CENTRO UNIVERSITÁRIO DE BRASÍLIA - UNICEUB

INSTITUTO CEUB DE PESQUISA E DESENVOLVIMENTO - ICPD

WINÍCIUS FERRAZ NERES

A IMPORTÂNCIA DO FATOR HUMANO E DA CULTURA DA SEGURANÇA DA INFORMAÇÃO NOS AMBIENTES CORPORATIVOS

Brasília, 2012

A IMPORTÂNCIA DO FATOR HUMANO E DA CULTURA DA SEGURANÇA DA INFORMAÇÃO NOS AMBIENTES CORPORATIVOS

WINÍCIUS FERRAZ NERES

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu na área de Rede de Computadores com Ênfase em Segurança.

Orientador: Professor Ms. Rafael Sarres.

Brasília, 2012

WINÍCIUS FERRAZ NERES

A IMPORTÂNCIA DO FATOR HUMANO E DA CULTURA DA SEGURANÇA DA INFORMAÇÃO NOS AMBIENTES CORPORATIVOS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação Lato Sensu na área de Rede de Computadores com Ênfase em Segurança.

Orientador: Professor Ms. Rafael Sarres.

Brasília, 27 de junho de 2012.

Banca Examinadora

Gilson Ciaralo

Rafael Sarres

Sylas Mendes

AGRADECIMENTOS

Agradeço primeiramente ao bondoso Deus por prover a saúde, o mais precioso de todos os bens. Também agradeço à Viviane, companheira doce, detentora de elevado conhecimento e que muito ajudou no desenvolvimento desse trabalho. Adicionalmente, cito meus queridos pais, supridores da minha educação e outros importantes valores que carrego. No ciclo familiar, não posso esquecer de agradecer e oferecer esse trabalho à minha irmã Wanessa, amiga e parceira de todos os momentos. Finalmente, agradeço ao meu orientador professor Rafael Sarres, mestre de elevadíssimo conhecimento, paciência e profissionalismo.

RESUMO

O presente trabalho tem por escopo analisar a importância do fator humano no âmbito da segurança da informação. Além disso, visa avaliar o nível da cultura da segurança da informação no mundo corporativo sob o olhar do usuário. Apreciando todos os aspectos envolvidos na criação e manutenção da segurança da informação, considera-se o fator humano o elo mais frágil e provavelmente o mais árduo de ser tratado. Adicionalmente, o grau da cultura da segurança da informação foi avaliado mediante pesquisa de campo quantitativa com auxílio de formulário. Com base na pesquisa de campo, citam-se a não realização de eventos e campanhas periódicas sobre segurança e a inexistente ou inadequada divulgação e implantação da Política de Segurança como pontos mais comuns em desacordo com a norma NBR 27002. Por fim, apesar de todas as dificuldades para se criar um ambiente minimamente seguro para o negócio da empresa, a pesquisa apontou que mais de 95% dos entrevistados concordam que a segurança da informação é muito importante para o negócio, apesar de alguns contratempos criados por ela.

Palavras-chave: Segurança da informação. Rede de computadores. Política de segurança.

ABSTRACT

The scope of this paper is to analyze the importance of the human factor in information security. It also seeks to assess the level of culture of information security in the corporate world from the perspective of the user. Appreciating all aspects involved in the creation and maintenance of information security, it is the human factor the weakest link and probably the hardest to be treated. Additionally, the degree of culture of information security was assessed by quantitative field research, in which was applied in a form. Based on field research, it can be mentioned the absense of events and periodic campaigns of safety and the nonexistent or inadequate dissemination and implementation of the Security Policy, in disagreement with NBR 27002. Finally, despite all the difficulties to create a local minimally safe for the company's business, the survey indicated that over 95% of respondents agree that information security is very important for business, despite some setbacks created by it.

Key words: Information security. Network of computers. Security policy.

SUMÁRIO

INTRODUÇÃO

O mundo atual, caracterizado pela globalização e competitividade, impõe que as pequenas e também as grandes organizações busquem o mais alto nível de excelência, haja vista que hoje o concorrente pode estar em qualquer lugar do mundo. Para superar o concorrente é necessário fabricar bons produtos, prestar serviços de qualidade e ainda manter um adequado relacionamento com os clientes. Nesse sentido, o uso eficiente da tecnologia como meio de evolução e desenvolvimento do negócio tornou-se fundamental para qualquer corporação (NAKAMURA; GEUS, 2007).

Nos últimos anos, as unidades de tecnologia da informação estão deixando de ser uma simples área provedora de sistemas e geradora de custos para ser um setor estratégico para o negócio da empresa. Os dados e informações constituem recursos cada vez mais críticos para o alcance da missão e dos objetivos organizacionais. Portanto, as informações críticas, como qualquer outro ativo do negócio, precisam ser protegidas contra as ameaças que podem levar à sua destruição, alteração ou exposição não autorizada (BEAL, 2003).

A globalização da economia, o aumento do intercâmbio de informações entre as organizações, a diversidade de aplicações corporativas e a crescente utilização de redes de computadores, principalmente a *Internet*, entre outros fatores, deixam o ambiente tecnológico cada vez mais complexo. Como consequência a todos esses acontecimentos, a segurança necessária a ser implantada tornou-se igualmente árdua e ampla. A figura 1 ilustra a complexidade e heterogeneidade de um ambiente de TI (Tecnologia da Informação) atual (NAKAMURA; GEUS, 2007).

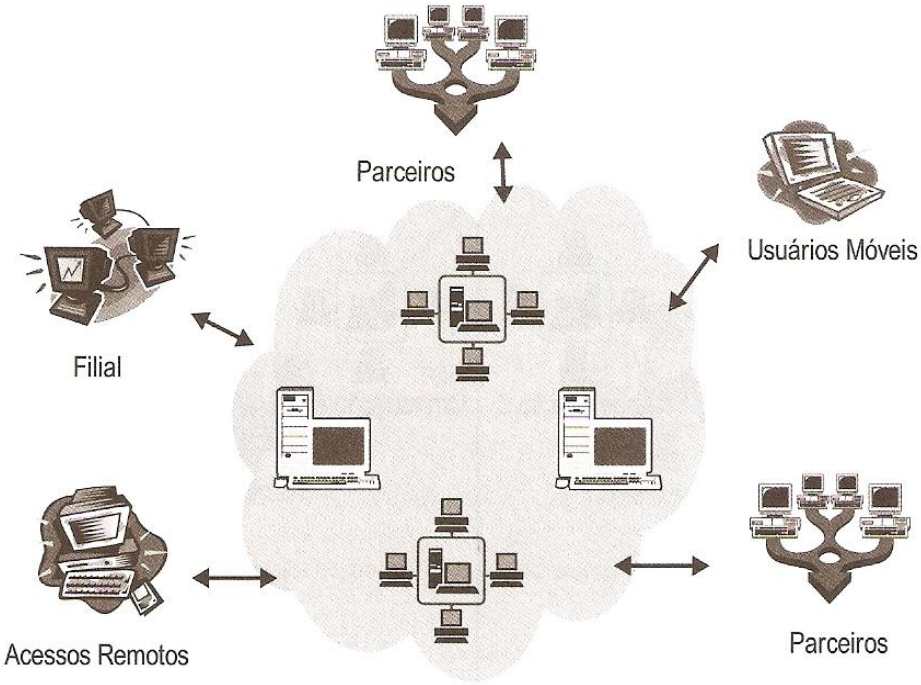

Figura 1: Diversidade de elementos num ambiente

Fonte: NAKAMURA e GEUS (2007)

Por consequência, as organizações devem entender que a segurança da informação deve existir não apenas nas relações entre organização e cliente, mas também na relação entre organização e seus fornecedores, parceiros e fornecedores e principalmente entre a organização e seus colaboradores. O ideal é que a segurança passe a ser um processo transparente, perene e natural dentro das organizações (NAKAMURA; GEUS, 2007).

