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

Luís Rafael Ferrari

A CONTRIBUIÇÃO DO BANCÁRIO NA SEGURANÇA DA INFORMAÇÃO DO CLIENTE USUÁRIO DO *INTERNET BANKING*

Porto Alegre
2011

Luís Rafael Ferrari

A CONTRIBUIÇÃO DO BANCÁRIO NA SEGURANÇA DA INFORMAÇÃO DO CLIENTE USUÁRIO DO *INTERNET BANKING*

Trabalho de conclusão de curso de Especialização, apresentado ao Programa de Pós-Graduação em Administração da Escola de 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

Tutora Orientadora: Me. Marinês Steffanello

Porto Alegre

2011

Luís Rafael Ferrari

A CONTRIBUIÇÃO DO BANCÁRIO NA SEGURANÇA DA INFORMAÇÃO DO CLIENTE USUÁRIO DO *INTERNET BANKING*

Trabalho de conclusão de curso de Especialização, apresentado ao Programa de Pós-Graduação em Administração da Escola de 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 aos meus pais, e minha esposa que sempre me deram apoio e incentivo, permitindo assim a sua realização.

AGRADECIMENTOS

Agradeço a Deus, por toda luz que me tem concedido.

Aos meus pais, pelos valores éticos e morais ensinados desde os primeiros anos de minha vida, minha eterna gratidão.

À Universidade Federal do Rio Grande do Sul e seus docentes pela dedicação e pelos ensinamentos recebidos.

A tutora orientadora Marinês Steffanello, pela amizade, dedicação e paciência na orientação deste trabalho. Sua orientação segura e seus comentários foram fundamentais para a realização deste estudo.

A minha esposa Fernanda pela paciência e pelo apoio que me deste para a realização deste trabalho.

Aos funcionários das agências bancárias que responderam aos questionários, minha sincera gratidão pelo precioso tempo dedicado a este trabalho.

“ ... nada é fixo para aquele que alternadamente pensa e sonha ... “

Gaston Bachelard

RESUMO

A realização do presente trabalho surgiu da necessidade de identificar quais aspectos podem ser melhorados no atendimento a clientes bancários pessoas físicas que utilizam o *internet banking*. Este trabalho trata-se de uma pesquisa realizada com bancários de algumas agências da Regional de Maringá sobre a orientação dos funcionários quanto à utilização do *internet banking* pelos clientes da instituição financeira. Considera-se que o objeto deste estudo não abrange todo o setor bancário do país, uma vez que os dados foram colhidos de algumas agências localizadas no norte do Estado do Paraná. No total foram enviados 67 questionários via *email* diretamente aos funcionários de nível operacional e gerencial que possuem contato direto com os clientes que utilizam o canal alternativo para suas transações bancárias, sendo que deste total 48 participaram da pesquisa. Através destes questionários analisou-se como a abordagem dos funcionários influencia a segurança das informações dos clientes pessoa física das agências de um banco do Paraná e corrobora na própria segurança dos dados bancários dos clientes. Com a realização deste estudo, evidenciou-se em qual ponto o funcionário é peça chave para redução das fragilidades dos usuários, iniciante ou não, e na consequente minimização de perdas com crimes virtuais. Além disso, verificou-se que a instituição financeira é tão responsável quanto o funcionário no estabelecimento de uma cultura de segurança.

Palavras chave: *internet banking*, fator humano, funcionalismo, riscos, fraudes eletrônicas.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O *internet banking* tem evoluído muito rapidamente em seus poucos anos de história. Entendendo-se por *internet banking* como a possibilidade de acesso às informações bancárias do cliente através do site. Este tipo de serviço se iniciou em 1996, quando apenas um grupo pequeno de bancos acreditou na w*eb* como um canal alternativo. Desde então, a ocupação da *web* como espaço para disponibilização de serviços bancários tem sido cada vez mais significativa, ao ponto de as principais instituições financeiras não conseguirem mais imaginar seus clientes sem acesso aos dados de suas contas bancárias pela *web*. O *internet banking* deixou de ser uma experiência arrojada de alguns e caminha para se tornar o principal elemento no conceito de serviços bancários virtuais (DINIZ; PORTO; SANTOS, 2007).

O conceito de segurança da informação sempre esteve associado às empresas ligadas a tecnologia da informação, entretanto esse conceito expandiu-se, atingindo todos os segmentos empresariais. Dentre estes segmentos, os bancos de varejo têm buscado cada vez mais oferecer aos seus usuários a conveniência dos canais alternativos como o *internet banking* (BEAL, 2005).

Atualmente, o desafio é maior para as empresas que dependem em maior grau dos meios informatizados para execução de suas transações de negócios. Para melhorar e desenvolver a segurança da informação nos ambientes corporativos é necessário disseminar seus princípios junto ao corpo funcional, independente de seu nível hierárquico, de forma a conscientizá-lo da importância do comprometimento de todos para sua efetivação.

De acordo com a Norma Brasileira 17799, que cobre os mais diversos tópicos da área de segurança, o primeiro passo para se estabelecer um ambiente que garanta a segurança da informação, é o desenvolvimento de uma política de segurança, na qual, entre outros fatores, sejam consideradas potenciais ameaças a este ativo, bem como os riscos de que estas ameaças possam explorar vulnerabilidades que comprometam a sua confidencialidade, integridade, disponibilidade e autenticidade, tornando a segurança da informação como preocupação constante para as empresas.

As empresas podem e devem lançar mão de diversas técnicas e procedimentos para eliminar ou atenuar os efeitos da concretização de ameaças sobre as informações corporativas, tanto no ambiente físico quanto no lógico, através de treinamento de equipes e simpósios, os quais contribuem para conscientização das pessoas, como pela adoção de sistemas

informatizados com credenciamento de acesso para sua utilização pelos usuários, e o estabelecimento de controle de acesso físico a áreas onde são armazenadas informações estratégicas da empresa.

Neste contexto, as instituições financeiras vêm desenvolvendo suas políticas internas de segurança, visto que a informação é tratada como ativo. Assim, qualquer perda ou dano à informação pressupõe perdas e risco de imagem das instituições envolvidas. A segurança é fator decisivo para um banco a ponto de comprometer todos os outros pertinentes ao negócio bancário (BEAL, 2005).

A proteção dos ativos de informação nas instituições financeiras deve ser tratada conforme seu impacto e alcançar todos os processos informatizados ou não. Também devem ser classificadas com base no grau em que os riscos são afetados em função da perda das propriedades de integridade, confidencialidade e disponibilidade. À medida que pessoas mal intencionadas esbarram na maior dificuldade tecnológica para obter ganhos espúrios, estes mesmos buscam utilizar o fator humano, seja ele interno ou externo em relação à instituição financeira, como brechas na segurança de seu próprio sistema (MITNICK, 2003).

A grande maioria dos incidentes tem a intervenção humana, seja de forma acidental ou não, a segurança está ligada a pessoas e processos, antes mesmo da tecnologia empregada, consequentemente, todos os recursos investidos em tecnologia da informação serão em vão se o fator humano for deixado em segundo plano. É sabido que os bancos possuem excelentes ferramentas de segurança, todavia os crimes virtuais continuam ocorrendo, logo algum aspecto pode ser melhorado (BEAL, 2005).

Quanto melhor preparados os funcionários, mais segura estará a organização e, por extensão, seus clientes. Nesse sentido, o presente trabalho visa responder a seguinte questão de pesquisa: **como a abordagem dos funcionários de uma instituição financeira pode influenciar na segurança das informações bancárias de seus clientes?**

1.1 OBJETIVOS

O objetivo geral da pesquisa é analisar a abordagem dos funcionários em relação à segurança das informações dos clientes pessoa física das agências do estado do Paraná de um banco público de atuação nacional.

Os objetivos específicos são os seguintes:

1. verificar se os funcionários possuem confiança em relação a segurança do *internet banking* da instituição onde trabalham e averiguar se os funcionários instruem corretamente seus clientes quanto a segurança da informação e ainda se os mesmos detém conhecimentos e são treinados para essa abordagem;

2. verificar qual dos participantes (instituição, funcionalismo ou usuário) é o maior responsável pelas perdas com fraudes eletrônicas e quais posturas a empresa pode adotar para que seu corpo funcional auxilie o cliente na tentativa de minimizar essas perdas.

3. Propor sugestões sobre posturas que a empresa pode adotar para que seu corpo funcional auxilie o cliente na tentativa de minimizar perdas a partir deste canal.

1.2 JUSTIFICATIVA

O investimento feito pelo setor bancário em segurança para as transações através do *internet banking* não tem tido o resultado esperado. No ano de 2009 as perdas financeiras representadas pelas investidas contra caixas eletrônicos e carros fortes, ações em que é utilizada força física, somaram no total, segundo a Federação Brasileira dos Bancos (FEBRABAN, 2009), cerca de R$ 50 milhões, enquanto os crimes virtuais em geral chegaram a R$ 900 milhões. Como ainda não há unanimidade jurídica com relação a esse tipo de crime, no que diz respeito à tratativa e ressarcimento, resta aos bancos minimizarem no que puderem as perdas com esse tipo de crime. Estes números demonstram que as instituições financeiras têm tido perdas financeiras significativas com investidas externas bem sucedidas contra os clientes, como por exemplo, capturas de senhas, páginas e *emails* falsos onde o cliente é enganado e pode ter seus dados sigilosos capturados. Assim, existe algo a mais que deve ser feito no momento da apresentação do canal pelos funcionários para que em conjunto com as ferramentas tecnológicas tenha o efeito esperado no sentido de maior proteção ao usuário.

É comum perceber o negócio principal de um banco pelo escopo financeiro, todavia com o advento de toda uma gama tecnológica e canais alternativos para transações essas empresas encontram-se diante de um novo paradigma. Antes mesmo que do escopo financeiro, é preciso ter a segurança nas informações, pois sem ela todos os demais aspectos estarão comprometidos.

Para tanto foram entrevistados funcionários de algumas agências bancárias no Paraná pertencentes a um banco público de atuação nacional, a partir da utilização de um

questionário composto por perguntas sobre a abordagem do funcionário quando no atendimento ao cliente.

1.3 ESTRUTURA DO TRABALHO

Além deste primeiro capítulo, com a introdução ao assunto abordado e sua justificativa para estudá-lo, o trabalho apresenta, em seu segundo capítulo, conceitos básicos sobre segurança da informação, envolvendo quesitos específicos como *internet*, informação bancária e a relação do funcionário com o cliente a fim de minimizar os riscos do mesmo.

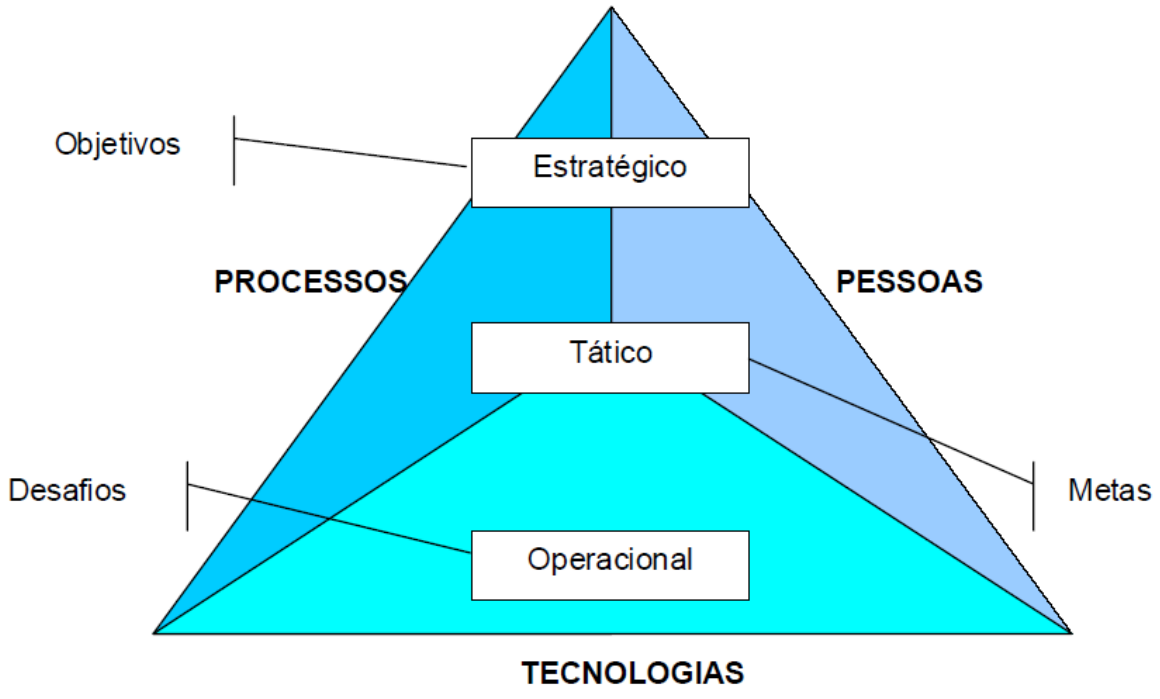
A seguir, serão apresentadas seções que abordarão os conceitos dos temas focados neste trabalho, o método utilizado para coleta dos dados da pesquisa, em seu capítulo 3; a apresentação e análise dos dados coletados e suas discussões acerca do tema apresentado e proposto; e, por fim, no capítulo 5, as conclusões do estudo com indicação das limitações e recomendações para pesquisas futuras.

2. O VALOR DAS INFORMAÇÕES

Este capítulo aborda definições importantes a cerca da segurança da informação, em especial no contexto bancário onde a confidenciabilidade é tratada como risco de imagem e é fundamental para a credibilidade da instituição.

