conhecimento técnico para realizar as atividades pertinentes ao cargo.

Na sequência será apresentado a tabela e gráfico para ilustrar a informação relativa a escolaridade.

Tabela 5 – Escolaridade

Escolaridade	**Frequência**	**Percentual**
Ensino Médio	20	35%
Graduação	28	50%
Especialização	7	13%
Mestrado/Doutorado	1	2%
Total	**56**	**100%**

Gráfico 5 – Comparativo da escolaridade



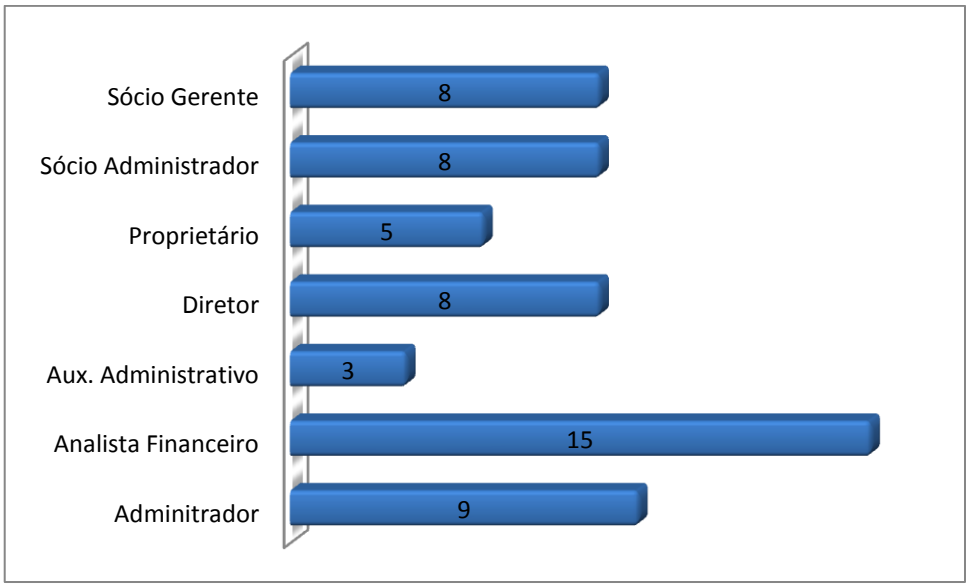
A escolaridade também é um ponto relevante no resultado da pesquisa. Um pouco mais da metade do público pesquisado possui graduação, somando com especialização e mestrado ou doutorado, esse percentual chega a 67%. Percebemos com este resultado que o conhecimento na área de atuação é fundamental para o funcionário atuar na área financeira da empresa.

Na sequência será apresentado a tabela e gráfico para ilustrar a informação relativa ao cargo que ocupa na empresa.

Tabela 6 – Cargo que ocupa na empresa

Cargo	**Frequência**	**Percentual**
Adminitrador	9	16%
Analista Financeiro	15	27%
Aux. Administrativo	3	6%
Diretor	8	14%
Proprietário	5	9%
Sócio Administrador	8	14%
Sócio Gerente	8	14%
Total	**56**	**100%**

Gráfico 6 – Comparativo do cargo que ocupa na empresa



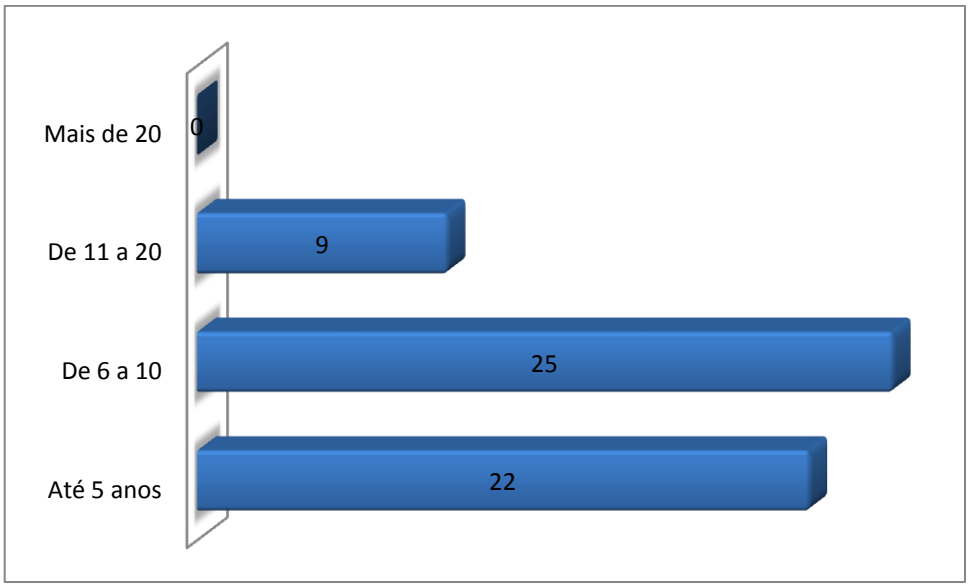
Com relação ao cargo que ocupa constata-se que cada vez mais as empresas estão em busca de funcionários com conhecimento e formação específica em finanças. É possível Verificar que 27% dos respondentes atuam no cargo de analista financeiro, auxiliar administrativo somam apenas 5%. Os demais dividem-se entre cargos de sócio gerente, proprietário, diretor e administrador, mostrando que quando a empresa não possui funcionário com a função específica, algum sócio ou proprietário assume esta função.

As informações referentes ao tempo em que atua na empresa serão apresentadas a seguir.

Tabela 7 – Tempo em que atua na empresa

Tempo de trabalho	**Frequência**	**Percentual**
Até 5 anos	22	39%
De 6 a 10	25	45%
De 11 a 20	9	16%
Mais de 20	0	0%
Total	**56**	**100%**

Gráfico 7 – Comparativo do tempo em que atua na empresa



O tempo em que este funcionário trabalha na empresa predominou na faixa de 5 a 10 anos, totalizando 84% dos respondentes. Pessoas com mais tempo de empresa costumam despertar mais confiança no empresário, mas a concorrência no mercado de trabalho, muitas vezes, não permite que a empresa consiga manter um funcionário por muito tempo. A rotatividade também muitas vezes é importante, para trazer novas motivações e experiências.

Em seguida são apresentados os resultados referentes à caracterização do respondente em relação a utilização do Internet Banking pela empresa em que trabalha.

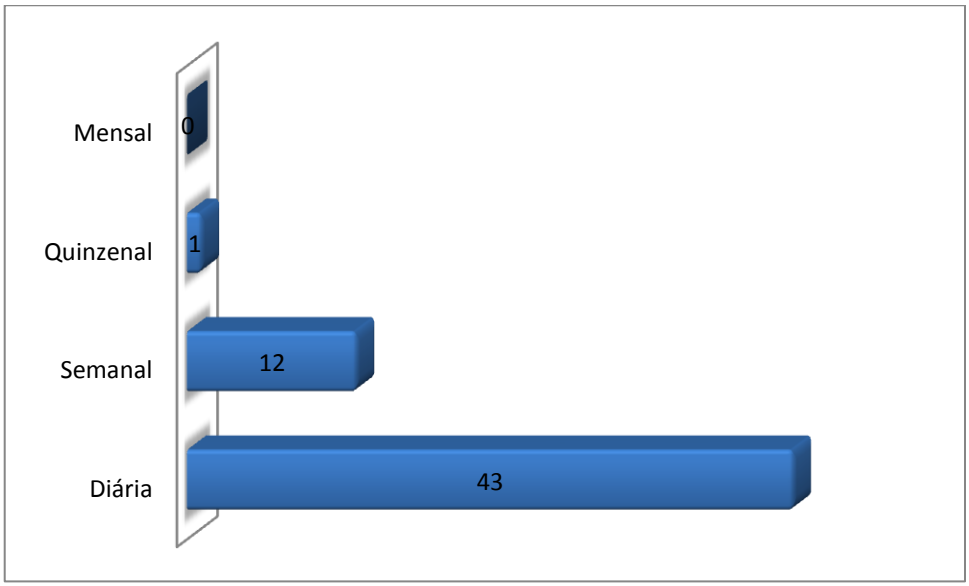
Primeiramente foi questionado se o respondente realiza transações financeiras pela internet para a empresa onde trabalha através do Internet Banking do Banco Amarelo, apenas para certificarmos de que o público pesquisado estava dentro do público-alvo da pesquisa, 100% dos respondentes confirmaram que utilizam este canal de atendimento, não sendo descartado nenhum dos questionários respondidos.