Cada vez mais em voga, o tema segurança da informação gradualmente tem se tornado algo fundamental dentro das corporações. A segurança da informação é usada para referenciar a proteção de informações mantidas em componentes tecnológicos. Entretanto, também é fundamental a proteção dos ativos de informação que possuam relação direta ou indireta com os seres humanos (BEAL, 2003).

Nos últimos anos, à medida que as empresas especializadas em segurança da informação buscaram o desenvolvimento contínuo de melhores tecnologias de segurança, tornou-se mais complexa e, por conseguinte, menos comum a exploração de vulnerabilidades técnicas. Consequentemente, em crescente escala, os atacantes voltaram-se com mais força para a exploração do elemento humano (MITNICK; SIMON, 2003).

Alguns profissionais de TI ainda possuem a ideia errada de que mantêm seus ambientes plenamente seguros com produtos de segurança padrão, tais como *firewalls*, sistemas de detecção de intrusos e *antimalwares*. Reforçando a tese de que segurança não é apenas tecnologia, Bruce Schneie afirma categoricamente que a segurança não é um produto, mas sim um processo (MITNICK; SIMON, 2003).

Ao longo desse trabalho, serão expostos ao leitor argumentos que indicam que segurança da informação, ao ser tratada dentro de um ambiente institucional, deve considerar outros fatores além dos recursos tecnológicos. Nesse sentido, um dos vetores fundamentais, abordado com destaque nesse trabalho, é o tratamento dispensado aos colaboradores e funcionários.

Objetivos

Este trabalho tem como foco dissertar sobre o fator humano inserido na segurança da informação e avaliar o nível da cultura da segurança da informação, sob a ótica do usuário nos ambientes corporativos, mediante pesquisa de campo. Além disso, com base nos dados coletados, gerar conclusões que possam ser utilizadas para embasar e apoiar ações de educação dentro das empresas.

Adicionalmente, esse projeto possui os objetivos específicos:

- Dissertar sobre a segurança da informação;
- Discorrer a respeito da cultura da segurança da informação no meio corporativo;
- Dissertar sobre as vulnerabilidades e ameaças relacionadas aos usuários corporativos.

Estrutura da Monografia

A seção Introdução objetiva introduzir o tema, explanar os objetivos gerais e específicos deste projeto, proporcionando ao leitor uma visão macro do assunto abordado ao longo do trabalho. Já o primeiro capítulo visa prover ao leitor conceitos relacionados à segurança da informação de uma forma ampla que possibilite o bom entendimento do trabalho.

O capítulo dois, por sua vez, propõe-se a destacar a importância do fator humano no âmbito da segurança da informação. Além disso, visa apresentar algumas ameaças e vulnerabilidades associadas aos usuários corporativos.

Adicionalmente, o capítulo três tem como objetivo explicar a metodologia da pesquisa de campo realizada e analisar os dados coletados dos usuários sobre a cultura e conhecimento a respeito da segurança da informação sob a ótica dos próprios usuários.

Por fim, a seção Conclusão intenta apresentar conclusões e propor sugestões de melhorias aos ambientes corporativos.

1 SEGURANÇA DA INFORMAÇÃO

Esta seção visa apresentar a segurança da informação e prover conceitos relacionados que permitam o bom entendimento deste trabalho. Seguindo esta linha, de acordo com Sêmola, pode-se definir segurança da informação da seguinte maneira: “Área do conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade” (SÊMOLA, 2003).

Outra definição comumente exposta e aceita é oriunda da norma NBR ISO 27002 que a define da seguinte forma: “Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Inseridas e relacionadas ao conceito de segurança da informação há diversas outras definições fundamentais que serão explanadas no decorrer desse trabalho.

1.1 CONCEITOS IMPORTANTES

Com o foco na exposição de conceitos relacionados, pode-se considerar ativo de informação qualquer elemento que manipule ou processe informação importante para o negócio. Adicionalmente, a norma NBR ISO 27002 a define de forma mais objetiva e direta: “Ativo é qualquer coisa que tenha valor para a

organização". Como exemplos de ativo de informação, cita-se a própria informação, as bases de dados, os arquivos e obviamente as pessoas.

Ainda, expondo alguns conceitos, pode-se definir vulnerabilidade como qualquer fragilidade presente ou associada a determinado ativo, que por sua vez poderá ser explorada por uma ameaça, ou seja, um causador potencial de um incidente indesejado. Ressalta-se que para cada vulnerabilidade pode haver uma ou mais ameaças associadas (SÊMOLA, 2003).

Com intuito de exemplificar a relação entre vulnerabilidade e ameaça, tem-se o quadro a seguir com alguns exemplos.

Exemplo de vulnerabilidade no ativo	**Exemplo de ameaça associada**
Edifício sem controle de acesso.	Intruso adentrar a corporação.
Inexistência de *software* de *antimalware.*	Infecção dos ativos de TI pelos *malwares.*
Inexistência de processos para contratação de pessoal.	Contratação de pessoal não qualificado e, ou mal intencionado.
Inexistência de *firewall* em uma DMZ (*Demilitarized Zone*).	Possibilidade de acesso indevido a computadores que deveriam ter acesso restrito.
Inexistência de treinamento sobre segurança da informação para os usuários.	Usuários suscetíveis a ataques que exploram a engenharia social.

Quadro 1: Exemplos da relação entre vulnerabilidades e ameaças

Adicionalmente, outro importante conceito interligado é a definição de incidente. De acordo com Sêmola, pode-se definir incidente como: “Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade” (SÊMOLA, 2003).

Ademais, é fundamental citar o conhecido tripé da segurança da informação: confidencialidade, integridade e disponibilidade. Em outras palavras, para que exista segurança a informação deve ser tratada com sigilo, exatidão e acessibilidade.

Por confidencialidade entende-se que a informação deve ser protegida com o adequado grau de sigilo, visando à restrição de seu acesso. Em relação à integridade, fica claro que toda a informação deve ser resguardada contra alterações indevidas, intencionais ou não. Finalmente, por disponibilidade entende-se que a informação deve estar disponível nos momentos necessários ou acordados (SÊMOLA, 2003).

Na busca do fortalecimento dos pilares da segurança e da redução das vulnerabilidades e, por conseguinte, das ameaças, as organizações devem buscar a implantação de medidas de proteção. Essas medidas serão tema da próxima seção (BEAL, 2003).

1.2 MEDIDAS DE PROTEÇÃO

Numa classificação didática, as medidas de proteção podem ser preventivas, reativas ou detectivas. As preventivas contemplam os controles que

amortizam a probabilidade de uma ameaça se materializar, reduzindo, por sua vez, a probabilidade de um ataque gerar efeitos negativos para a organização. Por exemplo: Política de segurança, controle de acesso físico, programas de conscientização e treinamento de funcionários (BEAL, 2003).

Por outro lado, as medidas reativas minimizam o impacto de um ataque ou incidente já concretizado. Elas são executadas durante ou após a ocorrência do evento. Por exemplo: Sistema de detecção de intrusão (BEAL, 2003).

As medidas detectivas expõem ataques ou incidentes e disparam medidas reativas, tentando evitar ou reduzir o dano. Por exemplo: Ação legal contra um atacante, restauração de um serviço e procedimentos de resposta a incidentes (BEAL, 2003).