A informação é o dado com uma interpretação lógica ou natural dada a ele por seu usuário (REZENDE; ABREU, 2000). Assim sendo, a informação é um conjunto de dados organizados onde ao mesmo tempo integra processos, pessoas e tecnologia, representando, ainda, vantagem competitiva para quem a possui e sabe utilizá-la em seu benefício. Segurança da informação é garantir que as informações estejam protegidas contra o acesso de pessoas não autorizadas, estando sempre disponíveis e sejam confiáveis (REZENDE e ABREU, 2000).

Figura 1 – Relacionamento de processos, pessoas e tecnologias.



Fonte: Laureano (2005).

A informação é um ativo que como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente precisa ser adequadamente protegida.

A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa (SÊMOLA, 2003).

É o bem mais importante para as pessoas e para as organizações e antigamente essas informações ficavam armazenadas em um único ambiente isolado. Atualmente são processadas, armazenadas e compartilhadas em um complexo ambiente tecnológico com grande disponibilidade, portanto necessitam de proteção (BRASIL, 2007).

2.1 SEGURANÇA E INFORMAÇÕES

De acordo com Caruso e Steffen (1999, p. 21), implantar um sistema de segurança num ambiente de informações seja do ponto físico ou lógico, não significa dizer que se atinge a perfeição no item, e sim, que esse sistema tem como objetivo eliminar o "máximo de pontos fracos ou garantir o máximo de segurança possível para os mesmos". Zerar os riscos é impossível, visto que da mesma maneira que novos controles são criados, existe também o desenvolvimento de novas técnicas para burla desses mesmos controles.

O objetivo da segurança, no que tange à informação, é a busca da disponibilidade, confidencialidade e integridade dos seus recursos e da própria informação (MOREIRA, 2001). A disponibilidade caracteriza o acesso contínuo e ininterrupto aos recursos da organização. A informação deve estar disponível para a pessoa certa no momento em que ela precisar. A integridade consiste em proteger a informação contra qualquer tipo de alteração sem a autorização explícita do autor da mesma. A perda da integridade pode ser intencional ou não e deve se levar em consideração quanto que a organização vai gastar para recuperar ou reconstituir os dados. A confidencialidade é a propriedade que visa manter o sigilo, o segredo ou a privacidade das informações evitando que pessoas, entidades ou programas não autorizados tenham acesso às mesmas. Infelizmente, grande parte das pessoas não tem a consciência de que, uma vez conectados à Internet, as informações podem não se tornar tão confidenciais quanto se imagina ou gostaria que estivessem (MOREIRA, 2001).

Sempre houve a preocupação de proteger a informação, entretanto, com o advento e o desenvolvimento da informática, alterou-se a relação de registro das mesmas. A informática possibilitou que a informação passasse a ter um significado maior para as empresas e que aumentasse sensivelmente o poder de armazenamento das mesmas. Onde antes necessitava de um grande espaço físico para papéis, alterou-se para computadores de grande porte (no início)

e com a chegada do microcomputador quebrou-se o paradigma da informação com o usuário: antes a informação não tinha mobilidade, pois se restringia aos profissionais de linguagem de programação (BEAL, 2005).

Com o advento da microinformática grande parte do corpo funcional tem acesso aos dados, variando conforme a sua função e nível hierárquico. As instituições ganharam em agilidade, mas abriram brechas para vazamento das informações visto que, o micro é um meio de registro, de alteração, armazenamento, acesso e de divulgação dos dados. As ameaças aumentaram com a chegada da internet, que, conectada a rede interna da empresa, tornou-se uma perigosa porta de entrada e saída de dados e informações. Diversas empresas direcionam seus esforços para preservação dos seus ativos físicos e financeiros, mas não se empenham com a mesma intensidade para manter a integridade das informações que possuem como: cadastro dos clientes e fornecedores, políticas estratégicas, de marketing, processos de produção, etc. Às vezes possuem uma estratégia eficiente quanto a segurança das informações, restringindo acessos físicos e lógicos, mas se esquece de um fator fundamental: o ser humano, um dos pontos mais frágeis da relação, suscetíveis a humores, realizações e sentimentos os mais variados possíveis. A relação empresa-funcionário deve ser um fator de importância na estratégia da empresa e, principalmente, numa instituição financeira, onde seus produtos/serviços são ativos financeiros (BEAL, 2005).

Numa instituição financeira, esses ativos financeiros não ficam restritos aos setores de informática (Centros de Processamento de Dados, Diretoria de Tecnologia, etc.), eles se encontram em todas as agências bancárias, espalhadas pelo país. Eles não se encontram apenas no ambiente informatizado, mas na maioria das vezes, estão em papéis e documentos arquivados fisicamente. Para os clientes operarem com o banco necessitam assinar contratos, cédulas entre outros e esses documentos devem ser mantidos mesmo após findar sua validade com prazos de expurgos diferenciados. Todavia já surge um novo método de relação negocial banco-cliente, os chamados certificados digitais permitem fechamento de contratos eletronicamente com razoável segurança (BEAL, 2005). Um exemplo prático são os contratos de câmbio que já são fechados através da internet via certificado digital (FONTES, 2008).

Como os bancos são altamente dependentes da informática, a preocupação com a segurança da informação é proporcional a necessidade de preservação da imagem para essas empresas. Pode-se perceber que tanto os bancos procuram não divulgar dados sobre invasões em seus servidores e tentam agora também não publicar nada sobre crimes virtuais que atingem seus clientes (CARUSO; STEFFEN, 1999).

As empresas teriam dificuldades de sobrevivência se passassem por uma crise no setor da segurança da informação, no caso dos bancos isso representaria risco direto de imagem e operacional. Para isso existem planos de contingência que visam minimizar estes impactos na rotina de um banco. Qualquer tipo de indisponibilidade pode afetar a imagem de um banco e desencadear uma crise de confiança dos aplicadores. Segurança da informação é garantir que as informações estejam protegidas contra o acesso de pessoas não autorizadas, estando sempre disponíveis e que sejam confiáveis. O treinamento do corpo funcional da empresa é de suma importância (CARUSO; STEFFEN, 1999).

Para Albertin (2004, p. 32) o conceito de comércio eletrônico, aplicado também ao *internet banking*, é amplo e abrangente, e é caracterizado como uma aplicação intensa de tecnologias de comunicação e de informação, atendendo os objetivos do negócio, por meio de processos no ambiente eletrônico. Já Cernev e Leite (2005, p. 5) citam que o receio com a segurança das transações via *internet banking* é um dos principais obstáculos para o seu crescimento.

Segundo Albertin (2004, p. 46), o preço da falta de segurança e de controle ou da omissão quanto a esses deveres tem sido cada vez mais alto para as pessoas, para as instituições e a sociedade de um modo geral. As facilidades e as disponibilidades do ambiente tecnológico geram conforto, mas, ao mesmo tempo, colocam o crime cada vez mais próximo das pessoas, exigindo cuidados adicionais. Exemplo disso é a *internet* com todas as suas inúmeras possibilidades e conveniências, entretanto a falta de controle e legislação específica tem causado prejuízos aos usuários, principalmente no caso do *internet banking*.

O crescente uso da rede seja para consultar um saldo bancário, seja para comprar um livro, envolve envio ou recepção de informações, que devem ser protegidas. A rede é aberta a todos que se conectarem a ela, visita-se uma página, de qualquer assunto, quem quiser e a hora que quiser, porém, como ferramenta de comunicação que é, não deve sofrer censura (GAMA, 2000).

Atualmente a mudança dos processos de mecânicos para virtuais ou automatizados, provocaram também uma virtualização do crime criando métodos novos de riscos, tais como roubo de informações pela internet, invasão de redes de comunicação de dados, fraudes eletrônicas e sabotagem virtual, causando paralisação de negócios. Algumas tipologias de crimes com o chamado uso da força bruta não sofreram muitas alterações como, por exemplo, os assaltos, sequestros e arrombamentos, não incomuns para as instituições financeiras no Brasil (SCHNEIER, 2001).

Estima-se que o crime movimenta anualmente cerca de US$ 3 trilhões em todo o mundo, representando, segundo a Organização das Nações Unidas (ONU), de 2% a 5% do PIB mundial. De acordo com os mesmos estudos, pelo menos US$ 1,5 trilhão circulam pelo sistema financeiro. Os dados da ONU indicam que as organizações criminosas também utilizam, para suas operações financeiras ilícitas, inclusive lavagem de dinheiro, do sistema financeiro mundial com as suas modernas redes de comunicação de dados e amplo nível de disponibilidade e acesso à clientela via *internet banking* (MITNICK, 2003). Mas, o sistema financeiro não está apenas sujeito a ser usado para operações financeiras ilícitas. Ao longo da história, os bancos têm sido vítimas diretas de crimes financeiros praticados por agentes internos ou externos – algumas vezes pelos dois. Um exemplo é o banco francês Societé Generale que sofreu perdas estimadas em US$ 7 bilhões por fraude praticada por um único funcionário durante o período de 01 ano (2007). Além do prejuízo financeiro, a fraude interna teve repercussão mundial e causou danos profundos à imagem do banco e à vida de seus dirigentes e funcionários (MITNICK, 2003).

As possibilidades do crime podem ter aumentado com as facilidades de acesso à comunicação e as disponibilidades do ambiente financeiro e comercial. Contudo, a diferença entre o uso confortável, sadio e produtivo desses aspectos passa por uma adequada atenção pessoal e corporativa com aspectos básicos de controle e segurança (ALBERTIN, 2004).

No contexto social, percebe-se claramente o ciclo e a correlação de problemas graves resultantes de um ambiente instável do ponto de vista de segurança. Qualquer esforço integrado entre o Estado e a sociedade/cidadão pode contribuir para a redução desses impactos (SCHNEIER, 2001).

No ambiente corporativo, o processo de segurança por estar diretamente envolvido com a proteção dos ativos e a eficácia dos negócios, mostra-se de forma mais objetiva, dinâmica a abrangente. O fato é que a grandiosidade dos riscos, especialmente nas instituições financeiras, provocou a incorporação das estruturas de segurança aos primeiros níveis hierárquicos de grandes bancos em todo o mundo, solidificando a governança corporativa na perspectiva de aumentar as condições internas para a identificação, prevenção e resposta a delitos, além da gestão de planos de continuidade de negócios e ações de educação e cultura em segurança (BEAL, 2005).

A composição do quadro funcional da empresa é muito importante antes de iniciar qualquer estudo ou tratativa sobre segurança, seja em qualquer aspecto (REZENDE, 2000). As necessidades funcionais da empresa, o perfil do funcionário, estagiário, parceiro, etc., devem ser bem definidas de forma que possibilite uma melhor interação entre as partes. Essa

relação deve ser acompanhada, estimulada, avaliada de forma que os objetivos da instituição sejam alcançados e seus “bens” tangíveis e intangíveis preservados.

Essa chamada “camada humana” é que oferece maior dificuldade para mensuração de riscos e gerenciamento da segurança tendo em vista os fatores intrínsecos do ser humano como emoção, aspectos sócio-culturais e psicológicos (SCHNEIER, 2001). Assim os bancos têm duplo desafio, ou seja, podem sofrer perdas financeiras advindas da fragilidade dessa camada tanto por parte de seu quadro funcional quanto de seus clientes que usam os canais virtuais.

2.2 FATOR HUMANO

A segurança é uma cadeia formada por vários elos, tão forte quanto o seu elo mais fraco. Segurança da informação, em particular, é uma cadeia que tem entre seus elos tecnologia, processos e pessoas. Os especialistas em Segurança da Informação são unânimes em apontar as pessoas como o elo mais fraco (CUNHA, 2007).

O usuário é quem inicia um processo ou procedimento, e é ele que tem o poder de decisão de ignorar algo que possa colocá-lo em risco (SÊMOLA, 2008).

O usuário é peça fundamental nos processos de segurança da informação. Essas mesmas pessoas são um fator crítico para o sucesso do processo de proteção da informação. A tecnologia existente possibilita à organização ter uma boa proteção, mas quem vai garantir que ela tire proveito dessa tecnologia e implemente de forma efetiva os controles adequados é o usuário (FONTES, 2008). Entretanto, é papel da organização zelar por seu recurso humano através de programas de conscientização e treinamento, pois o mesmo é fator crítico para o sucesso na proteção da informação (FONTES, 2008).

O usuário deve ter atenção tanto ao controle lógico quanto físico. Ele é responsável pela segurança de sua informação, entretanto a organização, destaca-se aqui as instituições financeiras, devem prover outros meios e funcionalidades, entre elas dispor de colaboradores também comprometidos com a segurança da informação que auxiliem o usuário a compreender melhor os riscos e sua responsabilidade no processo.

A maneira com que será realizada a conscientização dos usuários com relação a necessidade de segurança da informação é flexível, devendo se adaptar à realidade de cada organização. Para que as pessoas se desenvolvam no que se refere à segurança da informação

deverão existir recursos financeiros disponíveis, investimento de tempo das pessoas, alinhamento com a estratégia de negócio, planejamento de atividades e trabalho constante. Este processo deve abordar toda a organização, independentemente de níveis hierárquicos (FONTES, 2008).

O usuário deve entender que o processo de conscientização em segurança não existe simplesmente por existir ou por exigência dos responsáveis pela segurança da informação. O foco da conscientização é o usuário e ela acontece dentro dos processos de segurança da informação, mas sua motivação maior é proteger de acessos não autorizados os bens de informação necessários para a realização do negócio da organização (FONTES, 2008).