Logo em seguida foi questionado sobre a frequência de acesso, tempo em que faz uso do acesso a conta via internet pelo Banco Amarelo, e se realiza transações também por outro banco. Os dados são relacionados a seguir.

Tabela 8 – Frequência de acesso ao Internet Banking do Banco Amarelo

Frequência de acesso	Frequência	Percentual
Diária	43	77%
Semanal	12	21%
Quinzenal	1	2%
Mensal	0	0%
Total	**56**	**100%**

Gráfico 8 – Comparativo da Frequência de acesso ao Internet Bankingo do Banco Amarelo



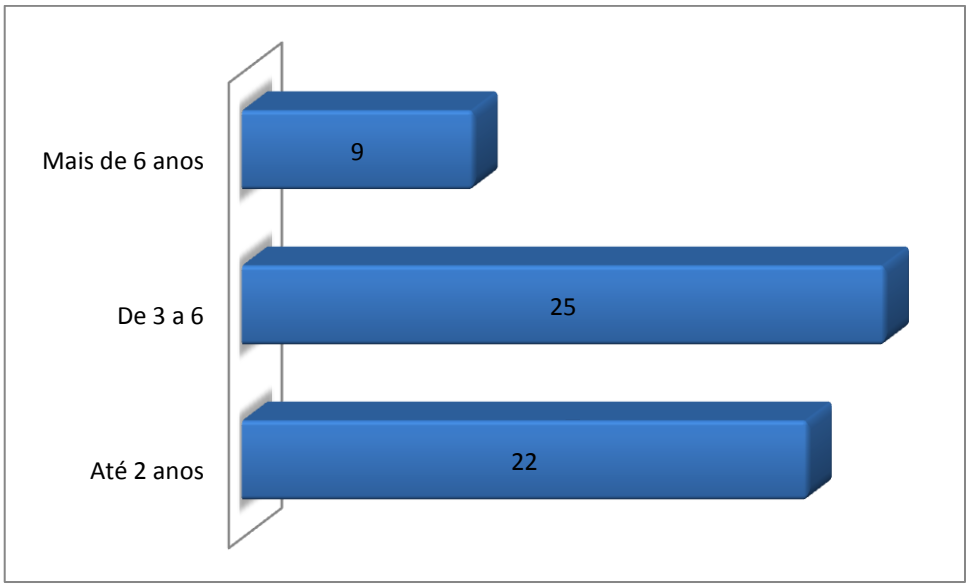
Analisando os dados obtidos verifica-se que os usuários fazem acesso ao Internet Banking do Banco Amarelo pela empresa em que trabalha com bastante frequência, 77% fazem tal acesso diariamente, e 21% semanalmente, isso mostra que cada vez mais as empresas têm optado por esta ferramenta na realização de suas transações financeiras, mostrando que o cuidado com a segurança deve ser constante.

Segue abaixo tabela e gráfico com a relação de quanto tempo faz o uso do Internet Banking do Banco Amarelo.

Tabela 9 – Há quanto tempo faz uso do Internet Banking do Banco Amarelo

Tempo de uso	Frequência	Percentual
Até 2 anos	22	39%
De 3 a 6	25	45%
Mais de 6 anos	9	16%
Total	**56**	**100%**

Gráfico 9 – Comparativo do tempo que faz uso do Internet Bankingo do Banco Amarelo



Relativo ao tempo que faz uso da ferramenta, ampla maioria ficou relacionada na faixa até 6 anos, constatando quanto é recente esta característica nas empresas. Esta constatação também está relacionada ao fato de as pessoas responsáveis são novas na empresa.

Segue abaixo tabela com a relação de quanto tempo faz o uso do Internet Banking do Banco Amarelo.

Tabela 10 – Se realiza transações financeiras para a empresa por outro banco

Acessa outro banco	Frequência	Percentual
Sim	32	57%
Não	24	43%
Total	**56**	**100%**

Com relação a realização de transações financeiras pela internet por outro banco, o resultado ficou bem dividido, com 57% dos respondentes confirmando que utilizam, esse resultado acompanha o número de clientes que utilizam o serviços de outros bancos. Se o cliente faz o uso do Internet Banking pelo Banco Amarelo e também é cliente de outro banco, a tendência é que ele também utilize do serviço por aquele banco.

4.3.2 Questões Objetivas

São apresentados a seguir os resultados alcançados pelas respostas das questões objetivas lançadas ao público pesquisado. Foram realizadas afirmações, nas quais o respondente caracterizou sua opinião com a seguinte escala: 1 – Discordo totalmente, 2 – Discordo parcialmente, 3 – Não concordo nem discordo, 4 – Concordo parcialmente e 5 – Concordo totalmente.

É relacionado a seguir uma tabela com o resumo das questões e suas respostas, logo em seguida, são apresentados de forma específica a análise de cada uma delas.

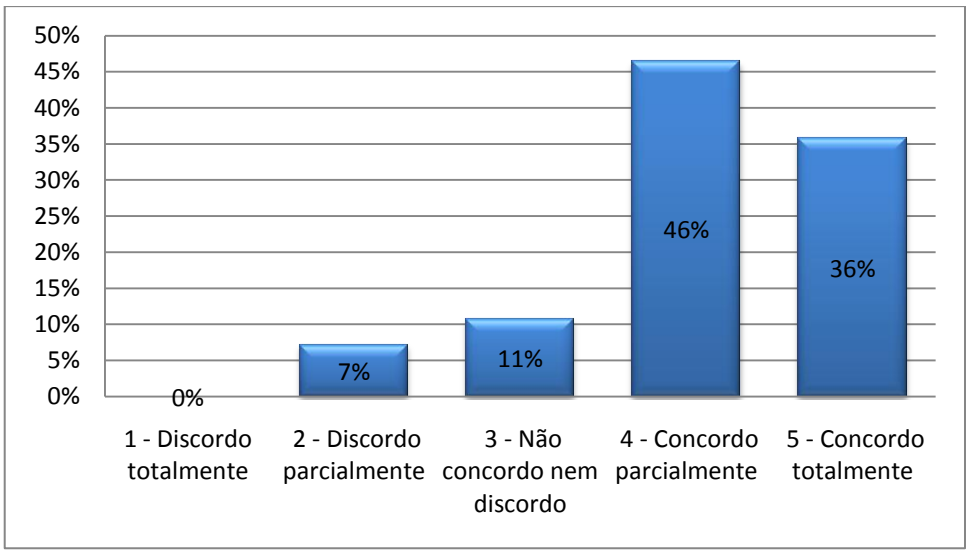
Tabela 11 – Resumo do resultado das questões objetivas

	1 - Discordo totalmente	**2 - Discordo parcialmente**	**3 - Não concordo nem discordo**	**4 - Concordo parcialmente**	**5 - Concordo totalmente**
Eu me sinto seguro(a) ao realizar transações financeiras pela Internet.	0	4	6	26	20
Eu classifico os mecanismos de segurança do Internet Banking do Banco Amarelo como adequados.	0	3	4	23	26
Eu conheço as recomendações dos bancos para um acesso seguro na Internet.	2	4	13	18	19
Eu utilizo programas de antivírus no computador com o qual acesso o Internet Banking.	0	0	0	18	38
Eu atualizo frequentemente o antivírus do computador com o qual acesso o Internet Banking.	1	2	4	26	23
Eu costumo abrir e-mails de remetentes desconhecidos.	28	21	5	0	2
Eu costumo acessar links recebidos por e-mail, independente do remetente.	35	17	2	0	2
Eu mantenho os cuidados necessários quanto a elaboração, atualização e sigilo das minhas senhas de acesso ao Internet Banking	0	1	3	28	24
Eu considero a segurança no acesso e na realização de transações bancárias pela Internet através do Internet Banking do Banco Amarelo maior que a dos outros bancos.	1	0	24	23	8

Segue abaixo gráficos das questões objetivas, com o percentual de resposta de cada uma delas e com a referida análise do resultado obtido.