Outro conceito que fora citado e merece destaque no âmbito da segurança da informação corporativa é a Política de Segurança da Informação. Política de Segurança da Informação é um documento que registra os princípios e as diretrizes de segurança adotadas pela organização, a serem observados por todos os seus integrantes e colaboradores. Ela deve refletir a preocupação da cúpula; portanto, deve contar com a participação dela no processo de elaboração. Além disso, deve contemplar aspectos como organização da empresa, classificação dos ativos, segurança do ambiente físico e lógico, segurança das comunicações e aspectos humanos da segurança (BEAL, 2003).

Adicionalmente, a complexa busca pela elevação do nível de segurança invariavelmente contempla vários aspectos, tais como: aspectos do negócio, tecnológicos, jurídicos, processuais e humanos. A figura 2 ilustra os aspectos citados (NAKAMURA; GEUS, 2007)

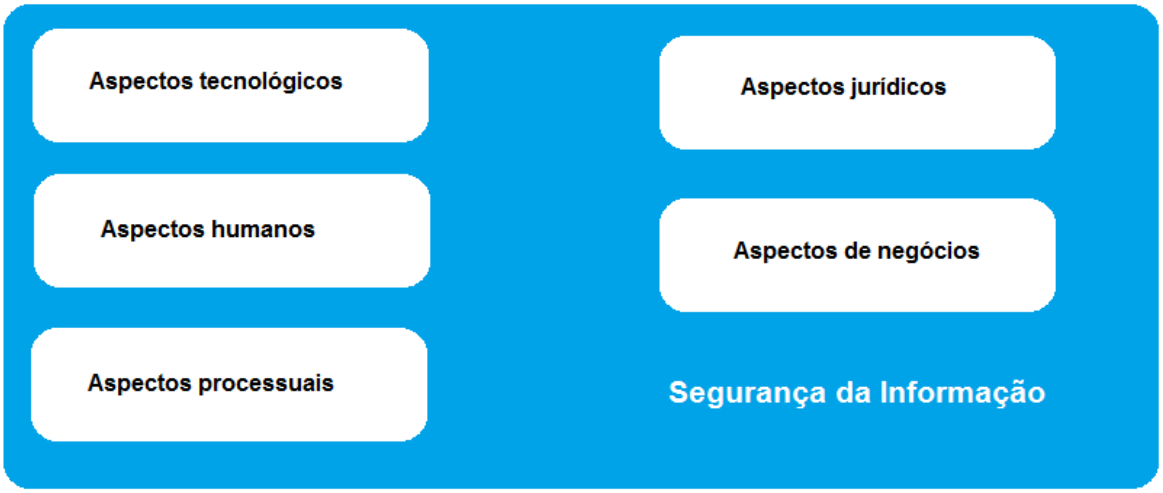

Figura 2: Aspectos envolvidos na segurança da informação

Fonte: NAKAMURA e GEUS (2007)

Com foco nos aspectos humanos inseridos na segurança da informação, dar-se-á início ao próximo capitulo.

2 O FATOR HUMANO

Pode-se afirmar que, considerando todos os aspectos envolvidos na criação e manutenção da segurança da informação num determinado ambiente, o fator humano é o elo mais frágil e provavelmente o mais complexo de ser tratado. Isso pode ser entendido facilmente quando se imagina que qualquer esquema de segurança pode ser derrubado, por exemplo, se o administrador da rede simplesmente divulgar sua senha para outra pessoa que decida utilizar dos privilégios (BEAL, 2003).

Apesar da maior atenção concedida pela mídia aos ataques externos causados pelos *hackers*, os números mostram que a maioria dos incidentes de segurança são provocados por membros internos da organização, sejam eles acidentais ou intencionais. Ao encontro das afirmações citadas é comum notícias de funcionários envolvidos em incidentes de segurança. A seguir, alguns casos que ganharam notoriedade e exemplificam as afirmações supracitadas (BEAL, 2003):

- Em 2006, funcionários do Departamento Americano de Assuntos dos Veteranos de Guerra roubaram informações pessoais de 26,5 milhões de clientes. Os dados incluíam nome, número do seguro social e datas de aniversário dos veteranos de guerra (a.IDG NOW, 2006).
- Em 2011, o ex-funcionário da Microsoft, Robert D. Curry, começou a cumprir pena de 33 meses por desviar dinheiro da gigante de *software* para uma empresa de fachada criada em seu nome. Ele admitiu o desfalque de 459 mil dólares, aparentemente como parte de uma campanha de vingança pelo tratamento que teria recebido enquanto lá trabalhou (b.IDG NOW, 2011).

- Também em 2011, a Microsoft acusou um ex-funcionário de roubar informação privilegiada e levá-la para a concorrência. A empresa acusou formalmente Matt Miszewski, um ex-gerente da companhia, de ter roubado nada mais que 600 MB de informações confidenciais. Miszewski deixou o cargo na Microsoft no dia 31 de dezembro para assumir a função de vice-presidente sênior da Salesforce, uma concorrente da Microsoft em alguns segmentos (Neowin.net, 2011).
- Em outubro de 1998, um atacante conseguiu obter alguns dados confidenciais do provedor America Online mediante engenharia social e, após isso, solicitou mudanças no registro de domínio de DNS (*Domain Name System*), de forma que todo o tráfego para a AOL fosse direcionado para outro servidor (NAKAMURA; GEUS, 2007).
- Outro caso que chamou atenção da mídia envolvendo engenharia social aconteceu em 2010, envolvendo o político e dirigente do Partido dos Trabalhadores, José Dirceu. Um atacante invadiu a caixa de *e-mail* dele, mantida pelo provedor UOL, após solicitar a mudança de senha mediante a informação de dados pessoais do usuário que o atacante havia conseguido (f.IDG NOW, 2011).

Além dos casos concretos de fraude, roubo e espionagem divulgados na mídia envolvendo o fator humano, pesquisas fortalecem a ideia de grande fragilidade deste ponto dentro da segurança da informação. Por exemplo, segundo pesquisa realizada pela Imperva, empresa especializada em segurança da informação e divulgada pelo *site* IDG NOW em 24 de novembro de 2010, revela que 72% dos funcionários admitem ter copiado informações sem autorização em *pendrives*,

notebooks ou celulares. A mesma pesquisa também afirma que 26% dos funcionários já obtiveram informações sobre os clientes de suas empresas sem o devido consentimento.

Em outra pesquisa, agora realizada pela Avira, empresa de segurança digital, e divulgada pelo *site* IT Web, afirma que apenas 38,95% dos funcionários levam a sério as normas de segurança de TI das empresas onde trabalham, enquanto apenas 35,42% conhecem as políticas de segurança e ainda não acham que seja importante. Em diferente pesquisa, agora realizada pela consultoria Kroll e noticiada no *site* Computer World, no ano de 2011, 60% dos casos de fraudes foram cometidos por funcionários da própria empresa, contra 55% na pesquisa anterior, realizada em 2010. Além dos casos e pesquisas noticiadas na mídia, convém citar alguns tipos de ataques que exploram a fragilidade do fator humano.

2.1 AMEAÇAS LIGADAS AO FATOR HUMANO

Esta seção cita algumas das diversas ameaças diretamente relacionadas à exploração do fator humano. A primeira ameaça mencionada é o *phishing*.

2.1.1 *Phishings*

Atualmente uma comum ameaça de segurança aos ambientes corporativos que procura explorar vulnerabilidades relacionadas aos usuários desatentos ou leigos é o *phishing*. De acordo com Cert.br, pode-se defini-lo como

uma fraude que acontece mediante o envio de mensagem eletrônica não solicitada, que se passa por algo lícito e que procura induzir o acesso a páginas fraudulentas, com intuito de furtar informações.