A preocupação com a maneira de utilização do *internet banking* pelos usuários é latente entre os bancos, tanto que para a FEBRABAN (2000) a segurança é um processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados. A federação ainda disponibiliza em seu site na internet os 20 mandamentos do acesso seguro às transações eletrônicas, entre eles destacam-se os relacionados ao uso do *internet banking*:

11. Se for efetuar compras com seu cartão pela Internet, procure, antes, saber se o site é confiável e se tem sistema de segurança para garantia das transações;

13. Atenção com e-mails de origem desconhecida, que aguçam a sua 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, delete o e-mail antes mesmo de abri-lo;

14. Mantenha seu sistema operacional e programas antivírus atualizados;

15. 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, de seu local de trabalho ou estudo que são compartilhados com outras pessoas;

16. Troque periodicamente a senha utilizada para acessar seu banco na Internet;

18. Se estiver em dúvida em relação à segurança de algum procedimento no Internet-banking, entre em contato com o banco. Prevenção é a melhor forma de segurança;

19. Acompanhe os lançamentos em sua conta corrente. Caso constate qualquer crédito ou débito irregular, entre imediatamente em contato com o banco;

20. Na desconfiança do acesso à página de seu Internet Banking, clique na barra superior de seu browser e movimente a janela, caso algum conteúdo existente na página não

acompanhe sua movimentação pode ser o indício de um programa espião em seu computador (Agite seu Internet Banking antes de usar).

Essa preocupação tem explicação uma vez que o setor bancário é o principal alvo dos criminosos virtuais e a fragilidade não está no aparato tecnológico e sim no fator humano, seja ele pertencente ao corpo funcional ou usuário final.

2.3 CRIMES VIRTUAIS

Os delitos praticados com o uso de computadores ou através da internet, são definidos como sendo aqueles em que o computador é o instrumento para a execução do crime, podendo também, ser o meio para atingir um propósito ilícito (GAMA, 2000).

Crimes virtuais são todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar (CORRÊA, 2000).

Os crimes virtuais são classificados em categorias, as quais são: puro, misto e comum. O crime virtual comum tem o objetivo exclusivo de danificar o sistema de computador, sendo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas. Crime virtual misto seria aquele que a internet é a principal ferramenta para a efetivação da conduta ilícita, a qual, por exemplo, pode ser as transferências de valores em um *internet banking*, onde o cracker retira diariamente pequenas quantias de dinheiro de milhares de contas bancárias e as transfere para uma conta. O crime virtual comum seria a utilização da internet apenas como forma de instrumento para realizar um delito que enquadra no Código Penal, como, por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, como *messengers*, e-mail ou outra forma de compartilhamento de dados (PINHEIRO, 2001).

ROSSINI (2002) demonstra algumas táticas para a violação da privacidade na rede mundial, dentre outras cita:

- *Spamming*: forma de envio de mensagens publicitárias por correio eletrônico a grupo deusuários da rede;

- *Cookies*: são pequenos arquivos de textos que são gravados no computador do usuário pelo browser quando ele visita determinados sites de comércio eletrônico, de forma a identificar o computador com um número único, e obter informações para reconhecer quem

está acessando o site, de onde vem, com que periodicidade costuma voltar e outros dados de interesse do portal;

- *Spywares*: programas espiões que enviam informações do computador do usuário da rede para desconhecidos, de maneira que até o que é teclado é monitorado como informação, sendo que alguns *spywares* têm mecanismos que acessam o servidor assim que usuário fica on-line e outros enviam informações por *email*;

- *Hoaxes*: são e-mails que possuem conteúdos alarmantes e falsos, geralmente apontando como remetentes empresas importantes ou órgãos governamentais, como as correntes ou pirâmides, *hoaxes* típicos que caracterizam crime contra a economia popular, podendo, ainda, estarem acompanhadas de vírus;

- *Sniffers*: programas espiões, semelhantes aos *spywares*, que, introduzidos no disco rígido, visam a rastrear e reconhecer *emails* que circulam na rede, de forma a permitir o seu controle e leitura;

- *Trojan horses* ou cavalos de tróia: abrem portas, tornando possível a identificação de informações, como senhas, arquivos etc.

Os crimes tradicionais relacionados à informática, descritos na legislação penal em vigor, mereceriam ser definidos em lei especial, para melhor interpretação e adequação. Com os recursos que a informática pode oferecer, a conduta delituosa chega quase que a perfeição dificultando, em muito, a sua identificação (GAMA, 2000).

Nos últimos cinco anos, houve uma crescente preocupação da comunidade com o abuso e a apropriação de informações eletrônicas e o uso de computadores para cometer crimes. A tendência do não uso de documentos de papel está tendo um enorme impacto na natureza de crimes tradicionais como, o roubo, a fraude e a falsificação. A introdução do dinheiro eletrônico, compras on-line e acesso a sistemas de computadores privados, trarão formas de crimes eletrônicos que irão requerer regulamentação e controle legislativo. A disponibilidade de computadores e a confiança da comunidade no sistema de informações são um valioso recurso para organizações e indivíduos potencializarem o uso dos computadores nos crimes que envolvem fraude, pornografia, drogas, pedofilia, direitos autorais, e espionagem (THOMPSON e BERWICK apud GAMA, 2000).

A proteção de contra senha é freqüentemente utilizada como um dispositivo protetor contra acesso sem autorização, porém, o *hacker* moderno pode evitar esta proteção, descobrindo a contra senha que lhe permite o acesso, introduzindo programa específico para este fim que irá capturar outras senhas de usuários legítimos. Se a intenção do agente for a de apenas penetrar no sistema, driblando a segurança, este será denominado hacker, mas se a

intenção for a de causar dano ou cometer outro ilícito, a denominação correta será *cracker* (GAMA, 2000).

As fraudes virtuais são utilizadas em muitos casos de crimes econômicos, como manipulação de saldos de contas, balancetes em bancos, transferências de dinheiro, etc, alterando, omitindo ou incluindo dados, com o intuito de obter vantagem econômica. A fraude virtual é o crime de computador mais comum, mais fácil de ser executado, porém, um dos mais difíceis de ser esclarecido. Não requer conhecimento sofisticado em computação e pode ser cometido por qualquer pessoa que obtenha acesso a um computador e a uma linha telefônica. Tradicionalmente a fraude envolve o uso de dados bancários roubados ou furtados (GAMA, 2000).

O posicionamento jurídico com relação às fraudes eletrônicas e sobre o dever de indenizar tem sido proferido, geralmente, em favor do usuário dado a sua hipossuficiência. Apesar de o código civil não tratar especificamente da matéria eletrônica, algumas disposições adaptam-se perfeitamente nas questões jurídicas referentes a internet (PAESANI, 2003).

3 MÉTODO

No desenvolvimento deste trabalho, foram utilizados os métodos de pesquisa aplicada e elaboração de questionário para realização do estudo.

O trabalho é apresentado na forma de estudo de caso, pois, segundo Gil (1996, p.56), baseado em levantamento de dados que consiste na interrogação direta das pessoas cujo comportamento se deseja conhecer. Basicamente, procede-se à solicitação de informações a um grupo significativo de pessoas a cerca do problema estudado para, em seguida, mediante análise quantitativa, obterem-se as conclusões correspondentes aos dados coletados.

Atualmente, o estudo de caso é adotado na investigação de fenômenos das mais diversas áreas do conhecimento. O estudo de caso pode ser visto como técnica psicoterápica, como método didático ou como método de pesquisa. Neste último sentido, que é o que interessa pode ser definido como:

> "... um conjunto de dados que descrevem uma fase ou a totalidade do processo social de uma unidade, em suas várias relações internas e nas suas fixações culturais, quer seja essa unidade uma pessoa, uma família, um profissional, uma instituição social, uma comunidade ou uma nação" (YOUNG, 1960 apud GIL, 1996).

3.1 EMPRESA ESTUDADA

O objeto da pesquisa foi dirigido aos funcionários de algumas agências de uma instituição financeira de abrangência nacional, de um banco público. Este banco possui diversas agências em todos os estados brasileiros que são divididas em regionais. A região selecionada para este presente estudo foi a chamada regional de Maringá, que engloba cidades do noroeste do Paraná. Entretanto, não foram entrevistados funcionários de todas as agências desta regional, pois, demandaria o envio do questionário aplicado para 46 agências.

A escolha de diferentes unidades bancárias foi feita exatamente para demonstrar que em grandes centros ou cidades do interior as perdas financeiras, decorrentes de crimes virtuais contra clientes e para o conglomerado, são representativas e fornecem a pesquisa uma variedade interessante de situações. Entretanto, os questionários enviados aos funcionários

por *email* destas unidades foram idênticos tendo em vista que as perguntas relacionadas são aplicáveis a todas essas agências.

A amostragem de funcionários reuniu quadros funcionais de tamanhos distintos e localizadas em praças com diferentes particularidades. O Quadro 1 apresenta o número de funcionários nas agências desta região.

Figura 2 – número de funcionários das agências da Regional de Maringá

Agência	**Dotação**	**Trabalham com Pessoa Física**
Paraíso do Norte	14 funcionários	05 funcionários
Astorga	25 funcionários	10 funcionários
Santa Fé	05 funcionários	02 funcionários
Canção-Maringá	44 funcionários	15 funcionários
Centro-Maringá	80 funcionários	35 funcionários

Fonte: Sindicato dos Bancários de Maringá e Região (2011)

A partir deste cenário, o instrumento de pesquisa foi dirigido às agências de acordo com a dotação mínima para cada setor, sendo que os funcionários participantes da pesquisa eram atendentes do segmento pessoa física. A amostra total selecionada foi de 67 funcionários e o perfil destes respondentes estarão explicitados no capítulo seguinte.

Os dados obtidos através dos questionários abrangeram estas 5 agências especificadas acima, sendo que somente 48 funcionários participaram do estudo (71,64% do quadro de funcionários das agências pesquisadas).

3.2 COLETA E ANÁLISE DOS DADOS

A pesquisa foi aplicada através de questionário estruturado, elaborado pelo autor, enviado por *email* e abordou assuntos como método de acesso ao *internet banking,* confecção de senhas, rotinas de segurança, ferramentas de diagnóstico, *check-list* para utilização. O questionário utilizado como instrumento de pesquisa está apresentado em anexo.

Os funcionários respondentes estão ligados ao atendimento de pessoas físicas nas agências de nível operacional, ou os escriturários, assistentes de negócios e gerente de contas que na verdade são os colaboradores que efetuam o contato direto com os clientes, apresentam

as ferramentas de auto-atendimento pela *internet* e que teriam o papel de instruir sobre o uso racional e seguro desse canal.

O período de envio e retorno dos questionários compreendeu os primeiros quinze dias do mês de outubro de 2011.

Segundo, Amaro, Póvoa e Macedo (2004), para elaboração de um questionário é importante, antes de mais, ter em conta as habilitações do público-alvo a quem ele vai ser administrado. Assim, elas devem ser desenvolvidas tendo em conta três princípios básicos: o Princípio da clareza (devem ser claras, concisas e unívocas), Princípio da Coerência (devem corresponder à intenção da própria pergunta) e Princípio da neutralidade (não devem induzir uma dada resposta, mas sim libertar o inquirido do referencial de juízos de valor ou do preconceito do próprio autor).

A escala utilizada para elaboração do questionário foi a escala de Likert. Esta escala apresenta uma série de cinco proposições, das quais se deve selecionar uma, podendo estas ser: concorda totalmente, concorda, neutra, discorda, discorda totalmente (AMARO, PÓVOA, MACEDO, 2004). Neste trabalho, utilizou-se a pontuação de 1 a 5.

Os dados obtidos foram analisados estatisticamente a fim de traçar o perfil do funcionário que orienta os clientes. Através de gráficos foi possível visualizar o comportamento, onde ocorrem falhas ou ainda a falta de conhecimento dos funcionários na orientação aos futuros e atuais clientes do *internet banking*.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

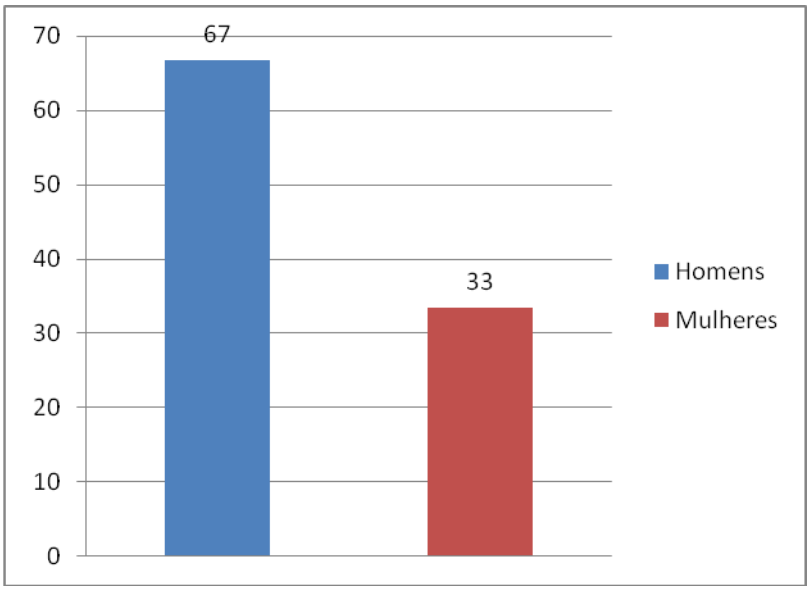
Este capítulo apresenta os resultados coletados nesta pesquisa a partir do questionário aplicado nas agências de uma instituição financeira do Paraná. Dos 67 questionários enviados 48 responderam correspondendo a uma taxa de 71,64% de retorno.