Neste bloco do questionário com questões objetivas, procurou-se entender a percepção do cliente quanto à segurança no acesso ao Internet Banking. A primeira questão buscou relacionar se o cliente que utiliza este mecanismo nas suas transações financeiras se sente seguro ao realizá-las. Segue a representação em gráfico.

Gráfico 10 – Eu me sinto seguro(a) ao realizar transações financeiras pela Internet

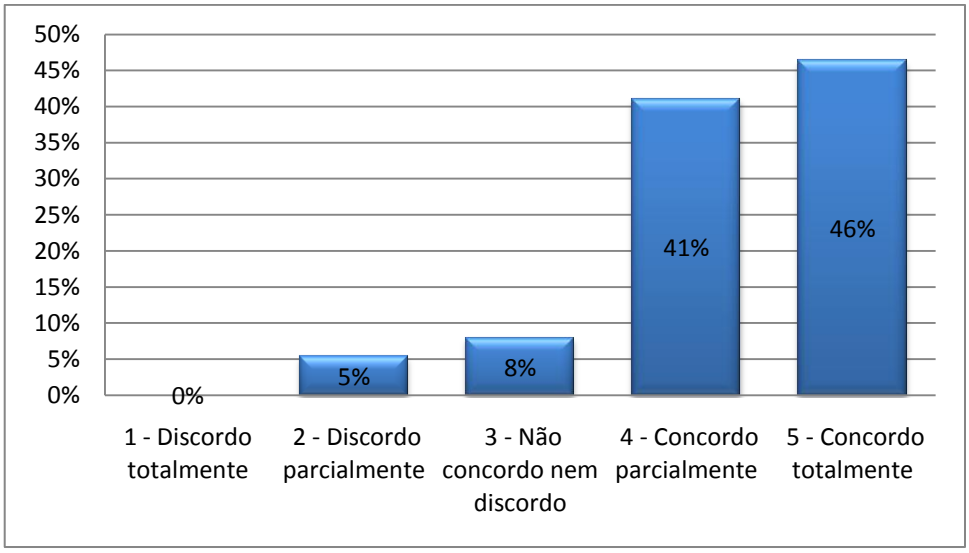


Como resposta, teve-se um grande percentual de concordância, 82% dos respondentes concordaram com a afirmação, prevalecendo os que concordam parcialmente, com 46% das respostas. O comentário que um dos respondentes fez nas questões abertas refere-se a esta questão: “Atualmente me sinto mais seguro em relação ao ambiente web para acesso bancário, no início ainda havia muitas brechas que ao meu ver já foram resolvidas, porém é necessário que a cada dia estejam sendo feitas melhorias”.

É importante o usuário ter confiança no seu acesso, mas o excesso desta confiança na realização de transações financeiras pela internet pode causar uma zona de conforto, fazendo com que o mesmo diminua ou pare de tomar certas medidas de segurança que antes adotava, isso precisa ser tratado com os clientes para que não aconteça, pois torna-se perigoso.

Em seguida foi relacionado a afirmação de que o cliente classifica os mecanismos de segurança do Internet Banking do Banco Amarelo como adequados. Esta questão teve como intenção verificar se o cliente conhece os mecanismos de segurança existentes para o acesso ao Internet Banking, relacionando com os quais precisa utilizar para realizar seu acesso, podendo assim classificá-los como adequados ou não. Segue a representação em gráfico.

Gráfico 11 - Eu classifico os mecanismos de segurança do Internet Banking do Banco Amarelo como adequados

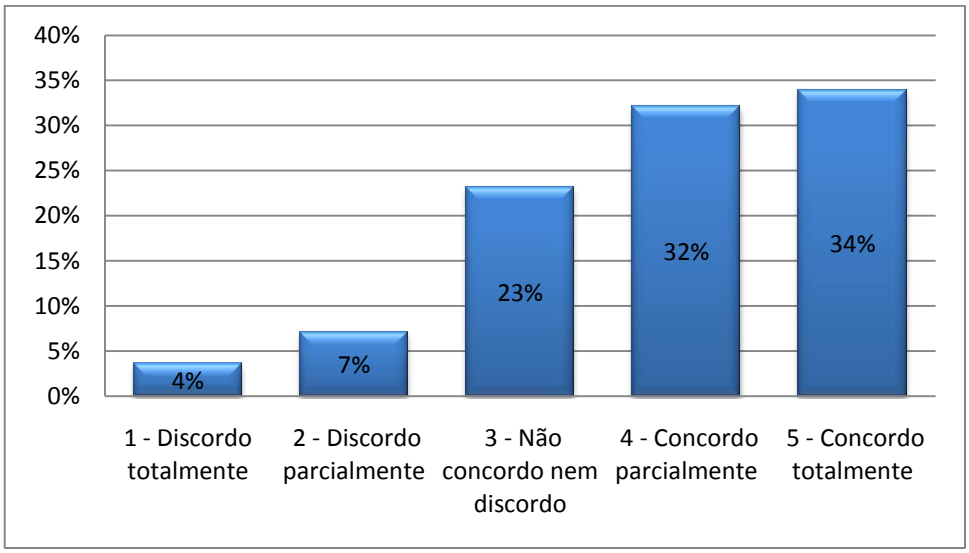


Foi obtido um grande percentual de concordância também nesta questão, com 87% das respostas concordando com a afirmação, com um percentual maior concordando totalmente, com 46%. É difícil classificar tais mecanismos como totalmente seguros, mas as respostas nos mostram a confiança do usuário pelos meios hoje utilizados pelo banco.

Nas questões abertas aos clientes, teve-se um comentário interessante sobre esta percepção do usuário: "Na minha opinião a única forma totalmente à prova de falhas e fraudes é a que alia leitura biométrica à presença física de certificação no equipamento. Quando tivermos a associação destes dois meios de identificação, seja em smartphones ou estações fixas o sistema estará livre de falhas e fraudes de acesso, excluindo-se os casos de banditismo presencial, como coação por meio de sequestro e/ou ameaça." Esta opinião traz uma realidade, a leitura biométrica, que faz a identificação da pessoa através do reconhecimento das suas veias, impressão digital, face, íris, ou outra parte do corpo, aliada a presença física dela para a autorização de uma transação, traria com certeza um acesso praticamente a prova de fraudes. Pode-se sim classificar este método como totalmente seguro.

A terceira questão traz a seguinte afirmação: eu conheço as recomendações do banco para um acesso seguro na Internet. Questão esta de grande importância para a obtenção do resultado proposto pela pesquisa, que é verificar a percepção do usuário quanto a sua importância no acesso seguro ao Internet Banking. Conhecer tais recomendações, já citadas nesta análise de resultados, é de suma importância para a garantia de um acesso seguro e confiável. Segue a representação em gráfico.