Um caso que ganhou notoriedade na mídia aconteceu no laboratório Oak Ridge. A invasão teve origem num *e-mail* de *phishing* enviado para aproximadamente 600 funcionários. Essa mensagem estava disfarçada e parecia ser um comunicado sobre mudanças de benefícios escritos pelo departamento de recursos humanos. Após alguns empregados clicarem no *link* anexado ao *e-mail,* o *malware* foi instalado em suas máquinas (d.IDG NOW, 2011).

Além disso, os *phishings* estão cada vez mais elaborados e personalizados, tornando-se muito similares às mensagens de fontes confiáveis. Adicionalmente, as informações de *sites* de redes sociais também estão sendo utilizadas para tornarem os ataques mais realistas e com aspecto pessoal (d.IDG NOW, 2011).

2.1.2 Engenharia Social

Outro tipo de ataque ainda muito efetivo e que envolve diretamente o empregado ou prestador de serviço de determinada empresa é conhecido como engenharia social. Pode-se definir este ataque como: “Técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar as pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização” (NAKAMURA; GEUS, 2007).

Um exemplo típico e comum de engenharia social, mas ainda muito eficiente, acontece quando um atacante envia um *e-mail* para alguns usuários apresentando-se como administrador da rede e solicita que ele informe sua senha de acesso à rede para a realização de uma atividade de manutenção do sistema (BEAL, 2003).

Levantamento realizado pela empresa Check Point com 850 profissionais de segurança, revela que 48% foram das empresas ondem eles trabalham foram vítimas de engenharia social nos anos 2010 e 2011. Além disso, 86% deles reconhecem a engenharia social como uma grande preocupação. O relatório da pesquisa também concluiu que os novos funcionários estão mais propensos a caírem em golpes de engenharia social e em seguida aparecem os terceirizados. Contudo, aproximadamente um terço das organizações pesquisadas não possui programa de prevenção à engenharia social ou qualquer outro plano de treinamento para os funcionários (e.IDG NOW, 2011).

2.1.3 Espionagem Empresarial

Adicionalmente aos exemplos de ataques que envolvem o fator humano, cita-se a espionagem industrial. Pode-se defini-la como um conjunto de ações ilegais ou desautorizadas para a obtenção indevida de informação. Esse tipo de ocorrência se tornou uma ameaça crescente às empresas, haja vista à busca frenética por alguma vantagem. As atividades da concorrência, a situação do mercado, as novas tecnologias dos produtos, as regras de negócio e planos de futuras fusões e

aquisições podem ser obtidas de forma ilegal por meio de funcionários mal intencionados (GOMIDE, 2005).

As coletas de informação por espionagens costumam ocorrer por meio de contatos verbais, verificações documentais ou digitais. Obviamente funcionários possuem maior facilidade na execução desse tipo de delito. Considerando que atualmente as informações constituem-se o bem mais precioso da maioria das empresas, tais furtos podem causar prejuízos irreparáveis (GOMIDE, 2005).

A título de ilustração de casos reais de espionagem, em janeiro de 2011, a montadora francesa Renault suspendeu três diretores suspeitos de vazar informações importantes sobre o projeto mais recente da empresa de um modelo de carro elétrico. Já em 1993, o executivo José Ignacio López, ex-diretor da General Motors na Europa, foi acusado de roubar informações e planos sigilosos e levá-los para a Volks (Revista Exame, 2011).

2.2 DIFICULDADES PARA ENFRENTAR O PROBLEMA

Após a explanação de algumas ameaças ligadas ao fator humano, torna-se fundamental discorrer sobre alguns pontos que dificultam o tratamento das vulnerabilidades associadas ao homem.

2.2.1 Pouco Apoio da Alta Administração

Primeiramente, para a implantação com sucesso de qualquer sistema ou modelo de gestão de segurança da informação, é fundamental e indispensável o comprometimento e apoio da alta direção da organização, principalmente quando as medidas de proteção envolvem recursos humanos. Em sentido oposto não são raros os casos em que os diretores e até o mesmo presidente da corporação não apoiam e até recriminam as ações voltadas para a segurança (BASTOS; CAUBIT, 2009).

A busca pela elevação do nível de segurança no contexto dos recursos humanos considera, por exemplo, medidas de proteção dentro dos processos de recrutamento, seleção, treinamento e demissão de pessoal. Adicionalmente, segundo a norma ISO 27002, convém que a política de segurança da informação contemple as punições para aqueles que infringirem as normas (BASTOS; CAUBIT, 2009).

Pelo exposto, fica evidente que uma política de segurança da informação é algo interdepartamental, ou seja, envolve vários setores durante sua formulação e posteriormente na execução. Além disso, ela engloba o sensível fator humano. Mediante os argumentos, fica claro que o apoio da alta direção na implantação de medidas de segurança da informação é basilar (BASTOS; CAUBIT, 2009).

A busca do apoio da alta direção na implantação de uma política de segurança ou um sistema de gestão de segurança pode ser uma tarefa árdua, entretanto necessária. Não existe um roteiro aplicável a todos os casos, mas alguns pontos devem ser considerados ao se buscar tal patrocínio.

Em primeiro lugar, uma política de segurança deve ser coerente com a organização. Por exemplo, uma empresa que atua no mercado financeiro possui um padrão de comportamento e conjunto de informações tratadas diferente de uma

empresa de comunicação. Além disso, uma política não deve ser um documento técnico, afinal a direção e usuários a princípio não possuem conhecimento para entendê-la. Ademais, uma política deve ser simples, pois deve ser claramente entendida por todos (FONTES, 2000).

Além disso, ao expor para a cúpula da empresa uma proposta de sistema de gestão de segurança da informação ou simplesmente de uma política, é necessário haver clareza quanto ao escopo. Isso minimiza o risco de frustração quanto ao trabalho a ser desenvolvido. Outro fator importante é expor os requisitos legais e marcos regulatórios aos quais a empresa está sujeita e, finalmente, apresentar uma análise de risco expondo as vulnerabilidades e riscos atuais (BASTOS; CAUBIT, 2009).

2.2.2 TI em Lado Oposto ao do Usuário

A segurança da informação contempla todos os setores de uma organização, entretanto a área de TI é uma das principais manuseadoras do ativo informação e, em sentido oposto, é comum haver situações em que a área de TI não está ao lado usuário. Por exemplo, há casos em que o usuário, seguindo todo o processo definido, solicita acesso a determinado sistema corporativo para a área de produção e tal demanda demora 15 dias para ser atendida. Como consequência do péssimo atendimento, é factível que ele use a senha de algum colega para realizar uma urgente demanda do negócio (FONTES, 2000).

Outro exemplo clássico do mau atendimento acontece quando a área de TI, mantenedora de diversos sistemas de negócios, fornece ao colaborador vários

usuários de acessos juntamente com diversas senhas. Diversas pesquisas já provaram que o usuário possui grande dificuldade no gerenciamento de senhas (FONTES, 2000).

Ademais, como possível forma de combate ao problema, é muito importante ter uma comunicação objetiva e amigável com o usuário. Essa comunicação engloba o diálogo entre os funcionários da TI e usuário, como também entre os sistemas e usuários. Sistemas simples de serem manipulados, mensagens explicativas e senhas unificadas para os diversos sistemas corporativos reduzem as possibilidades de um usuário criar uma vulnerabilidade ou ameaça (FONTES, 2000).