A análise dos resultados obtidos foi expressa em gráficos gerados com as respostas dadas pelos funcionários e a pesquisa anexada no final deste estudo.

4.1 CARACTERIZAÇÃO DA AMOSTRA

No quadro funcional total do banco analisado o percentual de homens é de pouco mais de 50%, ou seja, existe quase uma equiparação entre homens e mulheres. Neste gráfico abaixo visualiza-se que a maior parte dos respondentes da pesquisa foram do sexo masculino.

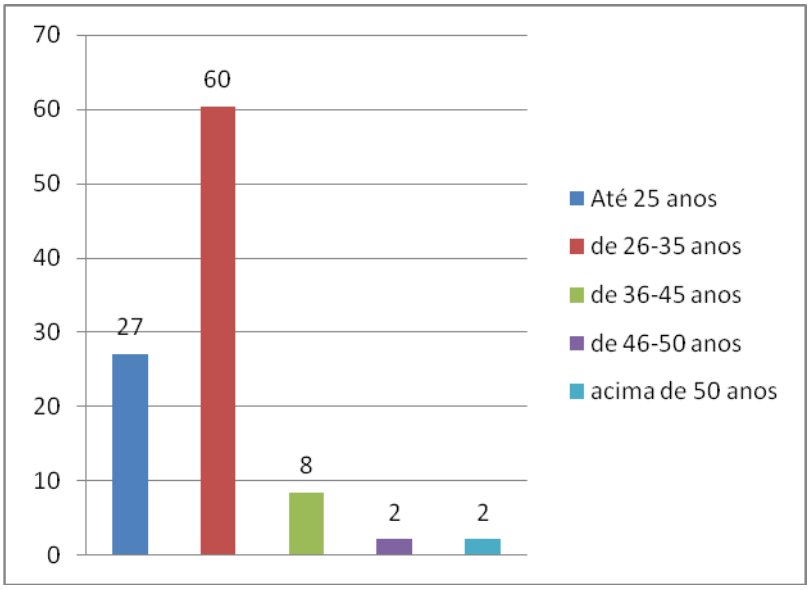
Gráfico 1 – Distribuição por sexo dos funcionários analisados.



No gráfico abaixo, verificou-se que houve maior participação dos funcionários que encontravam-se na faixa etária de 26 a 35 anos, correspondendo a 29 funcionários, representando 60% (sessenta por cento) do total analisado.

Nos dados obtidos pela pesquisa, dos 48 pesquisados, constatou-se que 13 funcionários encontravam-se na faixa etária de até 25 anos, correspondente a 27% (vinte e sete por cento) do total de participantes. Na faixa etária de 36 a 45 anos, verificou-se a participação de 4 funcionários, relacionado a 8% (oito por cento) do total de participantes. Na faixa etária de 46 a 50 anos, verificou-se a participação de 1 funcionário, correspondendo a 2% (dois por cento) do total analisado e na última faixa etária analisada, dos funcionários que possuíam acima de 50 anos, observou-se a participação de 1 funcionário, correspondendo a 2% (dois por cento) do total de 48 participantes do estudo.

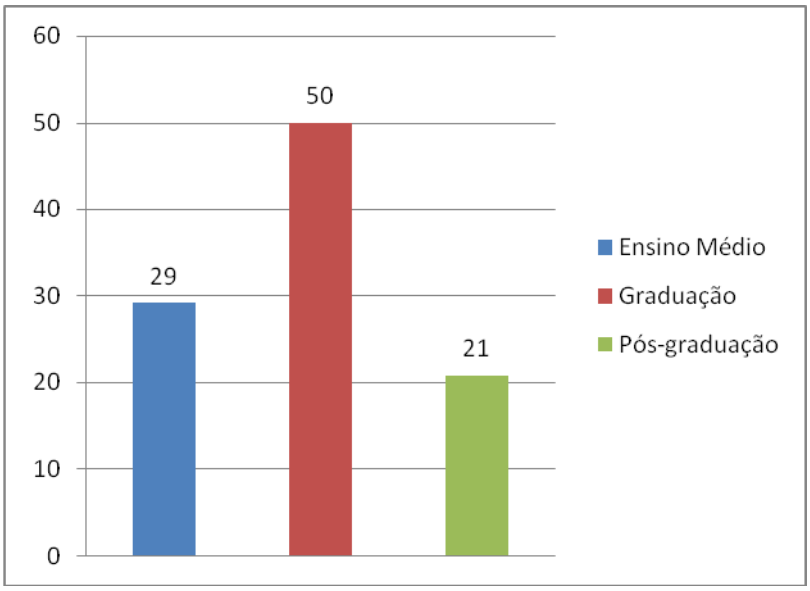
Gráfico 2 - Distribuição por idade dos funcionários analisados.



Representando 50% (cinquenta por cento) do total analisado, 24 funcionários possuíam graduação em termos de escolaridade.

Na análise dos dados, observou-se que do total de 48 participantes, 10 funcionários possuíam pós-graduação, representando 21% (vinte e um por cento) do total analisado e 14 funcionários possuíam somente o ensino médio, correspondendo a 29% (vinte e nove por cento) do total de 48 participantes do estudo.

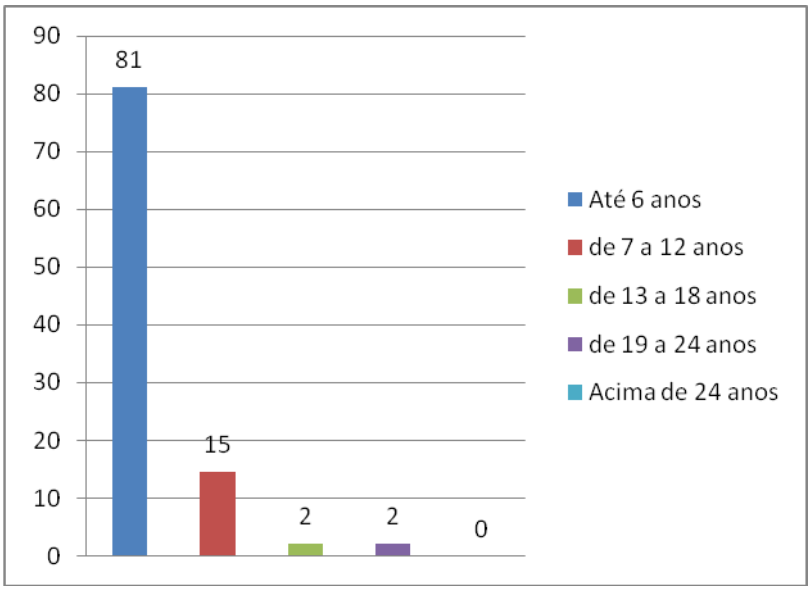
Gráfico 3 – Distribuição por escolaridade dos funcionários analisados.



Representando 81% (oitenta e um por cento) do total de analisados, verificou-se uma maior participação de funcionários que possuíam até 6 anos na carreira bancária, correspondendo a 39 funcionários do total de pesquisados.

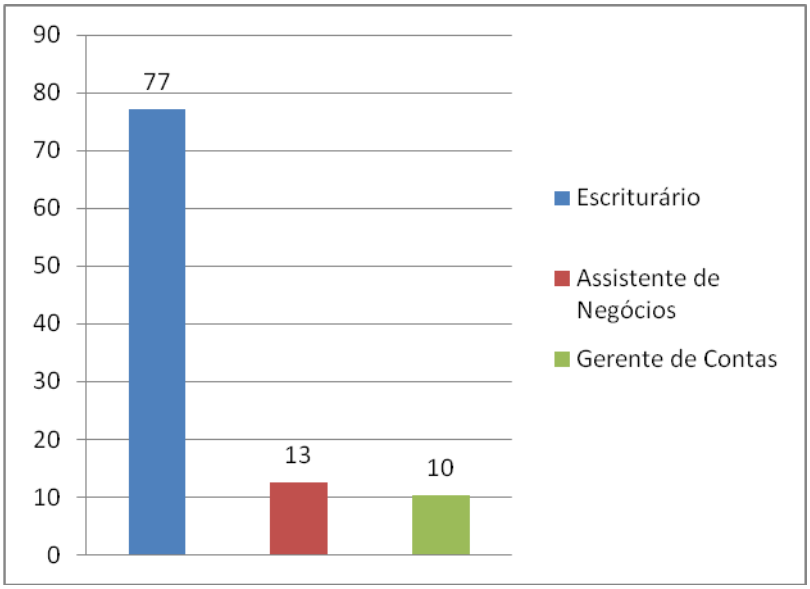
Na análise dos dados observou-se que do total de 48 participantes, 7 funcionários possuíam de 7 a 12 anos, correspondendo a 15% (quinze por cento) do total. Funcionários com tempo de banco de 13 a 18 anos representaram 2% (dois por cento), correspondendo a 1 funcionário do total analisado. Representantes da pesquisa com tempo de banco de 19 a 24 anos, obtiveram participação de 2% (dois por cento) correspondendo a 1 funcionário do total analisado. Funcionários que são bancários há mais de 24 anos não responderam a esta pesquisa.

Gráfico 4 - Distribuição dos funcionários por tempo de banco.



Nos dados obtidos na pesquisa efetuada, verificou-se uma maior participação dos funcionários que exerciam o cargo de escriturário nas agências bancárias. A amostra é composta por uma maioria de escriturários 77%, seguida de 13% de assistentes de negócios e 10% de gerentes de contas.

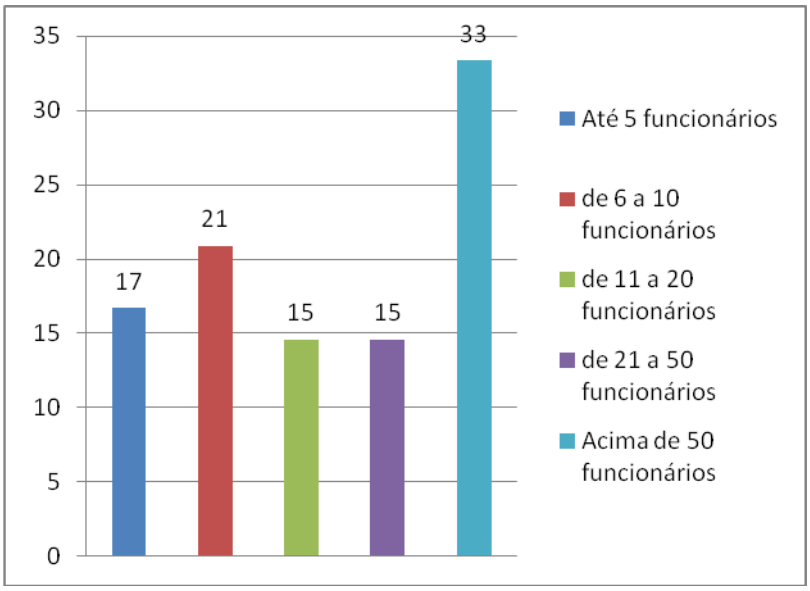
Gráfico 5- Distribuição dos funcionários por cargo exercido na agência bancária.



Na pesquisa realizada, verificou-se uma maior participação dos funcionários que trabalhavam em agências com mais de 50 funcionários, correspondendo a 16 funcionários, representando 33% (trinta e três por cento) do total de participantes desta pesquisa. Do total 8

funcionários representando 17% (dezessete por cento) trabalhavam em agências com até 5 funcionários, 10 participantes representando 21% (vinte e um por cento) do total, das agências que possuíam de 6 a 10 funcionários, 7 participantes correspondendo a 15% (quinze por cento) do total de agências de 11 a 20 funcionários e 7 participantes representando 15% (quinze por cento) das agências que possuíam de 21 a 50 funcionários.

Gráfico 6 – Distribuição por dotação de funcionários.



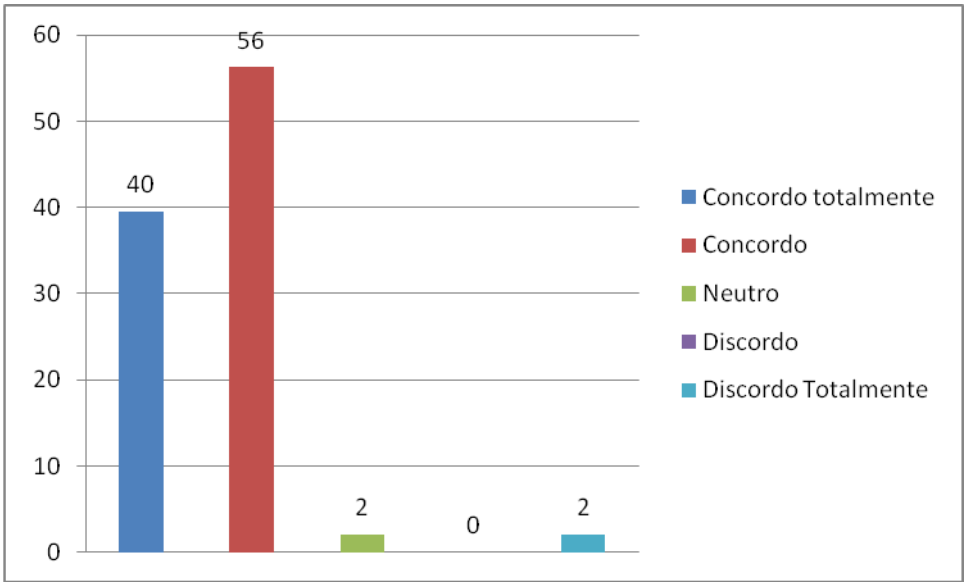
Com base nos dados obtidos, verificou-se que 56% (cinquenta e seis por cento) correspondendo a 27 funcionários pesquisados concordaram em relação à credibilidade da segurança do *internet banking* da instituição em que trabalham. Observou-se também que 19 funcionários concordaram totalmente com a afirmativa, representando 40% (quarenta por cento) do total de pesquisados. Houve também a participação de 1 funcionário, correspondendo a 2% (dois por cento) do total que optaram pela neutralidade e o mesmo percentual e participação de funcionários que discordaram totalmente.