Gráfico 12 - Eu conheço as recomendações dos bancos para um acesso seguro na Internet



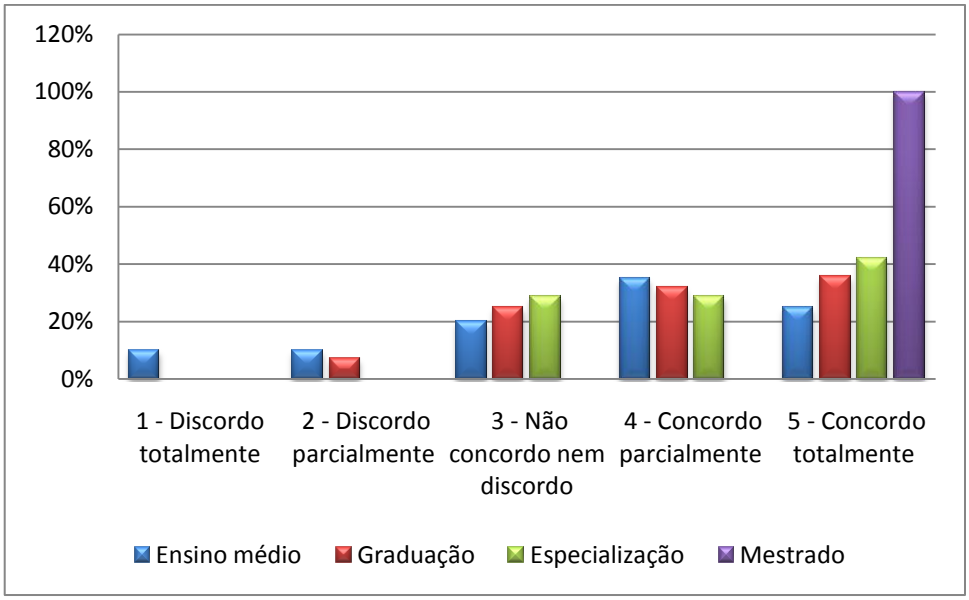
As respostas foram positivas quanto a este aspecto, 66% concordaram com a questão, divididos igualmente entre concordam parcialmente e totalmente. Obtivemos um percentual de 23% que não concordam e nem discordam, e um total de 11% que discordam, este público precisa ser trabalhado pelas instituições financeiras, provendo os usuários com as informações e recomendações para o acesso seguro, pois este percentual pode trazer grandes prejuízos aos clientes e aos bancos se forem relacionados a alguma fraude.

Fizemos uma relação desta questão com a escolaridade da pessoa responsável pelo acesso ao Internet Banking na empresa, com a finalidade de verificar se pessoas com uma maior instrução tem um conhecimento maior, ou tendem a buscar tal conhecimento quanto as recomendações de segurança.

Tabela 12 – Relação entre escolaridade e o conhecimento das recomendações do banco quanto a segurança

	1 - Discordo totalmente	**2 - Discordo parcialmente**	**3 - Não concordo nem discordo**	**4 - Concordo parcialmente**	**5 - Concordo totalmente**	**Total**
Ensino médio	2	2	4	7	5	**20**
Graduação		2	7	9	10	**28**
Especialização			2	2	3	**7**
Mestrado					1	**1**
Total	**2**	**4**	**13**	**18**	**19**	**56**

Gráfico 13 – Percentual da relação entre escolaridade e o conhecimento das recomendações do banco quanto à segurança



Analisando a relação proposta, verificou-se que realmente a escolaridade tem relação com o conhecimento ou a busca dele para com a segurança. Pode-se ver através do gráfico que usuários com ensino médio concordam em 60% com a afirmação, com graduação concordam em 68%, já os com especialização somam 71% e com mestrado 100%. Isso mostra que as empresas precisam investir em pessoal qualificado, na qualificação dos sócios ou dos funcionários com cargos relevantes. Educação é conhecimento, e conhecimento gera segurança em todos os aspectos.

Em seguida são relacionados os gráficos com o percentual de respostas quanto a utilização e atualização de antivírus.

Gráfico 14 - Eu utilizo programas de antivírus no computador com o qual acesso o Internet Banking

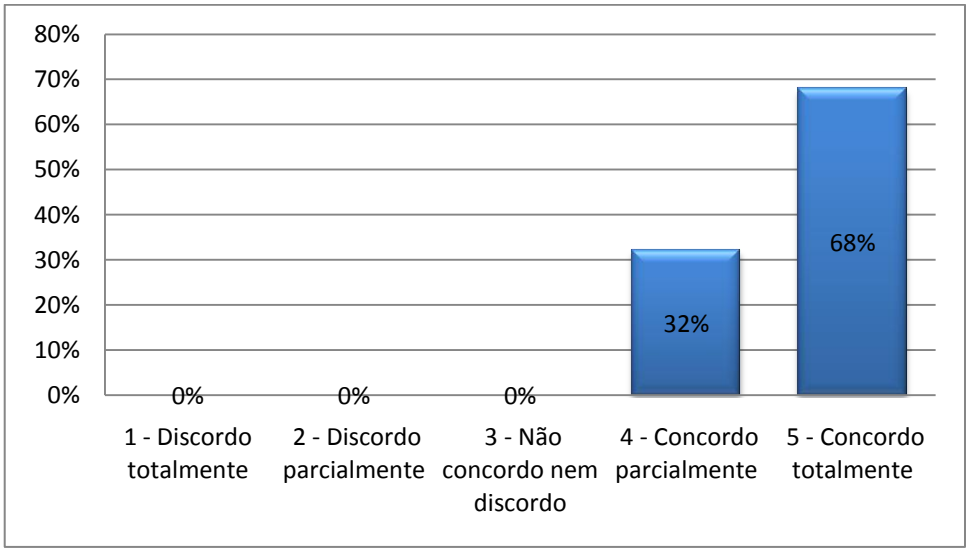
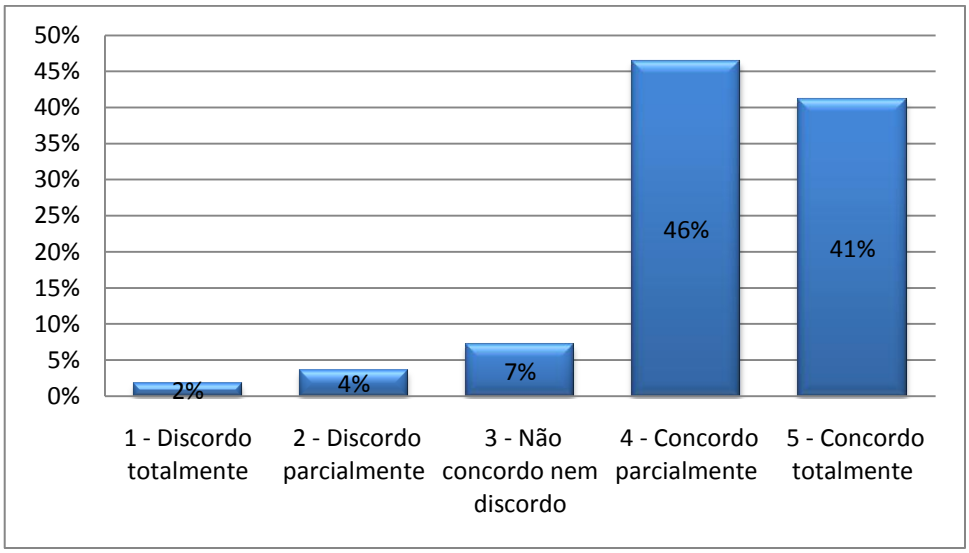


Gráfico 15 - Eu atualizo frequentemente o antivírus do computador com o qual acesso o Internet Banking



Analisando o gráfico referente a utilização do antivírus, vemos claramente que todos os clientes estão comprometidos com esta questão, 100% dos respondentes concordam com a afirmação. Procedimento este de grande importância na segurança dos computadores.