2.2.3 Políticas de Segurança Não Absorvidas

No mundo atual, cada vez está mais complexo gerar algo que mobilize e envolva verdadeiramente as pessoas. É fato que em muitas organizações as políticas, normas e procedimentos de segurança da informação não são entendidos, comunicados e aplicados corretamente. Entretanto, a causa não é apenas a falha no processo de implantação, mas também está relacionada com algumas características da sociedade moderna e interconectada (LACEY, 2009).

No mundo contemporâneo, em rápida mudança e rico em informações, as pessoas possuem muitas distrações. Um trabalhador típico que utilize informação verificará seu correio eletrônico pelo menos 50 vezes por dia e também acessará uma quantidade de *sites* próxima desse número. Adicionalmente, as mensagens instantâneas e de texto nos celulares são crescentes. O resultado disso é que as pessoas precisam ser seletivas sobre o que prestar atenção e provavelmente elas

se concentrarão nas questões mais relevantes e interessantes às suas necessidades pessoais. Possivelmente as questões sobre segurança da informação da empresa onde trabalham não estarão entre elas (LACEY, 2009).

Com isso, cada vez mais as abordagens tradicionais à segurança da informação, como publicação ou impressão e entrega de um simples manual não funcionam. Para o sucesso da referida abordagem, é necessário redesenhar a forma de implantação e comunicação das políticas de segurança e principalmente evitar os modelos prontos para tentar alcançar os usuários (LACEY, 2009).

Na busca do êxito, o trabalho de conscientização interno deve estar de acordo com o público alvo. Além disso, torna-se fundamental a participação de outros setores da empresa, como por exemplo, a área de endomarketing e recursos humanos para contribuírem na construção de campanhas eficientes e atrativas (LACEY, 2009).

2.2.4 Senhas Pessoais Mal Administradas

Uma grande vulnerabilidade que tem ligação direta com fator humano está relacionada com a criação e administração das senhas pessoais por parte dos usuários. Pesquisa realizada em 1993 por Courtney, publicada pelo NIST (*National Institute of Standards and Technology*), afirma que a senha foi identificada com a segunda vulnerabilidade mais grave associada ao fator humano. Isto é reforçado quando se percebe que as senhas são a principal fonte de autenticação dos usuários para a maioria dos sistemas da informação (CARSTENS et al., 2004).

Em 2004, foi publicado artigo que, além de dissertar sobre o impacto do fator humano dentro da segurança da informação, publicou pesquisa sobre o tratamento das senhas pessoais por parte dos usuários. O trabalho teve como objetivo avaliar as práticas dos usuários na determinação e memorização das senhas (CARSTENS et al., 2004).

O resultado da pesquisa com 255 usuários indicou que os indivíduos que possuem de 8 a 11 senhas de sistemas de informação, utilizadas no trabalho ou na faculdade, estão em maior risco, pois aproximadamente 2% deles se esquecem de pelo menos uma senha ao mês. Adicionalmente, já os usuários que possuem de 1 a 3 senhas, aproximadamente 0,5% deles se esquecem de alguma senha ao mês (CARSTENS et al., 2004).

O mesmo artigo publicou o resultado de outra pesquisa com 257 pessoas indicando que 73% delas escrevem alguma senha de algum sistema em papéis e destes que escrevem a senha, 75% são mulheres e apenas 25% são homens (CARSTENS et al., 2004).

O trabalho ainda concluiu que os usuários possuem grande dificuldade em memorizar muitas senhas dos mais diversos sistemas de informação e, além disso, eles consideram que é complexo formar algumas senhas. Portanto, é frequente criarem senhas fracas e comuns, não seguirem as políticas e anotarem suas senhas em papéis (CARSTENS et al., 2004).

Ao encontro do artigo citado, uma pesquisa publicada no *site* IDG NOW afirma que o grupo *hacker* LulzSec, após análise de 62 mil logins, chegou a conclusão que a senha mais comum é “123456”, seguidas por “123456789” e “*password*” (g.IDG NOW, 2011).

Além disso, recentemente vieram à tona alguns casos de violação de certificados digitais que possivelmente foram facilitados pela utilização de senhas fracas. Em 2011, a até então gigante autoridade de certificação digital holandesa, DigiNotar, assumiu que *hackers* geraram aproximadamente 500 certificados SSL (*Secure Socket Layer*) de forma ilegal, incluindo certificados para os *sites* do Google, Agência de Inteligência Americana e Yahoo, entre outros (Wired, 2011).

Os certificados digitais são utilizados para autenticar as páginas web usando o protocolo SSL e criptografar a comunicação entre o usuário e o *site*. Uma pessoa que possua um certificado de determinada página web pode conseguir representar o *site* legítimo para roubar as credenciais de acesso do usuário (Wired, 2011).

Segundo uma auditoria realizada pela empresa de segurança Fox-TI, os ativos de TI careciam de medidas básicas de segurança, tais como senhas fortes, proteção antivírus e *patches* de atualização. A empresa divulgou os fatos somente no mês de setembro; entretanto, afirmou que o problema havia acontecido em julho. Logo, se permitiu uma extensa janela para os ataques. Afinal, caso a notícia fosse publicada imediatamente, os fabricantes dos navegadores poderiam remover o quanto antes os certificados da DigiNotar da lista de certificados confiáveis. Estima-se que o certificado do Google fora utilizado para espionar cerca de 300 mil iranianos por meio de suas contas de *e-mail* do Gmail (Wired, 2011).

Ratificando a comum vulnerabilidade da senha fraca, após a divulgação do caso na mídia, um *hacker* iraniano de 21 anos assumiu a autoria do ataque e afirmou que teve acesso como administrador ao servidor da DigiNotar com a conta “administrator” e a senha “Pr0d@dm1n” (Wired, 2011).

Na busca da redução do problema, a pesquisa realizada por Cartens sugere que as vulnerabilidades associadas às senhas podem ser reduzidas através do uso de diretrizes de senha que auxiliarão os usuários na formatação e memorização de senhas seguras. Por meio de orientação e treinamento aos usuários, eles podem ser instruídos sobre o uso de técnicas mnemônicas no desenvolvimento das senhas. Essa técnica consiste basicamente em estabelecer associações criativas entre as informações a serem memorizadas (CARSTENS et al., 2004).

2.2.5 Dificuldade na Auditoria Comportamental dos Usuários

Pode-se considerar a auditoria como uma atividade que contempla o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada corporação, com intuito de aferir sua conformidade com certos objetivos e políticas institucionais, regras, normas ou padrões (DIAS, 2000).

Com o crescimento da importância da tecnologia perante os negócios, a auditoria tornou-se fundamental não apenas na área financeira, mas principalmente sobre as operações do setor de Tecnologia da Informação. Esse raciocínio ganhou tanta força nos últimos anos que foram criadas normas específicas para auditoria da TI, por exemplo, o COBIT (*Control Objectives for Information and Related Technology*) (SOLMS; VROOM, 2004).

Nos últimos anos, o trabalho do auditor foi agilizado na medida em que ele pode utilizar várias ferramentas tecnológicas para facilitar parte do seu trabalho. Hoje, por exemplo, o auditor pode utilizar *softwares* específicos para rastrear

eventos na rede e localizar modificação de permissões em diretórios. Além disso, na busca pela segurança da informação como um todo e com base na política de segurança da empresa, o auditor também deve se concentrar na análise dos processos, procedimentos de segurança e salvaguarda das informações, pontos que não são necessariamente tecnológicos (SOLMS; VROOM, 2004).