4.2 QUESTÕES SOBRE SEGURANÇA DA INFORMAÇÃO

Com base nas respostas obtidas, verificou-se que a maioria dos funcionários pesquisados acreditam que o ambiente do *internet banking* é seguro demonstrando confiança do corpo funcional em relação ao canal. Uma vez que o funcionário confia na ferramenta de acesso fica mais a vontade para oferecê-la ao cliente, demonstrar sua praticidade,

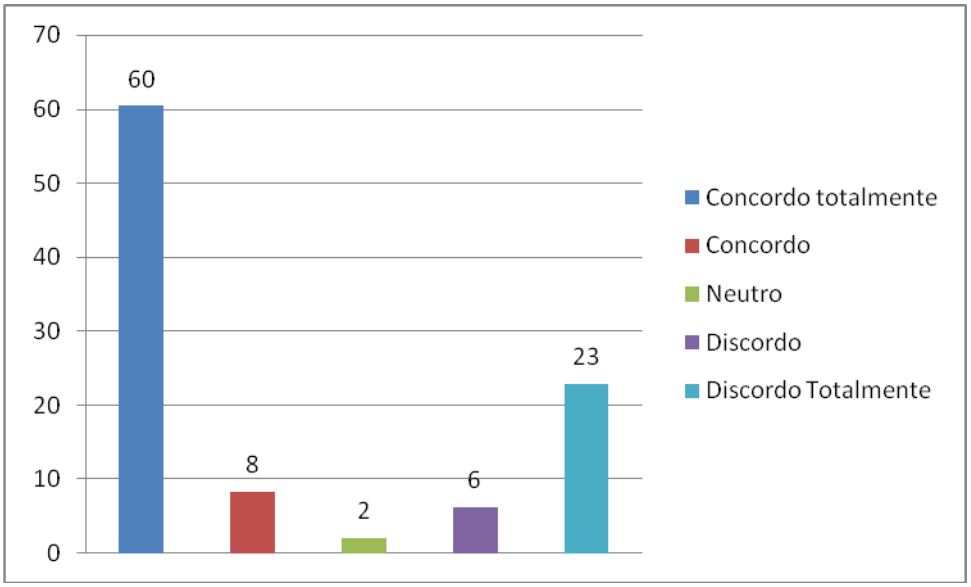
conveniência e segurança. Atesta também a percepção do funcionário de que o investimento feito pelo banco em tecnologia traduz-se em confiabilidade por parte do corpo funcional.

Gráfico 7 – Distribuição das respostas quanto à questão: Acredito na segurança do *internet banking* da instituição em que trabalho.



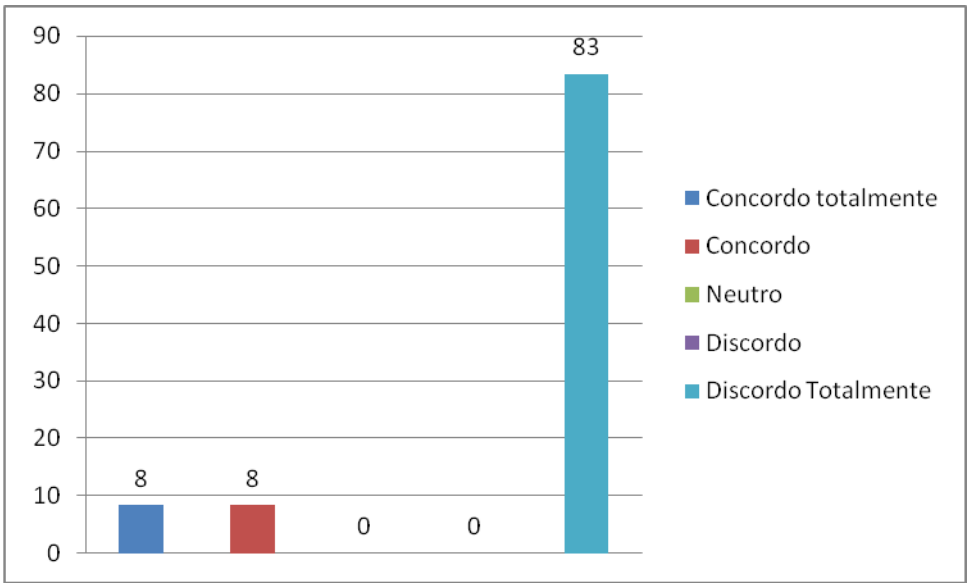
Com as respostas obtidas verificou-se que os funcionários pesquisados, em sua maioria, confiam no *internet banking* a ponto de utilizarem a ferramenta como canal alternativo para suas transações bancárias. Todo funcionário desta instituição também é um cliente da mesma, pois possui uma conta corrente, logo, ao acessar sua conta pelo *internet banking* está mostrando claramente que confia e usa o ambiente. Essa informação torna-se relevante, pois quando o próprio funcionário usa o canal fica mais fácil apresentá-lo ao cliente demonstrando que a ferramenta é segura.

Gráfico 8 - Distribuição das respostas quanto à questão: Utilizo o *internet banking* como canal alternativo para acesso às minhas transações bancárias particulares.



A maioria dos funcionários entrevistados nunca foram vítimas de crime virtual utilizando o *internet banking*. Isso demonstra que o funcionalismo utiliza de maneira segura o canal. Isso deve-se ao fato de que o funcionário detém conhecimentos sobre as regras básicas de segurança ao utilizar o canal, resta expor essas regras de maneira formal ao cliente no momento da abordagem e oferecimento do canal alternativo.

Gráfico 9 - Distribuição das respostas quanto à questão: Já fui vítima de algum tipo de crime virtual através do *internet banking*.

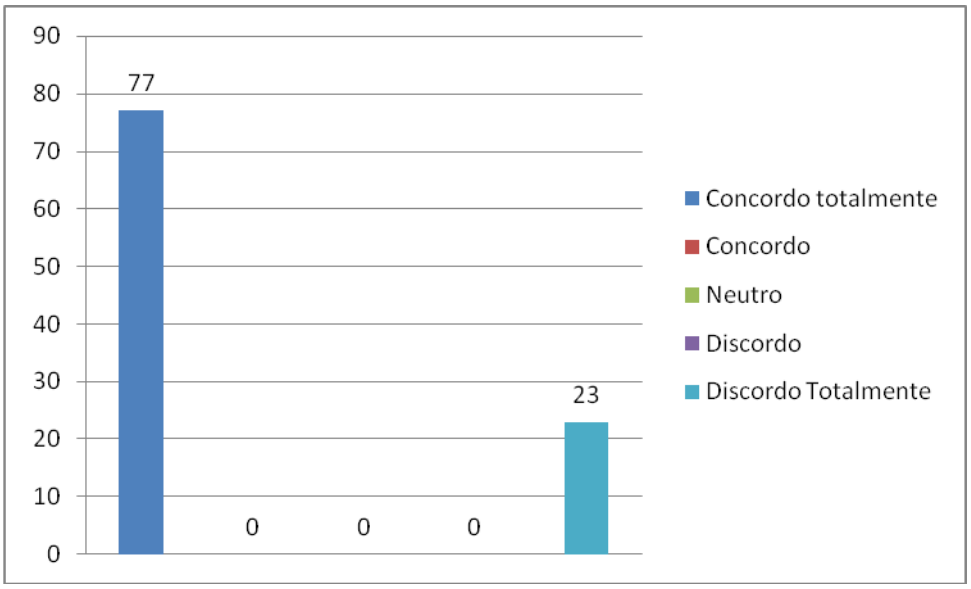


Baseado nas respostas obtidas, analisou-se que 37 funcionários representando 77% (setenta e sete por cento) concordaram totalmente com a afirmativa e 11 funcionários representando 23% (vinte e três por cento) do total de pesquisados discordaram totalmente.

Devido a pesquisa ter sido direcionada aos setores que atendem diretamente pessoas físicas das agências, a maioria dos pesquisados já conduziram processos de fraude em *internet banking*. Observou-se que da amostra um pequeno percentual não conduziu este tipo de processo demonstrando que na maioria das agências pesquisadas, verificou-se ocorrências da espécie. O resultado oferece consistência à amostra uma vez que o funcionário que já conduziu processos de fraude vivencia entre outros aspectos a fragilidade do usuário mal orientado e técnicas mais comuns de golpes.

Com base nas respostas obtidas, as informações fornecidas pela Federação Brasileira dos Bancos a respeito de crimes virtuais, condiz com a realidade vivida pelos funcionários, pois estes afirmaram que já conduziram processos fraudulentos com a utilização do *internet banking* pois, no ano de 2009, as perdas financeiras representadas pelas investidas contra caixas eletrônicos e carros fortes, ações em que é utilizada força física, somaram no total, segundo a Federação Brasileira dos Bancos (FEBRABAN, 2009), cerca de R$ 50 milhões, enquanto os crimes virtuais em geral chegaram a R$ 900 milhões.

Gráfico 10 - Distribuição das respostas quanto à questão: Já conduzi processos de fraude em *internet banking* de meus clientes.



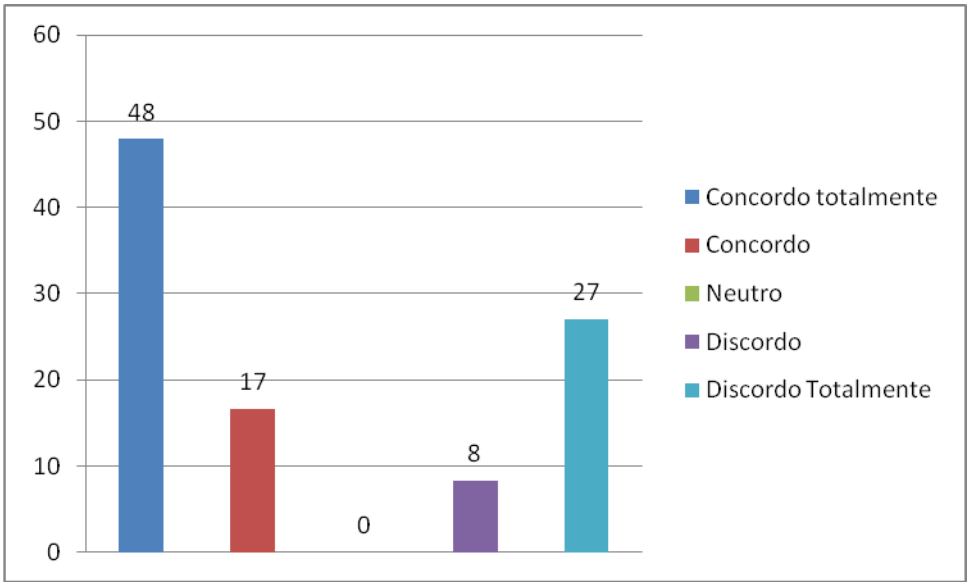
Com base na pesquisa realizada, verificou-se que 23 funcionários representando 48% (quarenta e oito por cento) do total de pesquisados concordaram totalmente com a afirmativa,

8 funcionários representando 17% (dezessete por cento) do total concordaram com a afirmativa, 13 funcionários representando 27% (vinte e sete por cento) discordaram totalmente, e 4 funcionários representando 8% (oito por cento) discordaram da afirmativa

Com a resposta dos participantes, conclui-se que a maioria do corpo funcional apresenta o ambiente virtual ao cliente, entretanto dada a não uniformidade das respostas conclui-se que praticamente metade da amostra apresenta o ambiente enquanto a outra metade ou simplesmente concorda, discorda ou discorda totalmente. Essas respostas demonstram que a cada 2 clientes que atendidos pelo menos 1 não recebe orientação sobre a ferramenta ou a recebe de maneira insuficiente.

De acordo com Sêmola (2008), é o usuário quem inicia um processo ou procedimento, e é ele que tem o poder de decisão de ignorar algo que possa colocá-lo em risco. Desta forma, se o funcionário não apresenta o canal *internet banking* aos seus clientes, coloca em risco a segurança da informação deste usuário, pois essas mesmas pessoas são um fator crítico para o sucesso do processo de proteção da informação.

Gráfico 11 - Distribuição das respostas quanto à questão: Apresento o ambiente virtual do *internet banking* aos meus clientes que nunca tiveram contato com o canal.