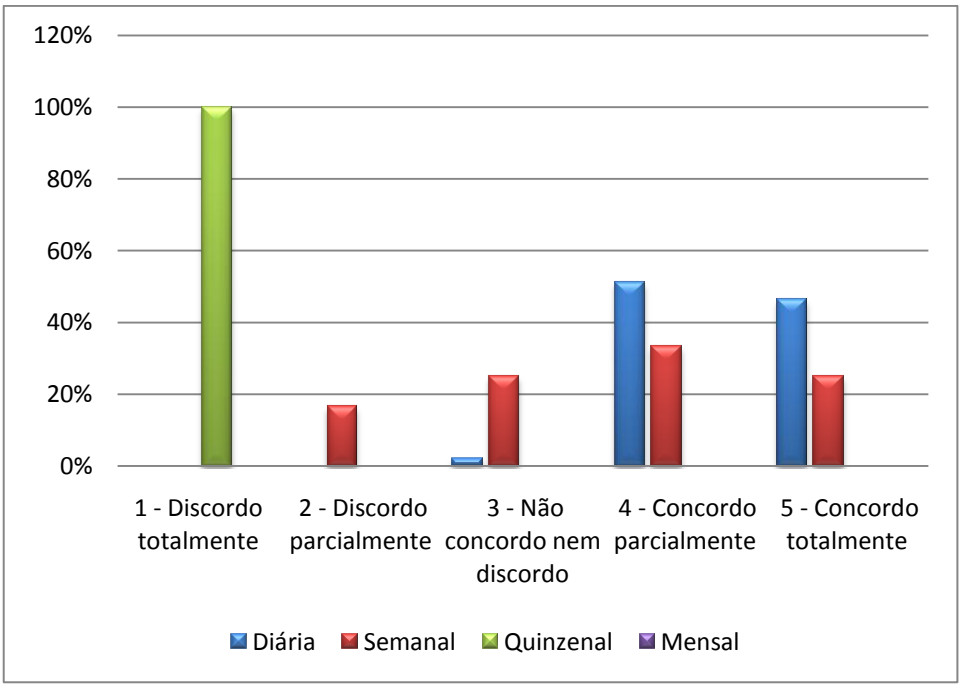
Com relação a atualização do antivírus, tivemos também um percentual alto que concordaram com a afirmação, 87%. Mas vemos que o percentual não é o mesmo da utilização. Estes 13% restantes representam um risco eminente as empresas, pois a atualização é tão importante quanto a utilização do antivírus.

Fizemos uma relação da atualização do antivírus com a periodicidade de acesso ao Internet Banking, com a finalidade de verificar se os usuários que fazem o uso desta ferramenta com mais frequência preocupam-se mais com esta questão.

Tabela 13 – Comparativo entre periodicidade de acesso e atualização do antivírus

	1 - Discordo totalmente	**2 - Discordo parcialmente**	**3 - Não concordo nem discordo**	**4 - Concordo parcialmente**	**5 - Concordo totalmente**	**Total**
Diária			1	22	20	43
Semanal		2	3	4	3	12
Quinzenal	1					1
Mensal						0
Total	**1**	**2**	**4**	**26**	**23**	**56**

Gráfico 16 – Percentual do comparativo entre periodicidade de acesso e atualização do antivírus



Verifica-se realmente que 98% dos usuários que fazem acesso ao Internet Banking diariamente faz a atualização de seu antivírus. Este dado é muito importante, e mostra o comprometimento de quem faz uso desta ferramenta no seu dia a dia. O percentual de quem discorda está totalmente em quem acessa semanalmente ou quinzenalmente. Esse público, apesar de não fazer acesso com frequência, também precisa tomar os cuidados necessários com esta atualização, pois somente um acesso pode ser necessário para que a conta seja violada, caso o computador esteja infectado com algum vírus.

Em seguida seguem os gráficos referentes ao comportamento do usuário quanto a utilização de seus e-mails.

Gráfico 17 - Eu costumo abrir e-mails de remetentes desconhecidos

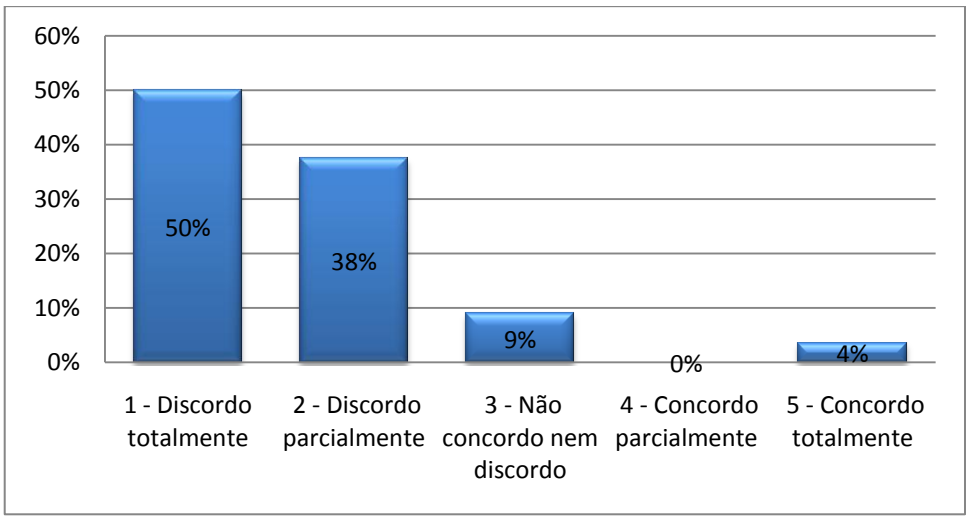
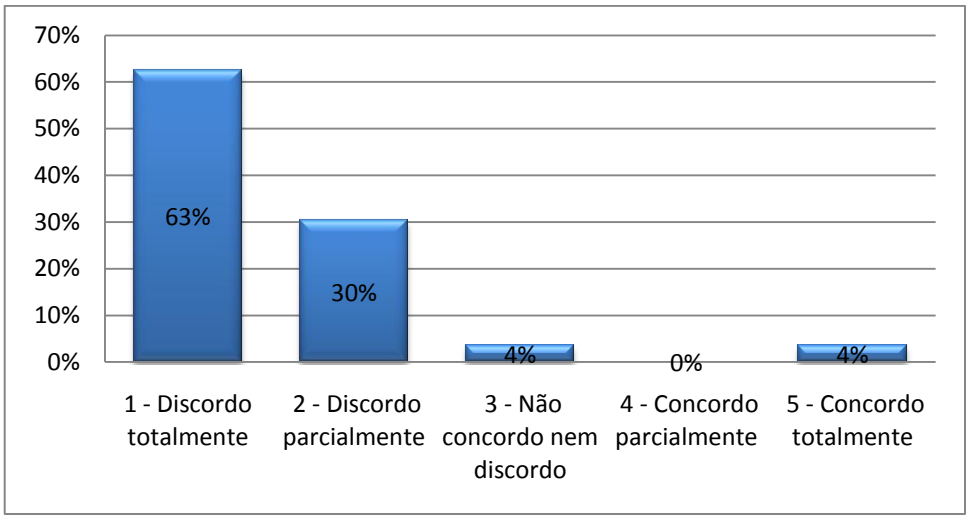


Gráfico 18 - Eu costumo acessar links recebidos por e-mail, independente do remetente



Analisando a percepção do cliente quanto a importância do cuidado no acesso a e-mails e links desconhecidos, através das respostas coletadas, apresentadas nos gráficos, vemos que a grande maioria declara que toma os devidos cuidados neste sentido.

Em relação à afirmativa de que costuma abrir e-mails de remetentes desconhecidos, 88% declaram que discordam parcialmente ou totalmente, um número bem expressivo, que mostra a atenção do usuário quanto a este cuidada.

Na questão seguinte, que afirma: eu costumo acessar links recebidos por e-mail, independente do remetente, também temos um grande percentual de discordância: 93%. Número também muito expressivo e positivo. Esta maior porcentagem em relação à questão anterior mostra um comportamento que realmente deve ser tomado. A abertura de um link recebido via e-mail tem muito mais risco do que somente a abertura de um e-mail de remetente desconhecido. Lembrando claro que os dois cuidados devem sempre ser tomados.