Dentro os fatores não tecnológicos há o fator humano. Entretanto, de forma geral, boa parte das auditorias considera apenas aspectos técnicos da organização. Por exemplo, se um empregado realizar tentativas de acesso não autorizadas à determinada informação, os logs de auditoria as registrarão. Essa tentativa de acesso muito possivelmente passará despercebida até que um auditor analise os logs no caso de algum incidente posterior, caso isso aconteça, ou seja detectado. Isso demonstra que auditoria verifica no máximo as consequências do comportamento e não o comportamento em si (SOLMS; VROOM, 2004).

Devido a enorme influência que o empregado tem sobre o negócio, principalmente no que diz respeito à segurança da informação, o comportamento dele deve ser examinado. Em suma, existe a necessidade real de encontrar um método para garantir que comportamento do empregado está em conformidade com as políticas da empresa, entretanto isso vem se mostrando não ser uma tarefa fácil (SOLMS; VROOM, 2004).

Investigar o comportamento dos funcionários dentro do âmbito da segurança da informação é semelhante à condução de avaliações de desempenho, sendo esta um pouco mais fácil, haja vista que pode ser baseada em alguns resultados objetivos. Como exemplo da complexidade da análise, há alguns anos a empresa National Labs demitiu vários funcionários com base em avaliações de

desempenho, mas vários deles recorreram à justiça e ganharam o caso. Os funcionários ganharam o caso basicamente por duas razões. Em primeiro lugar, as avaliações de desempenho não foram realizadas num ambiente controlado e, em segundo lugar, muitos supervisores que realizaram a avaliação não estavam suficientemente familiarizados com os funcionários que estavam sendo avaliados por eles (SOLMS; VROOM, 2004).

Os principais problemas associados com as avaliações podem ser resumidos em duas palavras: confiabilidade e validade. Estes problemas descrevem a adequação das informações recolhidas, bem como a qualidade do processo de avaliação (SOLMS; VROOM, 2004).

Há vários fatores que podem influenciar negativamente a validade e confiabilidade da avaliação e seus resultados. Por exemplo, os fatores pessoais do empregado ou do avaliador podem afetar o resultado. Nesse sentido, o humor do avaliador ou sua antipatia por um empregado poderia impactar na avaliação. Em outra situação, uma suposta crise familiar de um empregado também poderia influenciar seu desempenho no exato dia da avaliação (SOLMS; VROOM, 2004).

Todos os fatores citados podem em algum momento distorcer uma avaliação de desempenho. Portanto, também se pode argumentar que problemas semelhantes igualmente surgem quando se tenta auditar ou avaliar o comportamento do colaborador no que diz respeito à segurança da informação (SOLMS; VROOM, 2004).

Além dos principais fatores, ou seja, confiabilidade e validade, na prática existiriam muitos obstáculos para realizar uma avaliação de comportamento, apesar de sua importância. As pessoas não se comportam como máquinas, elas são

imprevisíveis e muitas vezes inconstantes. Ademais, seria caro e haveria diversas implicações legais a serem consideradas se a empresa usar os resultados da avaliação para basear decisões sobre o emprego do funcionário (SOLMS; VROOM, 2004).

Está claro que o papel dos empregados é vital para o sucesso de qualquer companhia, principalmente quando se rememora que eles formam o elo mais fraco dentro do âmbito da segurança da informação. Nesse sentido, uma forma alternativa à auditoria comportamental dos usuários é tratar firmemente o aspecto da cultura organizacional com ênfase na segurança da informação (SOLMS; VROOM, 2004).

De acordo com Edgar Schein, cultura organizacional pode ser definida como um padrão de pressupostos básicos que dado grupo criou, descobriu ou desenvolveu, com o objetivo de aprender a lidar com problemas de adaptação interna ou externa. Além disso, a cultura organizacional contempla as ideias compartilhadas pelos funcionários a respeito de uma organização (SOLMS; VROOM, 2004).

Ao se investigar mais profundamente a cultura organizacional, Schein desenvolveu um modelo de três camadas principais, ilustrado pela figura 3, que devem ser entendidas e tratadas. O primeiro nível engloba os artefatos da organização e eles devem ser visíveis e facilmente encontrados. No contexto da segurança da informação, cita-se a segurança física, por exemplo, itens como portas e catracas. (SOLMS; VROOM, 2004).

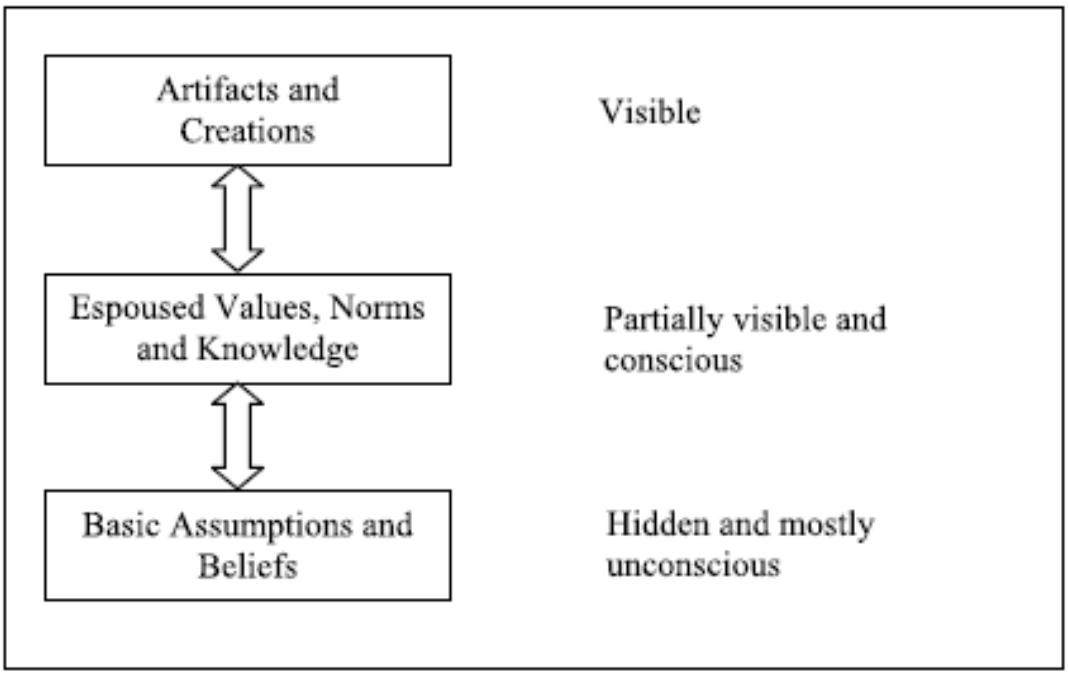

Figura 3: Modelo da cultura organizacional de Schein

Fonte: SOLMS e VROOM (2004)

O segundo nível do modelo consiste dos valores compartilhados e são parcialmente visíveis dentro da organização. Exemplos destes incluem a boa comunicação e o trabalho em equipe. O nível final e mais profundo na organização são os pressupostos tácitos. Estes não são visíveis claramente, entretanto contemplam o inconsciente dos indivíduos e englobam as crenças e valores subjacentes das pessoas (SOLMS; VROOM, 2004).

A cultura organizacional possui enorme impacto sobre a segurança da informação e isso pode ser negativo ou positivo. Assim, é fundamental que a cultura organizacional reflita uma atitude positiva sobre a segurança da informação em toda a organização. Uma vez que o lado cultural de uma organização é entendido, torna-se possível alterá-lo com intuito de criar a cultura da segurança. Ao fazer isso, o

comportamento do indivíduo irá se adaptar para incorporar a consciência da segurança (SOLMS; VROOM, 2004).