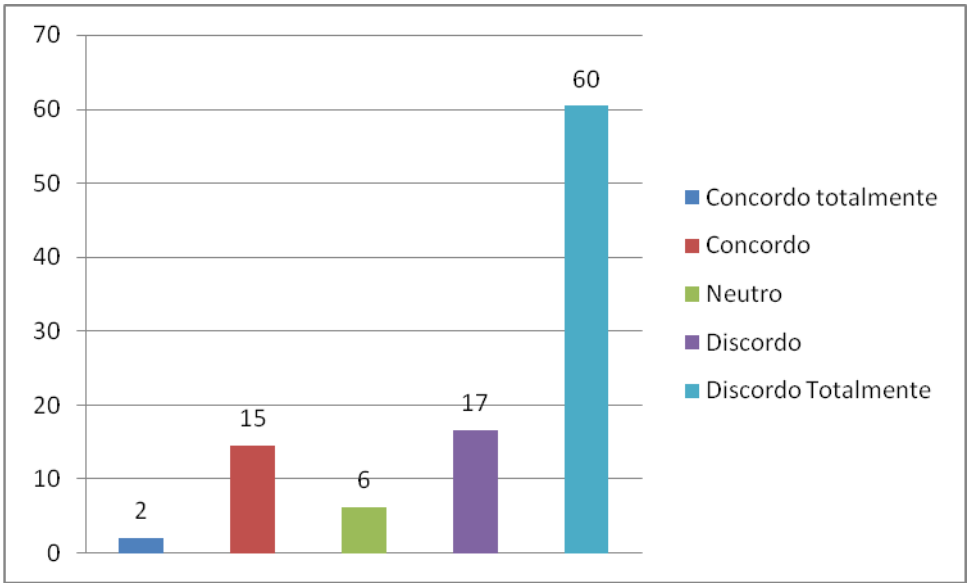


Verificou-se que 29 funcionários, representando 60% (sessenta por cento) do total de pesquisados discordaram totalmente da afirmativa. Verificou-se também que 1 funcionário, tendo representatividade de 2% (dois por cento) do total analisado concordaram totalmente, 7 funcionários representando 15% (quinze por cento) do total apenas concordaram com a afirmativa, 3 funcionários correspondendo a 6% (seis por cento) do total optaram pela

neutralidade e 8 funcionários, representando 17% (dezessete por cento) do total de pesquisados discordaram da afirmativa.

Observou-se que a maioria dos funcionários sequer sabe da existência dessa ferramenta no site do banco. Isso demonstra uma fragilidade na abordagem tendo em vista que a ferramenta é essencial para a segurança do usuário do *internet banking* uma vez que a mesma faz um diagnóstico no computador do usuário para verificação de versões adequadas de navegador, máquina virtual instalada, *firewall*, etc. O não conhecimento implica em deixar de informar sobre procedimentos de segurança. A apresentação dessa ferramenta poderia contribuir significantemente na minimização das perdas decorrentes de fraudes eletrônicas apenas com a informação repassada pelo funcionário de que existe esse aplicativo e ele deve ser executado antes da utilização do *internet banking* pela primeira vez no computador do cliente.

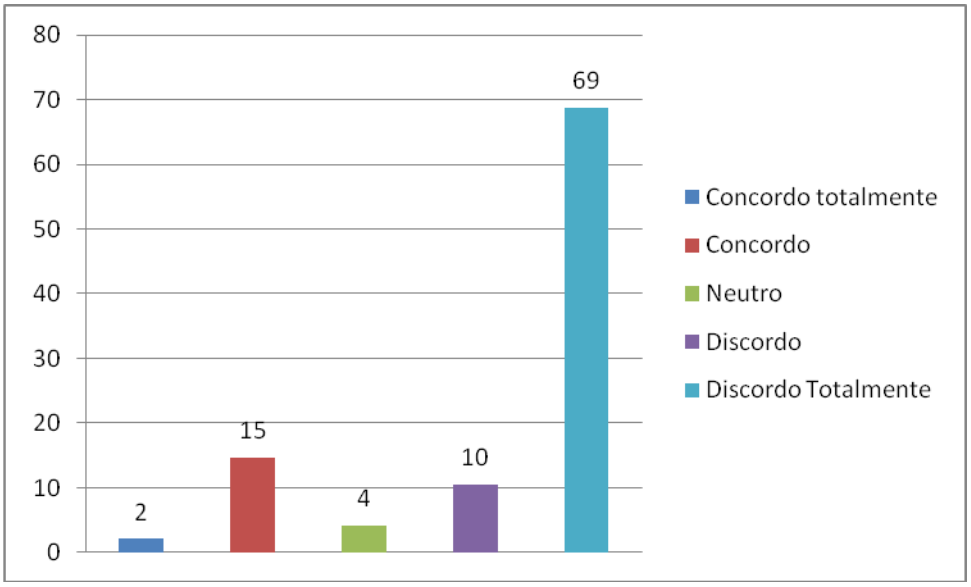
Gráfico 12 – Distribuição das respostas quanto à questão: Informo sobre as ferramentas de diagnóstico existentes no site do banco.



Baseado nos dados obtidos, verificou-se que 33 funcionários representando 69% (sessenta e nove por cento) discordaram totalmente da afirmativa. Observou-se que 7 funcionários representando 15% (quinze por cento) do total analisado concordaram com a afirmativa, 1 funcionário representando 2% (dois por cento) concordaram totalmente e 5 funcionários, representando 10% (dez por cento) do total discordaram da afirmativa. Por fim, observou-se que 2 funcionários representando 4% (quatro por cento) não expressaram opinião.

Tendo em vista o não conhecimento por parte dos funcionários da existência da própria ferramenta, sua divulgação consequentemente não tem sido feita, salvo por uma minoria da amostra. Isto demonstra que de acordo com Sêmola (2008), a tecnologia existente possibilita à organização ter uma boa proteção, mas quem vai garantir que ela tire proveito dessa tecnologia e implemente de forma efetiva os controles adequados são os usuários. Destaca-se aqui novamente o papel do funcionalismo em orientar a ação do usuário que por si só esteja alheio a essa informação.

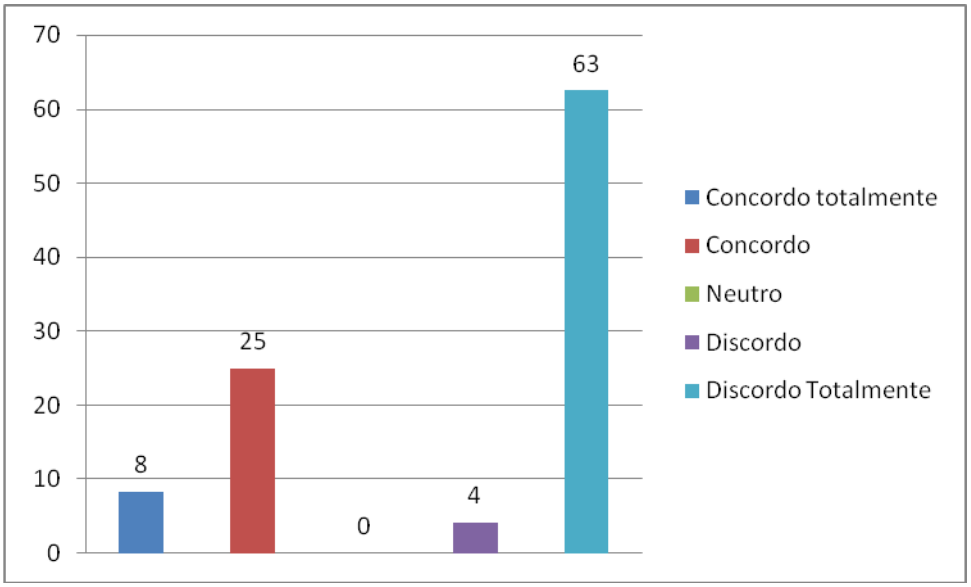
Gráfico 13 - Distribuição das respostas quanto à questão: Solicito que sejam executadas essas ferramentas ao acessar o *internet banking* pela primeira vez.



Com base nos dados obtidos, verificou-se que 63% (sessenta e três por cento) discordaram totalmente da afirmativa, correspondendo a 30 funcionários do total de pesquisados. Observou-se também que 2 funcionários equivalendo a 4% (quatro por cento) do total discordaram da afirmativa, 12 funcionários representando 25% (vinte e cinco por cento) do total de pesquisados concordaram e 4 funcionários representando 8% (oito por cento) do total concordaram totalmente com a afirmativa.

Verificou-se que apesar da maioria dos funcionários não conhecerem as técnicas mais comuns utilizadas pelos criminosos virtuais, alguns entrevistados detêm esse conhecimento. O desconhecimento dessas técnicas é um dos motivos que levam o funcionário a não dar a devida atenção à importância da orientação ao cliente.

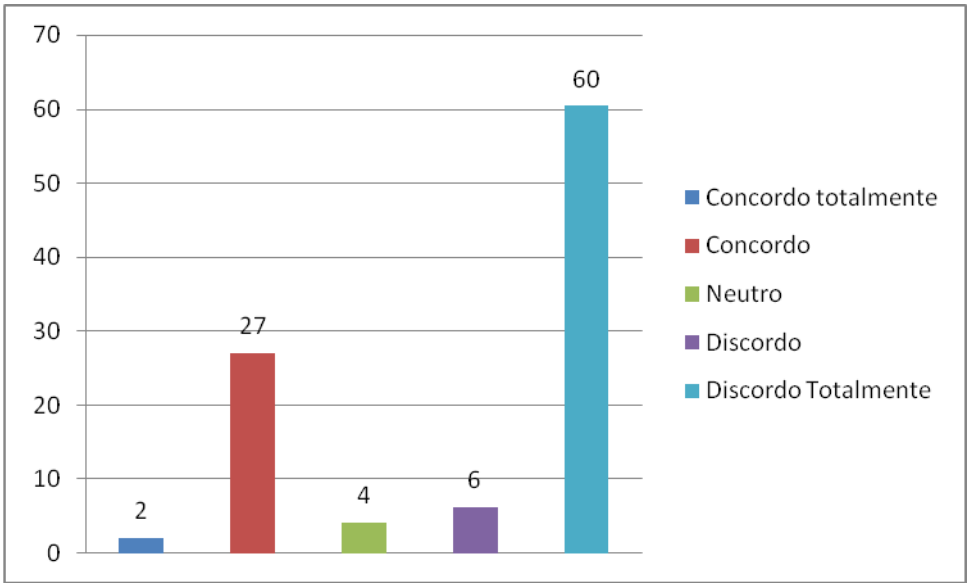
Gráfico 14 - Distribuição das respostas quanto à questão: Conheço as técnicas mais comuns de captura de dados (p. ex., *phishing scam*, clonagem de páginas, *trojans*, *keyloggers*, etc).



Observou-se que 29 funcionários representando 60% (sessenta por cento) do total analisado discordaram totalmente da afirmativa. Também verificou-se que 13 funcionários representando 25% (vinte e cinco por cento) do total concordaram com a afirmativa, 2 funcionários não expressaram opinião representando um percentual de 4% (quatro por cento) do total de pesquisados, 3 funcionários discordaram da afirmativa, representando 6% (seis por cento) do total e 1 funcionário concordou totalmente, tendo representatividade de 2% (dois por cento) do total de pesquisados.

Observou-se que a grande parte dos entrevistados não informa aos clientes sobre estes aspectos tendo em vista que a maioria das respostas foi discordo totalmente. Com base nestas respostas, verificamos mais uma vez que o fator humano é sim o elo mais fraco. Quando disponibilizamos a alguém uma alternativa, é necessário dar informações importantes e relevantes neste caso, a respeito de como utilizá-la de forma adequada. Informações simples que parecem não chamar atenção, ou que podem passar por despercebidas podem ser as principais causas das ocorrências de crimes virtuais.

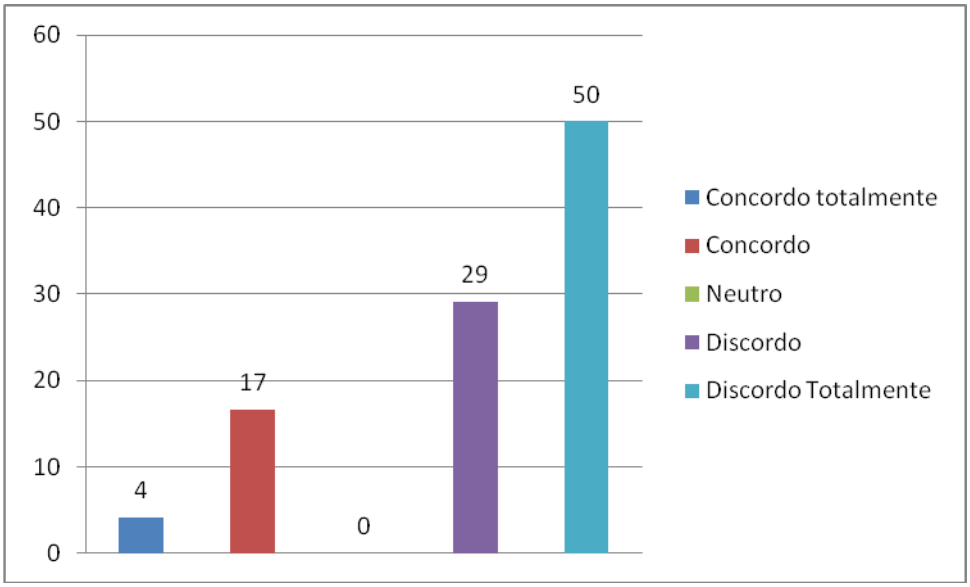
Gráfico 15 - Distribuição das respostas quanto à questão: Informo ao cliente que ele deve observar aspectos simples de segurança na internet (p.ex., *https*, cadeado no navegador).



Baseado nos dados obtidos, analisou-se que 24 funcionários representando 50% (cinquenta por cento) discordaram totalmente da afirmativa. Observou-se também que 14 funcionários, equivalentes a 29% (vinte e nove por cento) do total discordaram da afirmativa, 8 funcionários representando 17% (dezessete por cento) concordaram e 2 funcionários equivalentes a 4% (quatro por cento) do total de pesquisados concordaram totalmente com a afirmativa.