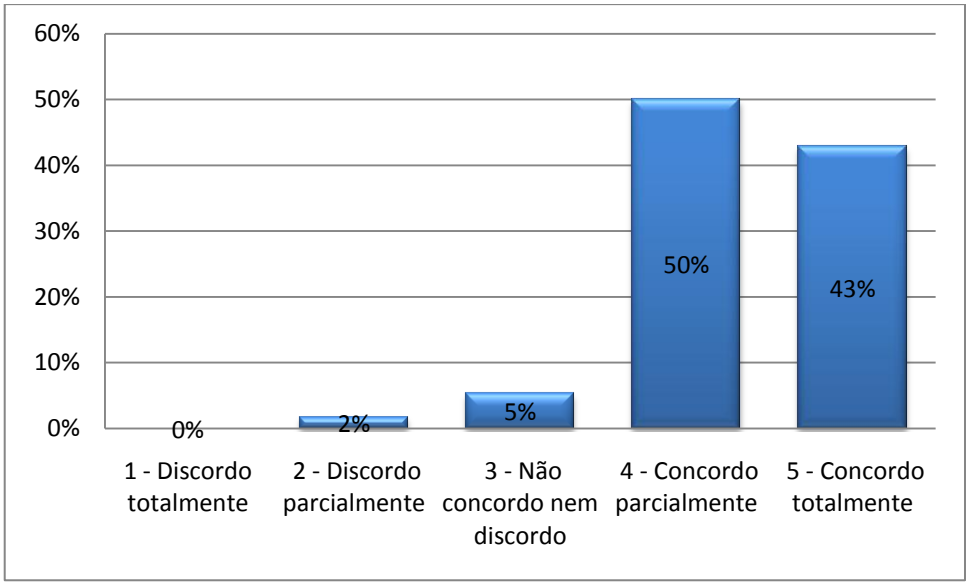
A experiência do encaminhamento do próprio questionário de pesquisa foi um parâmetro para a análise desta questão, pois mesmo o e-mail sendo enviado com a devida identificação da finalidade e do remetente como funcionário do banco, muitos clientes ficaram receosos em acessar o link que dava acesso ao questionário, indagando a veracidade do mesmo em contato pessoal, via e-mail ou telefone.

Tivemos um comentário com uma percepção interessante referente a esta parte: “Creio que para maior segurança, o computador que se utiliza para acessar o banco, deveria ser exclusivo para esse fim. Um desktop que não teria contas de e-mail configuradas, nem acesse outras coisa que não seja de interesse da empresa.” Esta medida pode ser considerada um pouco exagerada, pois em muitas vezes pode se tornar inviável para o funcionário. Mas seria

interessante este ser orientado a utilizar apenas o e-mail corporativo, deixando e-mails pessoais para acesso em casa ou em outras máquinas.

Em seguida é apresentado os resultados relativos aos cuidados com as senhas de acesso.

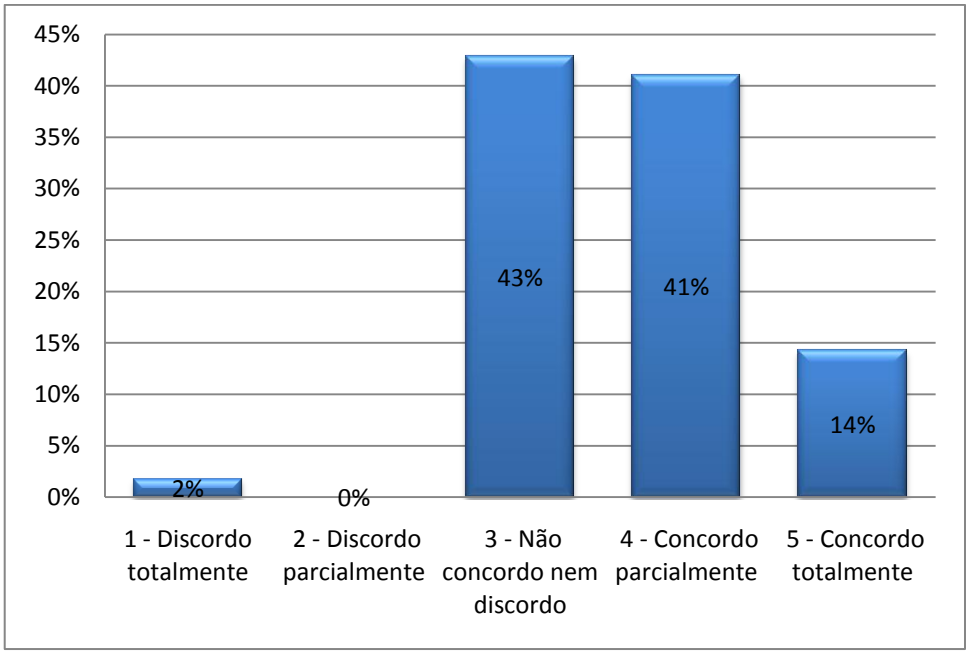
Gráfico 19 – Eu mantenho os cuidados necessários quanto a elaboração, atualização e sigilo das minhas senhas de acesso ao Internet Banking



Com relação a esta questão proposta, que afirma que o usuário toma os cuidados necessários quanto à elaboração, atualização e sigilo das senhas de acesso ao Internet Banking, tivemos um alto índice de concordância, com 93%. Destes, 50% concordando parcialmente e 43% concordando totalmente. Muito importante essa consciência do usuário, pois as senhas de acesso são extremamente confidenciais e importantes para a segurança das informações e das transações financeiras na internet.

A última questão objetiva trata do comparativo entra a segurança no acesso pelo Banco Amarelo em relação aos outros bancos pela visão do cliente.

Gráfico 20 - Eu considero a segurança no acesso e na realização de transações bancárias pela Internet através do Internet Banking do Banco Amarelo maior que a dos outros bancos



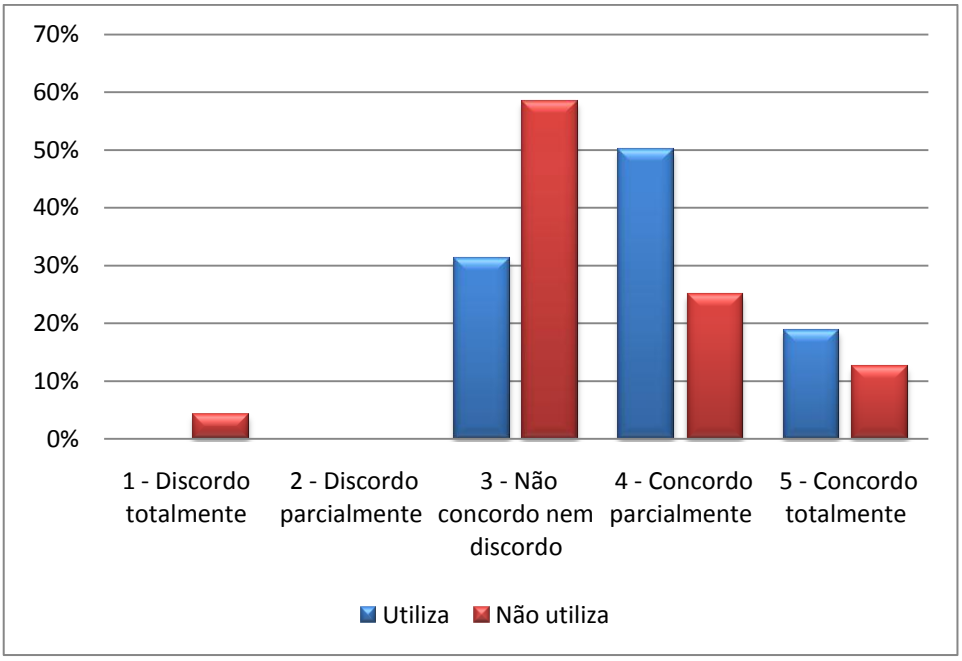
Analisando o gráfico das respostas recebidas, percebe-se que a maioria dos clientes não concordam e nem discordam com a afirmação de que a segurança no acesso e na realização de transações bancárias pela Internet através do Internet Banking do Banco Amarelo maior que a dos outros bancos. Do total de respondentes, 43% assim responderam. O restante ficou concentrado na afirmação de que concordam, com a soma de 55%. É difícil para o usuário comparar e fazer esta relação, ainda mais aqueles que não utilizam o Internet Banking por outro banco.