Para alcançar a citada consciência de segurança, a empresa precisa atuar nos três níveis do comportamento organizacional: Indivíduo, grupo e organização formal. Analisando o primeiro nível, sabe-se que cada pessoa é única, portanto, cada indivíduo traz várias características pessoais para a organização. Da mesma forma, a organização possui forças capazes de afetar a atitude, motivação e satisfação do empregado (SOLMS; VROOM, 2004).

O grupo, composto por indivíduos, desenvolve características além das características individuais dos membros do grupo. Assim, os grupos precisam ser analisados de forma independente e não apenas como vários indivíduos. Além disso, os valores dos grupos podem desempenhar um papel essencial na forma como os empregados se comportam em suas funções (SOLMS; VROOM, 2004).

O último nível, conhecido como organização formal, é criado de acordo com as características comuns entre os membros da organização. Ela é totalmente influenciada pelo ambiente, mas também exerce forte impacto nos colaboradores e na operação interna. Em suma, ao influenciar os grupos para se tornarem mais conscientes sobre segurança da informação, a organização como um todo se beneficiará (SOLMS; VROOM, 2004).

Com intuito de iniciar a mudança da cultura, é necessário, em primeiro lugar, identificar as áreas que necessitam de mudança. Indivíduos, grupo e organização precisam ser examinados para entender como cada parte afeta a cultura da organização (SOLMS; VROOM, 2004).

Em primeiro lugar, o comportamento organizacional é utilizado para alterar os valores compartilhados e de conhecimento do grupo. Uma vez que o comportamento do grupo começa a alterar, ele influenciará os empregados individuais da mesma forma. Como consequência terá efeito na organização formal (SOLMS; VROOM, 2004).

Por fim, a ideia de auditoria ou monitoramento comportamental do empregado é extremamente difícil, como citado anteriormente. O número de fatores que podem afetar o resultado de uma auditoria desse cunho a torna não muito favorável para influenciar ou induzir o empregado a seguir as politicas de segurança. Dessa forma, um método alternativo sugerido parte da ação sobre a cultura da organização. O entendimento sobre o comportamento e como o empregado é influenciado é extremamente útil nesse trabalho de mudar a cultura da organização com objetivo de criar um ambiente mais seguro. A figura 4 ilustra a relação entre cultura organizacional e comportamento (SOLMS; VROOM, 2004).

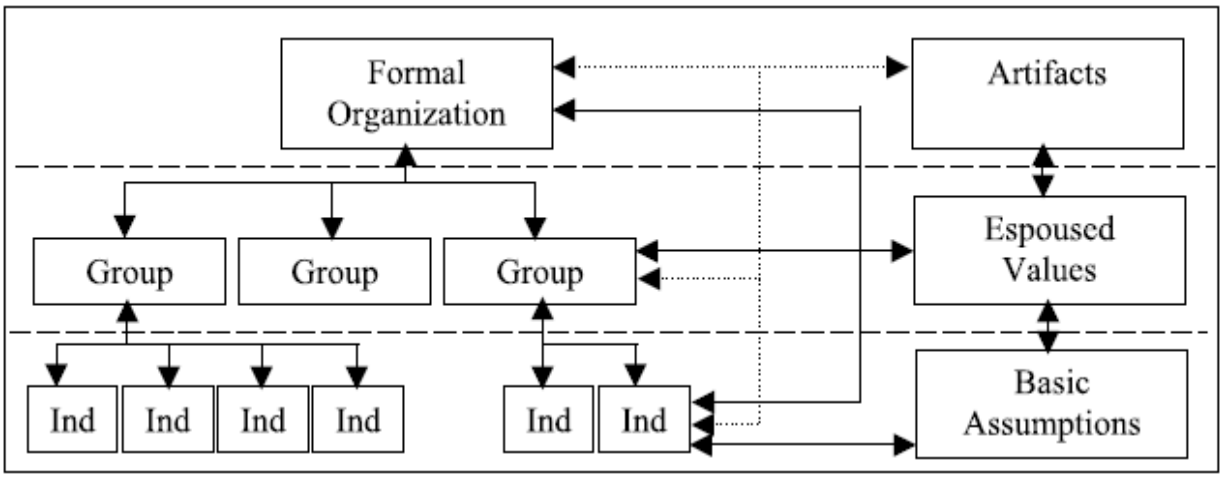

Figura 4: Interação entre cultura organizacional e comportamento

Fonte: SOLMS e VROOM (2004)

Após a exposição da importância do tratamento do fator humano, algumas ameaças relacionadas, determinadas dificuldades encontradas para o combate delas e possíveis formas de minimizar o problema; dar-se início a próxima seção.

3 PESQUISA DE CAMPO

As seções anteriores trouxeram o conceito de segurança da informação e os demais termos associados. Além disso, expôs as diversas relações e implicações do fator humano inseridas no âmbito da segurança da informação no mundo corporativo.

Por sua vez, esta seção propõe-se a expor ao leitor uma pesquisa de campo realizada com o intuito de avaliar o conhecimento dos usuários corporativos sobre itens básicos relativos à segurança da informação e de analisar como as empresas estão tratando esse tema, sob a ótica dos próprios colaboradores.

3.1 O MÉTODO

Numa pesquisa, seja ela qual for, é fundamental trabalhar com método a fim de assegurar a si e aos demais que os resultados da pesquisa são confiáveis. Segundo o matemático e filósofo René Descartes, pode-se definir método como um conjunto de regras precisas e fáceis, dos quais se terá certeza de nunca tomar um erro por uma verdade (LAVILLE; DIONNE, 1999).

A definição de Descartes é considerada válida até os dias de hoje. O método indica regras, sugere um procedimento que norteia a pesquisa e auxilia a executá-la com eficácia. Constitui-se em “regras precisas e fáceis”, como sugere Descartes, “para não desperdiçar as forças de sua mente” (LAVILLE; DIONNE, 1999).

O conhecimento no ramo da Ciência da Computação é obtido usando as seguintes grandes metodologias: pesquisa analítica, bibliográfica qualitativa e quantitativa (LAVILLE; DIONNE, 1999).

A pesquisa analítica é o método mais comum para se obter conhecimento sobre *softwares* e algoritmos. Ela faz algumas pressuposições sobre dados do programa ou sobre o *hardware* onde o *software* será executado e prova matematicamente alguma importante propriedade do programa. Por exemplo, a análise de complexidade assintótica de algoritmos é uma forma de pesquisa analítica. Além disso, a análise de algoritmos e programas onde se modela a distribuição de probabilidade dos dados são também exemplos de pesquisa analítica (WAINER, 2007).

A pesquisa bibliográfica consiste em uma coleta de artigos relevantes à pesquisa, além de contemplar também as práticas de revisão sistemática e meta análises. Em ambas, o foco é coletar artigos publicados que reportam algum experimento quantitativo pelo qual estamos interessados (WAINER, 2007).

A pesquisa qualitativa baseia-se na observação cuidadosa dos ambientes onde o sistema está sendo utilizado e do entendimento das perspectivas dos usuários. Ela se propõe a coletar particularidades e interpretações individuais, podem ser útil na busca de um novo conceito de *software* ou funcionalidade. Por fim, a pesquisa qualitativa intenta o desenvolvimento e aperfeiçoamento de novas ideias mediante análise após ampla pesquisa (WAINER, 2007).