A maioria dos funcionários entrevistados não orientam que um anti-vírus é importante para o usuário, entretanto, é uma orientação simples que se o usuário não possui conhecimento poderá trazer maiores transtornos. A simples conscientização do cliente de que para utilizar seu computador para acessar dados bancários ele precisa estar protegido de ameaças virtuais, poderia minimizar perdas financeiras e evitar possíveis fraudes. Trata-se de cultura da segurança e isso deveria ser transmitido pelo funcionário do banco pois reverte em menores perdas para as partes.

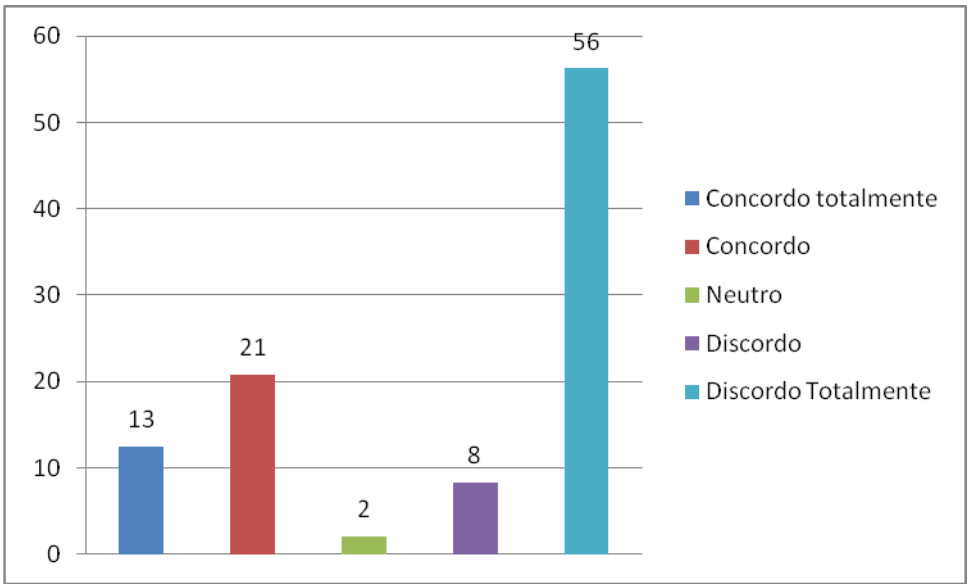
Gráfico 16 - Distribuição das respostas quanto à questão: Oriento que é necessário um bom anti-vírus instalado no computador.



Com base na pesquisa realizada, 56% (cinqüenta e seis por cento) discordaram totalmente, correspondendo este percentual a 27 funcionários do total analisado. Nas demais escalas de concordância, observou-se que 8% (oito por cento) do total de analisados equivalendo a 4 funcionários dos pesquisados discordaram da afirmativa, 1 funcionário não expressou opinião representando 2% (dois por cento) do total, 10 funcionários representando 21% (vinte e um por cento) do total concordaram com a afirmativa e 6 funcionários representando 13% (treze por cento) do total de analisados concordaram totalmente.

Baseado nas respostas, percebeu-se que a maioria dos funcionários simplesmente não orientam sobre a composição das senhas constituindo um risco para o cliente. Apesar de o sistema corporativo criticar senhas de fácil dedução, o papel do funcionário é conscientizar o cliente de que a senha é a sua maior segurança e pode mitigar aborrecimentos no uso do *internet banking*.

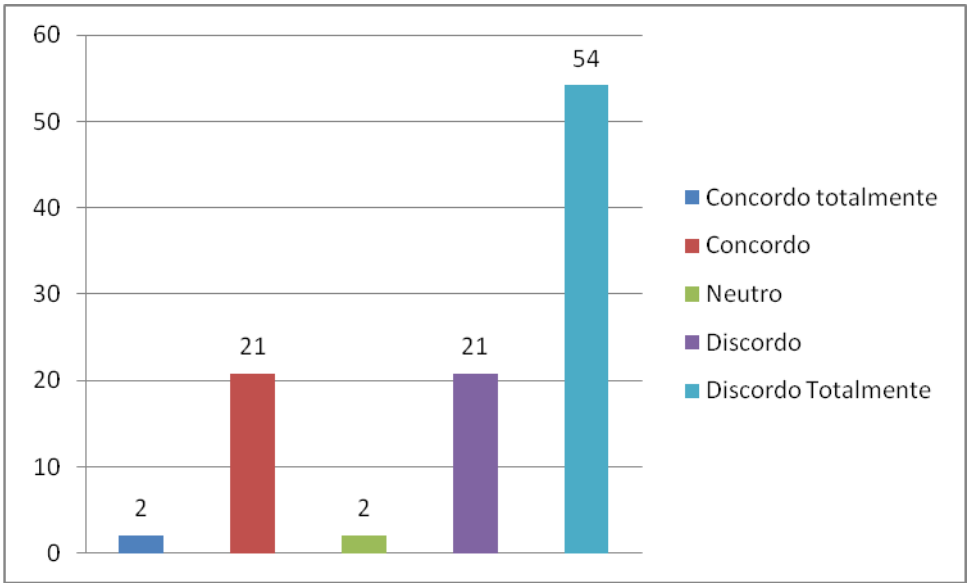
Gráfico 17 - Distribuição das respostas quanto à questão: Oriento meus clientes na construção das senhas de acesso ao *internet banking*, para que evite composições simples (p. ex., sequências, repetições, data de nascimento).



De acordo com os dados obtidos, verificou-se que do total analisado 54% (cinquenta e quatro por cento) discordaram totalmente, representando este percentual 26 funcionários que participaram da pesquisa realizada. Observou-se que 10 funcionários equivalendo a 21% (vinte e um por cento) do total analisado discordaram da afirmativa, 1 funcionário equivalendo a 2% (dois por cento) não opinou, 10 funcionários sendo equivalentes a 21% (vinte e um por cento) do total concordaram com a afirmativa e 1 funcionário correspondendo a 2% (dois por cento) do total de pesquisados concordaram totalmente com a afirmativa.

As respostas obtidas demonstram que apesar da maioria não informar da necessidade de atualizar as senhas periodicamente, existe o fato de que como a maioria dos entrevistados já conduziram processos de fraudes, e nestas ocorrências é obrigatório a alteração de todas as senhas dos clientes, surgiram tendências de respostas como concordo ou discordo, ou seja, em algum momento o funcionário teve a obrigação de informar da necessidade de alteração. Mesmo que essa alteração ou atualização tenha sido exigida devido à fraude já ter ocorrido.

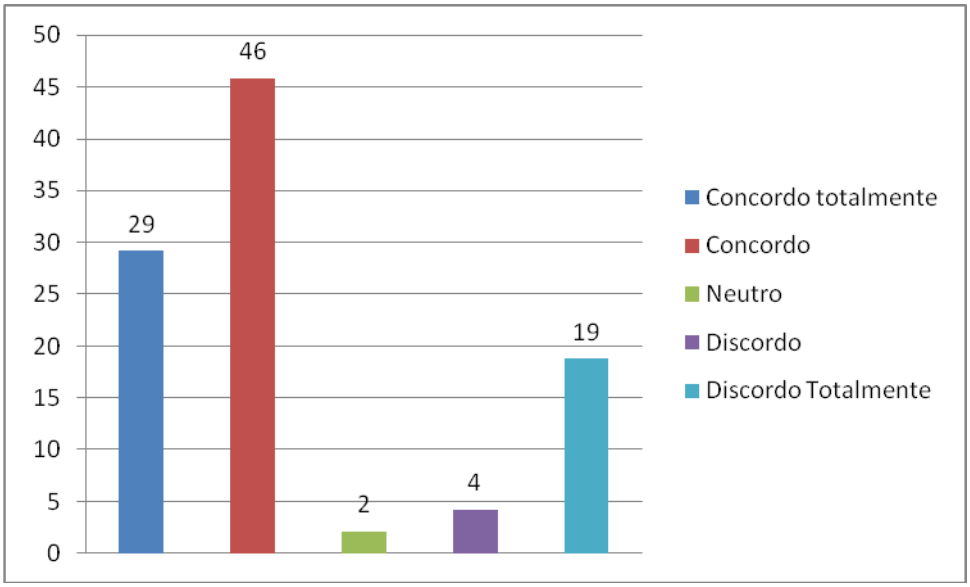
Gráfico 18 - Distribuição das respostas quanto à questão: Informo ao cliente que é necessário atualizar essas senhas periodicamente.



Na análise dos dados obtidos verificou-se que dos pesquisados, 22 funcionários representando 46% (quarenta e seis por cento) do total concordaram com a afirmativa. Observou-se também que 29% (vinte e nove por cento) do quadro analisado correspondendo a 14 funcionários concordaram totalmente com a afirmativa, 1 funcionário não expressou opinião representando 2% (dois por cento), 2 funcionários equivalendo a 4% (quatro por cento) do total discordaram da afirmativa e 9 funcionários representando 19% (dezenove por cento) do total analisado discordaram totalmente da afirmativa.

Baseado nas respostas obtidas percebeu-se que trata-se de quase um consenso entre os funcionários de que o usuário é negligente na utilização do *internet banking*. Isso deu-se devido ao fato de que geralmente em condução dos processos verificou-se que o usuário foi o maior responsável pelo seu próprio ônus. Seja por negligência ou desconhecimento, o cliente acabou facilitando a ação do criminoso virtual. Ainda que neste presente estudo tenha sido demonstrado que o funcionário pode contribuir com a formação de conhecimento pelo cliente.

Gráfico 19 - Distribuição das respostas quanto à questão: Acredito que o usuário é negligente com questões básicas de segurança no uso do *internet banking*.



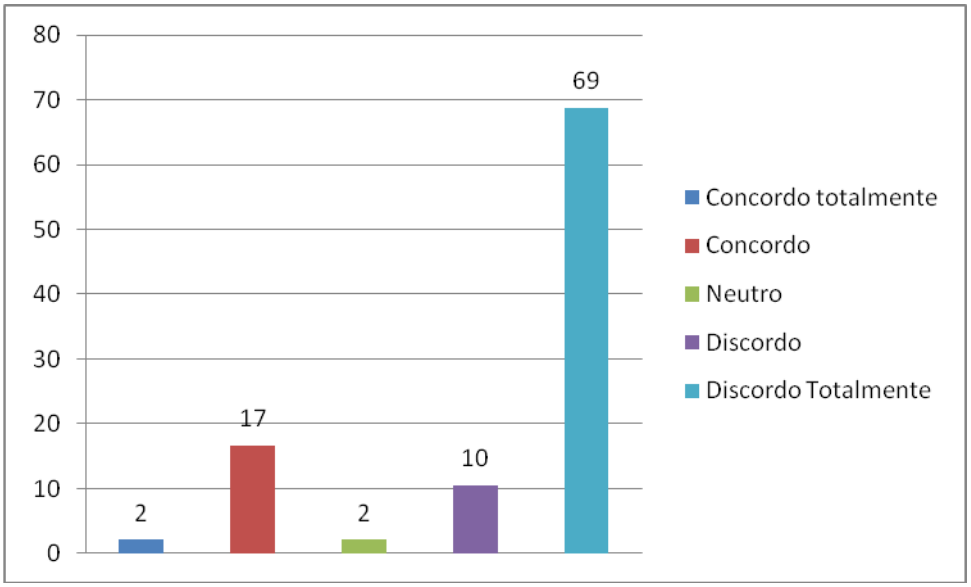
De acordo com os dados obtidos na pesquisa, observou-se que 33 funcionários representando 69% (sessenta e nove por cento) do total de pesquisados discordaram totalmente da afirmativa. Dos pesquisados também observou-se que 5 funcionários representando 10% (dez por cento) do total discordaram da afirmativa, 1 funcionário com representatividade de 2% (dois por cento) não opinou, 8 funcionários com um percentual de 17% (dezessete por cento) concordaram com a afirmativa e 1 funcionário equivalendo a 2% (dois por cento) do total de pesquisados concordou totalmente com a afirmativa.

De acordo com as repostas, os funcionários acreditam que o treinamento com relação a segurança da informação é insuficiente. Esse pode ser um dos motivos que faz com que o funcionalismo não oriente de maneira adequada o cliente, pois não foi treinado para isso. Uma vez carente de treinamento o funcionário não se sente seguro para prestar as informações necessárias. A resposta a esta questão ratifica e explica algumas outras, ou seja, o funcionário pouco treinado não sabe da existência de ferramentas de apoio, não orienta sobre construção de senhas, não conhece as técnicas mais comuns. Enfim, treinamento seria um dos pontos que deveriam melhorar na percepção dos respondentes.

De acordo Fontes (2008), é papel da organização zelar por seu recurso humano através de programas de conscientização e treinamento, pois o mesmo é fator crítico para o sucesso na proteção da informação. As organizações, destaca-se aqui as instituições financeiras, devem prover outros meios e funcionalidades, entre elas dispor de colaboradores também

comprometidos com a segurança da informação que auxiliem o usuário a compreender melhor os riscos e sua responsabilidade no processo.

Gráfico 20 - Distribuição das respostas quanto à questão: Recebo treinamento com relação às práticas de combate aos crimes eletrônicos e segurança da informação.



Com base na pesquisa realizada, observou-se que 20 funcionários representando 42% (quarenta e dois por cento) do total de pesquisados concordaram com a afirmação, 17 funcionários representando 35% (trinta e cinco por cento) do total analisado concordaram com a afirmativa, 1 funcionário não expressou opinião equivalendo a 2% (dois por cento) do total, 2 funcionários representando 4% (dois por cento) do total discordaram e 8 funcionários do total analisado, representando 17% (dezessete por cento) do total de pesquisados discordaram totalmente da afirmativa.