Por este motivo, fizemos uma relação com as respostas do questionamento sobre a utilização ou não do Internet Banking por outro banco, com suas respostas nesta questão.

Tabela 14 - Comparativo entre o uso ou não do Internet Banking por outro banco com a relação da segurança entre os bancos

	1 - Discordo totalmente	**2 - Discordo parcialmente**	**3 - Não concordo nem discordo**	**4 - Concordo parcialmente**	**5 - Concordo totalmente**	**Total**
Utiliza	0	0	10	16	6	**32**
Não Utiliza	1	0	14	6	3	**24**
Total	**1**	**0**	**24**	**22**	**9**	**56**

Gráfico 21 – Percentual do comparativo entre o uso ou não do Internet Banking por outro banco com a relação da segurança entre os bancos



Analisando quem utiliza o Internet Banking por outros bancos, nesta comparação, vemos que o percentual de quem não concorda nem discorda diminui, aponta 31%, o restante, 69%, concordam com a afirmação. Com certeza quem faz o aceso por outro banco, tem como relacionar melhor os dois sistemas e fazer esta análise. Muito importante este resultado para o Banco Amarelo, pois a confiança do cliente é importante para incentivar e manter o uso do canal de auto atendimento pela internet cada vez mais popular.

4.3.3 Questões Abertas

Foram relacionadas duas perguntas abertas no questionário de pesquisa aplicado aos clientes. A primeira delas indagando o que levaria o cliente a não utilizar o Internet Banking. Nas respostas relacionadas, percebemos que a maioria delas, cerca de 90%, esteve relacionada falta de segurança ou o acontecimento de alguma fraude no acesso. Isso nos mostra que os clientes que fazem uso desta ferramenta tem a preocupação quanto a segurança, assim como o banco também tem e trabalha para que isso não ocorra.

Seguem algumas respostas relevantes: “A diminuição dos itens de segurança, como por exemplo, o cadastro do computador, senhas diferentes para acesso e efetivação de transação, tempo de expiração da seção em 15 min, entre outros”.

“Talvez uma frequência de transtornos causados por rackers, como roubos, por mais que se saiba que o banco é responsável por monitorar isto, mesmo assim acho que ninguém quer ter incômodos e transtornos”.

A segunda questão traz a seguinte reflexão: Comente sobre a sua percepção quanto à segurança da informação no acesso bancário na Internet. Esta questão foi elaborada buscando obter respostas diretas dos clientes para a questão de pesquisa do trabalho, que busca descobrir percepção dos clientes pessoa jurídica quanto à sua responsabilidade perante a segurança no acesso ao Internet Banking. Através das respostas buscou-se observar se os clientes colocam apenas o banco como responsável por esta segurança, ou ele se incluem neste papel.

Os resultados não foram muito positivos, pois foram relacionadas poucas respostas com este aspecto. É citada uma delas: “Hoje considero bem seguro, desde que tomamos os cuidados de sigilo das senhas e antivírus ativado bem como sistema para evitar invasão”. A maioria dos respondentes relacionaram os mecanismos de segurança adotados pelos bancos em suas respostas, bem como o compromisso das instituições quanto a garantia desta segurança. Seguem algumas das respostas:

“Aparentemente parece ser muito seguro os dispositivos de segurança, tanto nas transações bancárias quanto no acesso, não costumava efetuar tantas operações pela internet quanto nos últimos tempos, mas sempre o receio quanto a segurança fica em aberto”.

“Atualmente tenho a percepção que os mecanismos estão mais seguros, sem que o usuário tenha que ficar preocupado ou alertado toda a vez que acessa ou processa uma transação on-line”.

“Desconheço qualquer ocorrência sobre fraude / clonagem através do uso do internet banking; no entanto, confesso que o que mais me atrai a utilizar essa ferramenta é realmente a rapidez e comodidade. Quanto à segurança, sei que em um eventual problema terei apoio do banco no que diz respeito à estorno e até mesmo reembolso de despesas indevidas. Indico o uso da internet banking a todos os conhecidos, tal a facilidade do acesso”.

A partir destes comentários, destaca-se que o conhecimento do cliente quanto aos mecanismos utilizados pelo bancos, e o compromisso das instituições quanto ao estorno de possíveis fraudes, deixam o cliente muitas vezes em um conforto que pode ser perigoso. Ele precisa ter a noção de que os cuidados que ele precisa tomar são iguais ou mais importantes do que as ferramentas que os bancos disponibilizam.

5 CONSIDERAÇÕES FINAIS

O atendimento aos clientes via internet tem crescido a cada ano e se mostrado cada vez mais seguro e importante para os usuários e instituições financeiras. Importante para os clientes devido à facilidade e praticidade na realização de suas transações financeiras e para os bancos pela diminuição no atendimento presencial nas agências, o que demanda mais funcionários e eleva os custos operacionais.

A segurança neste canal de auto atendimento vem aumentando, pois como o número de adeptos cresce, o número de transações e valores envolvidos nas transações também aumenta gradativamente, e com isso as instituições financeiras tendem a investir cada vez mais na sua segurança e na de seus clientes, pois precisam que este processo seja lucrativo para eles e a confiança do cliente não seja afetada.

Teve-se como premissa principal do trabalho identificar a percepção dos clientes pessoa jurídica que realizam transações financeiras através do Internet Banking quanto à importância e sua responsabilidade para garantia de um acesso seguro e confiável em agências bancárias da cidade de Joinville/SC. E este objetivo foi alcançado durante a aplicação do instrumento de pesquisa. Através deste questionário, aplicado a um percentual do público em questão, verificou-se o perfil do usuário, perfil da empresa por qual faz o acesso e o nível de conhecimento deste para com as medidas de segurança na internet, notou-se que a grande maioria tem conhecimento dos compromissos e cuidados que precisa tomar para tornar o seu acesso seguro e assim o faz. Quanto a responsabilidade do cliente neste processo, chegou-se a conclusão que muitos colocam o banco como principal responsável pela garantia da segurança, o que torna o acesso perigoso, caso estes não façam a sua parte.

Através de pesquisas junto às instituições financeiras, internet e publicações específicas, também foram classificados os métodos mais utilizados para ataques e invasões de informações bancárias; descritos e comparados os mecanismos de segurança adotados pelos bancos e relacionados os métodos e procedimentos necessários para que os clientes façam este acesso com segurança.

Os resultados encontrados são de grande importância, tanto para usuários de Internet Banking como para as instituições financeiras. Foi possível explorar os mecanismos de segurança por parte dos bancos e dos usuários, comparando-os e analisando-os, podendo assim verificar os diversos sistemas e indicações de segurança utilizados. Foi possível

também compreender o perfil e as características dos usuários deste serviço e se estão atentos a seus compromissos para um acesso seguro.

A desconfiança do público pesquisado quanto à veracidade da pesquisa foi um desafio do trabalho, superado posteriormente no andamento da aplicação do instrumento de pesquisa.

A empresa cujos clientes foram entrevistados, através da análise apresentada, terá a oportunidade de trabalhar junto a este público um maior entendimento e comprometimento quanto a responsabilidade dos usuários na segurança do acesso a transações financeiras pela internet.

Poderão também ser realizadas pesquisas futuras junto a clientes específicos de outros bancos, para trabalhar um comparativo maior na análise de resultados, trazendo mais informações para o banco já pesquisado e para os demais.

REFERÊNCIAS

ANTISPAM.BR. **O que é Spam.** Disponível em: < http://www.antispam.br/conceito/>. Acesso em: 28 set 2011.

CERT.BR. **Cartilha de segurança para internet.** Versão 3.1, 2006. Disponível em: <http://cartilha.cert.br/> Acesso em: 28 set 2011.

CLESIO, Flávio. Segurança da Informação – Básico**. Revista Info**. Disponível em: <http://info.abril.com.br/forum/seguranca>. Acesso em 20 jul. 2011.

CUNHA, Meire Jane Marcelo. **Proposta de documentação para subsidiar as atividades de implantação da Segurança da Informação.** 2005. Disponível em: <http://www.acso.uneb.br/marcosimoes/TrabalhosOrientados/CUNHA2005.pdf>. Acessado em: 12 out 2011.

D'ANDRÉA, Edgar R. P. et al. **Segurança em Banco Eletrônico.** São Paulo: PricewaterhouseCoopers, 2000.

DELGADO, Silvio. **Febraban divulga 20 passos de segurança.** Disponível em: <http://www.silviodelgado.com.br/febraban-divulga-20-passos-de-seguranca/>. Acesso em: 26 out 2011.

DINIZ, Eduardo H. **Evolução do uso da web pelos bancos.** RAC – Revista de Administração Contemporânea, Curitiba, v. 4, n. 2, p. 29–50, maio/ago. 2000.

_____. **Cinco décadas de automação. GV–Executivo. Editorial Era Digital. Edição especial 50 anos.** FGV–EAESP, São Paulo, v. 3, n. 3, p. 55–60, ago./out. 2004.

_____. **Redes locais e downsizing de sistemas de informação: um estudo em bancos brasileiros.** 108 f. Dissertação (Mestrado em Administração), FGV–EAESP, São Paulo, 1994.

FEBRABAN, Federação Brasileira dos Bancos. **Internet com segurança**. Disponível em: <http://www.febraban.org.br/Febraban.asp?id_pagina=115>. Acesso em 10 out 2011.

_____. **O setor bancário em números.** Disponível em: <http://www.febraban. org.br/Acervo1.asp?id_texto=214&id_pagina=85&palavra>. Acesso em: 10 out 2011.

GARCIA, Luciene. **Ataques virtuais a serviços bancários aumentam 45%.** Disponível em: <http://www.jornalacidade.com.br/editorias/economia/2011/10/24/ ataques-virtuais-a servicos-bancarios-aumentam-45.html>. Acesso em: 19 out 2011.

LANYWAY. **O que é SSL.** Disponível em: <http://www.laniway.com.br/br/ corporativo/certificado.do>. Acesso em: 20 out 2011.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente internet banking.** Dissertação (Mestrado em Engenharia) – Curso de Engenharia da Escola Politécnica da

Universidade de São Paulo, São Paulo, 2006. Disponível em: <http://teses.usp.br/teses/disponiveis/3142>. Acesso em: 15 jul. 2011.

OLIVEIRA, Wilson José de. **Segurança da Informação – técnicas e soluções.** Florianópolis: Visual Books, 2001.

RODRIGUES, Renato. **Segurança – ataques e ameaças.** Disponível em: <http://idgnow.uol.com.br/seguranca/2010/08/31/fraudes-online-deram-prejuizo-der900 - milhoes-em-2009-diz-febraban/>. Acesso em: 19 out 2011.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – uma visão executiva.** 12 ed. Rio de Janeiro: Elsevier, 2003.

SOUZA, Luis H. C. **Mensagem FEBRABAN. Segurança em Banco Eletrônico.** São Paulo: PricewaterhouseCoopers, 2000.

WEBER, Raul Fernando. **Segurança na Internet.** Porto Alegre: Instituto de Informática da Universidade Federal do Rio Grande do Sul, 1999. Disponível em: <www.inf.ufsc.br/~mauro/curso/redes/segur.doc >. Acesso em 20 jul. 2011.

WENDEL, Guglielmetti Henrique. **Malwares VS Antivírus.** Disponível em: <http://www.h2hc.com.br/repositorio/2007/wendel.pdf>. Acesso em: 20 out 2011.

WIKIPEDIA. **Segurança da informação.** Disponível em: <http://pt.wikipedia.org/wiki/Segurança_da_informação>. Acesso em 16 out 2011.

ANEXO A – INTRUMENTO DE PESQUISA

Questionário sobre a segurança da informação dos clientes pessoa jurídica no acesso ao Internet Banking do Banco Amarelo

Parte 1 - Caracterização da Empresa

1. Ramo de atividade da empresa onde você trabalha:

( ) Indústria

( ) Comércio

( ) Serviços

2. Tempo de atuação da empresa no mercado:

( ) Até 5 anos

( ) De 6 a 10

( ) De 11 a 20

( ) Mais de 20

3. Porte da empresa por faturamento anual:

( ) Microempresa - Menor ou igual a R$ 2,4 milhões

( ) Pequena Empresa - Maior que R$ 2,4 milhões e menor ou igual a R$ 16 milhões

( ) Média Empresa - Maior que R$ 16 milhões e menor ou igual a R$ 90 milhões

( ) Média-grande Empresa - Maior que 90 milhões e menor ou igual a R$ 300 milhões

( ) Grande Empresa - Faturamento maior que R$ 300 milhões

Parte 2 - Caracterização do Respondente

1. Faixa etária:

( ) Até 20 anos

( ) De 21 a 30

( ) De 31 a 40

( ) De 41 a 50

( ) Acima de 50 anos

2. Escolaridade:

( ) Ensino Médio

( ) Graduação

( ) Especialização

( ) Mestrado ou Doutorado

3. Cargo que ocupa na empresa: _____

4. Tempo em que trabalha na empresa:

( ) Até 5 anos

( ) De 6 a 10

( ) De 11 a 20

( ) Mais de 20

5. Você realiza transações financeiras pela Internet para a empresa onde trabalha através do Gerenciador Financeiro do Banco do Brasil?

( ) Sim

( ) Não

6. Se sim, com qual frequência?

( ) Diária

( ) Semanal

( ) Mensal

( ) Não utilizo

7. Há quanto tempo você faz o uso do Gerenciador Financeiro pela empresa?

( ) Até 2 anos

( ) De 3 a 6 anos

( ) Mais de 6 anos

8. Você realiza transações financeiras pela Internet para a empresa onde trabalha por outro banco?

( ) Sim

( ) Não

Parte 3 - Questões Objetivas

Avalie as afirmações a seguir de acordo com a escala: 1 - Discordo totalmente 2 - Discordo parcialmente 3 - Não concordo nem discordo 4 - Concordo parcialmente 5 - Concordo totalmente

1. Eu me sinto seguro(a) ao realizar transações financeiras pela Internet.

1 2 3 4 5

Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

2. Eu classifico os mecanismos de segurança do Internet Banking do Banco Amarelo como adequados.

1 2 3 4 5

Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

3. Eu conheço as recomendações dos bancos para um acesso seguro na Internet.

1 2 3 4 5

Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

4. Eu utilizo programas de antivírus no computador com o qual acesso o Internet Banking.

1 2 3 4 5

Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

5. Eu atualizo frequentemente o antivírus do computador com o qual acesso o Internet Banking.

1 2 3 4 5

Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

6. Eu costumo abrir e-mails de remetentes desconhecidos.

1 2 3 4 5
Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

7. Eu costumo acessar links recebidos por e-mail, independente do remetente.

1 2 3 4 5
Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

8. Eu mantenho os cuidados necessários quanto a elaboração, atualização e sigilo das minhas senhas de acesso ao Internet Banking.

1 2 3 4 5
Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

9. Eu considero a segurança no acesso e na realização de transações bancárias pela Internet através do Internet Banking do Banco Amarelo maior que a dos outros bancos.

1 2 3 4 5
Discordo totalmente ( ) ( ) ( ) ( ) ( ) Concordo totalmente

Parte 4 - Questões Abertas

1. O que levaria você a não utilizar o Gerenciador Financeiro?

_____

_____

_____

_____

2. Comente sobre a sua percepção quanto à segurança da informação no acesso bancário na Internet.

_____

_____

_____

_____