Percebe-se que o funcionalismo não encontra amparo nos normativos internos para orientação ao cliente. Trata-se de uma carência no sentido da instituição formalizar as instruções direcionadas ao funcionário prestando informações importantes referente à segurança ao cliente.

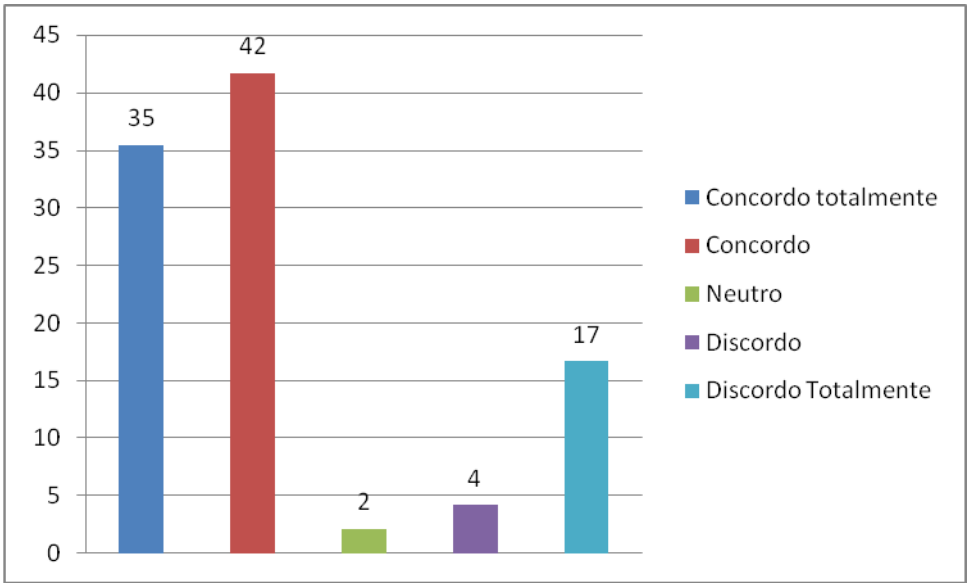
A normatização formal seria uma das ações imediatas que deveriam ser implementadas e contribuiriam de imediato para a correta instrução dos funcionários. Se as dicas de segurança fossem compiladas e disponibilizadas como uma base de conhecimento o funcionário teria conteúdo atestado e revisado pela instituição, evitando-se então orientações erradas ou fora de padrão.

Percebeu-se na instituição uma tendência de alocar funcionários com menor nível hierárquico e menos tempo de banco no atendimento direto ao cliente que usa o *internet banking*. Somado a falta de treinamento e instruções deficitárias temos um cenário propício a não propagação das melhores práticas com relação à segurança da informação e uso do *internet banking*. A solução poderia ser um curso que tornaria o funcionário um especialista em divulgar essas melhores práticas, dotado de material de apoio, normas bem definidas que abordassem exatamente os aspectos mais importantes no uso seguro do computador como canal alternativo para transações bancárias.

A resposta ainda demonstra que a instituição não tem focado em seus normativos um dos pontos mais importantes da segurança da informação que é o fator humano, pois de acordo com Beal, (2005) a grande maioria dos incidentes tem a intervenção humana, seja de forma acidental ou não, a segurança está ligada a pessoas e processos, antes mesmo da tecnologia empregada, consequentemente, todos os recursos investidos em tecnologia da informação serão em vão se o fator humano for deixado em segundo plano. É sabido que os bancos possuem excelentes ferramentas de segurança, todavia os crimes virtuais continuam ocorrendo, logo algum aspecto pode ser melhorado.

Assim a sugestão de melhoria seria o desenvolvimento de cursos instrucionais sobre o tema e melhorias nos normativos internos sobre o tema.

Gráfico 21 - Distribuição das respostas quanto à questão: Considero as instruções normativas do banco insuficientes com relação à orientação ao cliente.



5 CONSIDERAÇÕES FINAIS

Com base na pesquisa efetuada junto aos funcionários percebeu-se que os mesmos confiam na segurança da informação no uso do *internet banking*, todavia não instruem adequadamente os clientes sobre a segura utilização do mesmo. A contribuição do bancário na segurança da informação do cliente usuário do *internet banking* tem sido limitada pelo desconhecimento dos mesmos com relação aos aspectos básicos de segurança. Se por um lado o usuário ou cliente é negligente no uso e observação dos aspectos de segurança, o funcionário não tem dado a devida atenção ao assunto no momento da orientação ou apresentação do canal ao cliente.

Entretanto, a principal conclusão a que se chega é que a instituição ainda não percebeu que o fator humano é preponderante para mitigar as perdas decorrentes de fraudes eletrônicas. Não há treinamentos específicos sobre o papel do funcionário na orientação dos clientes com vistas a reduzir perdas com essas fraudes, e ainda os normativos são insuficientes e não abordam o assunto.

Com o transcorrer deste trabalho verificou-se que não é o funcionário o principal responsável, seja por omissão ou qualquer outro fator, ou o usuário por negligência ou desconhecimento das perdas que ambos os lados tem tido com o crescimento dos crimes virtuais. A própria instituição financeira está falhando no sentido do treinamento direcionado ao funcionário para que ele repasse ao cliente.

Os resultados obtidos demonstraram que o funcionário não possui a cultura da orientação de segurança, entretanto não se pode cobrar do colaborador a execução espontânea e sem padrão dessa orientação. É papel da instituição treinar os funcionários de maneira adequada para essa abordagem seguindo padrões normatizados e de eficácia já auferida. Caso contrário, a falta de padrão na abordagem e orientação poderia ainda trazer outros prejuízos de ordem financeira e imagem à instituição. Concentrar investimentos em segurança apenas em ferramentas tecnológicas não resolve o problema conforme demonstrado na pesquisa.

Portanto, o papel do funcionalismo é preponderante sim para reduzir o passivo com as perdas decorrentes de fraudes eletrônicas, pois é o funcionário que está em contato direto com o cliente. Todavia, a instituição deve zelar pela otimização do atendimento ao cliente, principal interessado na segurança de sua movimentação bancária, buscando aperfeiçoamento de seu corpo funcional e revisão constante de seus normativos.

A principal limitação desta pesquisa foi o fato da participação parcial dos funcionários previamente selecionados e uma maior disposição dos lotados em agências de praças maiores em responder os questionários. Assim a amostra foi relativamente pequena em relação ao quadro geral de funcionários desta instituição.

A sugestão para futuras pesquisas seria um estudo sobre os resultados positivos de ações de melhoria no atendimento e orientação dos usuários do *internet banking*. Com a comparação entre os resultados referentes a perdas para a instituição antes e depois da implantação de um treinamento efetivo ou criação de uma norma regulamentando o assunto.

REFERÊNCIAS

ALBERTIN, A. L. **Comércio Eletrônico**: Modelo, Aspectos e Contribuições de sua Aplicação. 5. ed. São Paulo: Atlas, 2004.

AMARO, Ana; PÓVOA, Andreia; MACEDO, Lúcia. **A arte de fazer questionários**. 2004. Disponível em: http://www.slideshare.net/nadiacachado/a-arte-de-fazer-questionarios. Acesso em 02 de jul/2011.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BRASIL, Tribunal de Contas da União. **Boas práticas em segurança da informação / Tribunal de Contas da União**. 2. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** São Paulo: SENAC, 1999.

CERNEV, A; LEITE, J. C. Segurança na Internet: a percepção dos usuários como fator de restrição ao comércio eletrônico no Brasil. **Anais. Brasília: ENANPAD**, 2005.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2000.

CUNHA, Roberto. 2007. **Treinando macacos, educando pessoas**. Projeto de Redes. [Online] 2007. [Citado em: 18 de junho de 2008.] <http://www.projetoderedes.com. br/apostilas /apostilas_seguranca.php>. Acesso em: 01 de Set/2011.

DINIZ, Eduardo H.; PORTO, Roseli M.; SANTOS, Heloísa M. Relacionamento virtual via internet banking: uma análise de respostas de e-mail. **RAC-Eletrônica**, v. 1, n. 1, art. 6, Jan./Abr. 2007. Disponível em http://www.anpad.org.br/rac-e. Acesso em 14 de set/2011.

FEBRABAN. **Os 20 mandamentos do acesso seguro às transações eletrônicas**. São Paulo 2011. Disponível em: http://www.febraban.org.br/p5a_52gt34++5cv8_4466+ff145 afbb52ffrtg33fe36455li5411pp+e/sitefebraban/Os%2020%20mandamentos.pdf>.Acesso em: 01 de Set/2011.

FONTES, E. L. G **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008.

GAMA, Remy. **Crimes da informática**. Brasília:Copy Market. 2000.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 3ª ed. São Paulo: Atlas, 1996.

ISO 17799. ABNT NBR ISO/IEC 17799:2005. **Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas**. Rio de Janeiro: ABNT, 2005.

MITNICK, Kevin D. **A Arte de Enganar**. São Paulo: Pearson Education do Brasil, 2003.

MOREIRA, Nilton Stringasci. **Segurança mínima: uma visão corporativa da segurança de informações**. Rio de Janeiro : Axcel Books, 2001.

PAESANI, Liliana Minardi, **Direito e internet - Liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.

PINHEIRO, Reginaldo César. **Os crimes virtuais na esfera jurídica brasileira**. São Paulo: IBCCrim, 2001 .

REZENDE, Denis Alcides; ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais.** São Paulo: Atlas, 2000.

ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. **Caderno Jurídico: ESMP**, São Paulo, ano 2, jul. 2002.

SCHNEIER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

SÊMOLA, M. As principais ameaças à segurança em 2008. **IDG NOW! Tecnologia em primeiro lugar**: São Paulo, 2008. Disponível em: <http://idgnow.uol.com.br/seguranca/firewall/idgcoluna. 2007-12-20.0767720515/paginador/pagina_2>. Acesso em: 15 de Jul/2011.

SÊMOLA, M. **Gestão da Segurança da Informação** – uma visão Executiva. Rio de Janeiro: Campus, 2003.

APÊNDICE A – INSTRUMENTO DE PESQUISA

Caro colega, o presente questionário faz parte da pesquisa para o meu trabalho de conclusão de curso no MBA em Gestão de Negócios Financeiros, que está sendo realizado na Escola de Administração da Universidade Federal do Rio Grande do Sul. Sua finalidade é avaliar a abordagem dos funcionários desta instituição financeira em relação à segurança da informação dos clientes que utilizam o *internet banking.* Os dados serão tratados com sigilo e o nome dos respondentes não será divulgado em hipótese alguma. A estimativa de tempo para resposta é de 5 minutos. Após o preenchimento completo deste questionário ele deve ser devolvido para o email: **lrferrari@hotmail.com.**

Agradeço sua colaboração de todos.
Luís Rafael Ferrari (44) 9933 3716 (44) 3226 1275

Parte I: caracterização do respondente

1) Sexo: ( ) Masculino ( ) Feminino

2) Faixa etária: ( ) até 25 anos ( ) de 26 a 35 anos ( ) de 36 a 45 anos ( ) de 46 a 50 anos ( ) acima de 50 anos

3) Escolaridade: ( ) Ensino médio ( ) Ensino superior ( ) Pós-graduação

4) Há quantos anos você trabalha no Banco? ( ) até 6 ( ) de 7 até 12 ( ) de 13 até 18 ( ) de 19 até 24 ( ) acima de 24

5) Cargo que ocupa: ( ) Escriturário ( ) Assistente de Negócios ( ) Gerente de Contas

6) Quantos funcionários possui a agência em que você trabalha?
( ) até 5 ( ) de 6 a 10 ( ) de 11 a 20 ( ) de 21 a 50 ( ) acima de 50

Parte II: relação do respondente com a segurança da informação

Responda os itens de acordo com a tabela de concordância a seguir:

5 Concordo totalmente	4 Concordo	3 Neutro	2 Discordo	1 Discordo totalmente

	5	**4**	**3**	**2**	**1**
1) Acredito na segurança do *internet banking* da instituição em que trabalho.					
2) Utilizo o *internet banking* como canal alternativo para acesso às minhas transações bancárias particulares.					
3) Já fui vítima de algum tipo de crime virtual através do *internet banking.*					
4) Já conduzi processos de fraude em *internet banking* de meus clientes.					
5) Apresento o ambiente virtual do *internet banking* aos meus clientes que					

nunca tiveram contato com o canal.					
6) Informo sobre as ferramentas de diagnóstico existentes no site do banco.					
7) Solicito que sejam executadas essas ferramentas ao acessar o *internet banking* pela primeira vez.					
8) Conheço as técnicas mais comuns de captura de dados (p. ex., *phishing scam*, clonagem de páginas, *trojans*, *keyloggers*, etc).					
9) Informo ao cliente que ele deve observar aspectos simples de segurança na internet (p. ex., *https*, cadeado no navegador).					
10) Oriento que é necessário um bom anti-vírus instalado no computador.					
11) Oriento meus clientes na construção das senhas de acesso ao *internet banking*, para que evite composições simples (p. ex., sequências, repetições, data de nascimento).					
12) Informo ao cliente que é necessário atualizar essas senhas periodicamente.					
13) Acredito que o usuário é negligente com questões básicas de segurança no uso do *internet banking.*					
14) Recebo treinamento com relação às práticas de combate aos crimes eletrônicos e segurança da informação.					
15) Considero as instruções normativas do banco insuficientes com relação à orientação ao cliente.					