A pesquisa de campo incluída neste trabalho utilizou como metodologia a pesquisa quantitativa exploratória, ou seja, não possui relevância estatística. Além disso, utilizou como item de apoio um questionário. Ele foi empregado para saber a

opinião de diversos profissionais ativos sobre o tema em questão. Para cada uma das perguntas foi oferecida, predominantemente, aos interrogados respostas em escala, conhecida como escala de Likert, que lhes permitiu assinalar se estavam em total desacordo, em parcial desacordo, sem opinião, de acordo parcialmente ou totalmente de acordo com o enunciado (LAVILLE; DIONNE, 1999).

3.2 OPERACIONALIZAÇÃO DA PESQUISA

Para a automatização e operacionalização da pesquisa foi utilizado o *site* www.surveymonkey.com. O formulário foi disponibilizado e publicado na *Internet* pelo endereço https://www.surveymonkey.com/s/pesquisa_winiciusf durante os dias 24/3/2012 e 30/3/2012.

A divulgação do endereço foi realizada de duas formas. Primeiramente, por meio da rede social Facebook para os 180 contatos pessoais do autor desse trabalho. Em segundo lugar, mediante a distribuição via *e-mail* para 40 contatos pessoais também do mesmo autor.

O público-alvo abrangeu profissionais que exerciam qualquer atividade profissional remunerada, sem restrição. Cada formulário possuía as afirmações e possibilidades de respostas citadas e explicadas a seguir:

1- Possuo cargo de nível gerencial na empresa onde sou colaborador.

Sim	Não

Explicação: Este item objetiva determinar se existia alguma diferença de nível de conhecimento sobre segurança da informação entre funcionários com cargo gerencial e aqueles que não detêm cargo em tal nível.

2- Eu estou ciente de que posso receber contatos maliciosos, via *e-mail* ou telefone, simulando comunicações confiáveis de minha ou outras empresas com intuito de roubar informações corporativas ou pessoais.

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Esta questão está diretamente relacionada ao item 2.1. deste trabalho, seção que tratou das principais ameaças ao fator humano. Ela se propõe a avaliar se os colaboradores institucionais possuem consciência dos comuns ataques de *phishing* e engenharia social.

3- Percebo que a direção da organização é comprometida com a segurança da informação.

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Este item relaciona-se com a seção 2.2.1 deste trabalho, tópico que dissertou sobre a necessidade do apoio da alta administração para o sucesso da implantação de qualquer sistemática. Ela intenta aferir se os colaboradores percebem que alta direção está interessada e envolvida com a segurança da informação.

4- A área de TI da empresa onde trabalho atende em tempo hábil às demandas de seus usuários.

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Esta questão está diretamente relacionada ao item 2.2.2, seção que expôs a importância da área de TI ser eficiente frente ás demandas da corporação. Ela visa medir se os colaboradores estão satisfeitos com o atendimento de suas necessidades por parte da área de TI.

5- Conheço plenamente a Política de Segurança da Informação da empresa onde presto serviço (Caso não exista a política, marque “Discordo totalmente”).

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Este questionamento está vinculado ao item 2.2.3, parte que tratou da necessidade de existência e absorção da Política de Segurança, bem com a dificuldade de se conseguir isso. Ela visa avaliar o quanto os colaboradores conhecem a Política de Segurança da Informação da empresa.

6- Tenho muita dificuldade de criar e gerenciar as senhas de acesso aos sistemas corporativos.

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Este item está relacionado ao item 2.2.4, que abordou sobre a dificuldade apresentada pelos usuários para gerenciar as próprias senhas pessoais. A questão objetiva identificar a intensidade desse problema.

7- A corporação organiza periodicamente eventos e ações sobre segurança da informação, tais como palestras, reuniões, folhetos e *e-mails* informativos.

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Este item está ligado ao item 2.2.5, tópico que tratou da auditoria comportamental dos usuários e explanou o porquê da necessidade das campanhas educacionais. O item propõe-se a aferir quanto as empresas fazem campanhas e eventos sobre segurança da informação.

8- Considero que a segurança da informação é algo muito importante para o sucesso da empresa, apesar de ela gerar alguns contratempos.

Discordo totalmente	Discordo parcialmente	Não sei opinar	Concordo parcialmente	Concordo totalmente

Explicação: Esta questão visa avaliar se os usuários consideram a segurança da informação algo importante para o negócio, apesar da segurança da informação ser inversamente proporcional à comodidade.

3.3 RESULTADOS

Após 7 dias de recebimento de formulários preenchidos, passou-se à análise dos resultados obtidos, mediante o cotejamento das respostas dos 58 participantes da pesquisa.

Em relação à primeira questão, 22 pessoas afirmaram que exercem cargo de nível gerencial e 36 alegaram não possuir cargo de tal nível. A figura 5 ilustra o resultado.

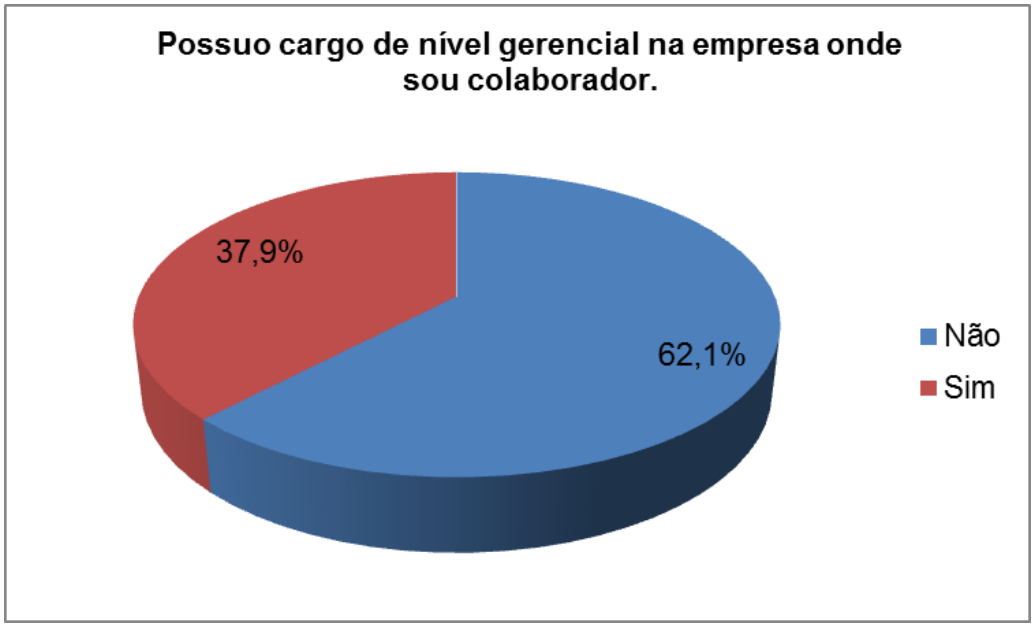

Figura 5: Sumarização das respostas da questão 1

Em relação à segunda questão, 57 das 58 pessoas responderam “Concordo totalmente” ou “Concordo parcialmente” quando indagados sobre o conhecimento da possibilidade de ataque de Engenharia Social.

De acordo com a figura 6, 98,2% dos entrevistados afirmaram concordar totalmente ou parcialmente quando perguntados se estavam cientes da

possibilidade de sofrerem ataques de Engenharia Social. O item 2.1 dissertou sobre o ataque citado que é considerado um dos mais ataques mais eficazes e citados na mídia, segundo as bibliografias pesquisadas durante esse trabalho.

Após a pesquisa bibliográfica realizada e o conhecimento de vários ataques que utilizaram a Engenharia Social, considera-se elevado o percentual de colaboradores que conheciam o ataque em questão. Todavia, com a pesquisa não foi possível avaliar os reais níveis de conhecimento e preparo dos usuários para detectar e enfrentar o citado ataque.

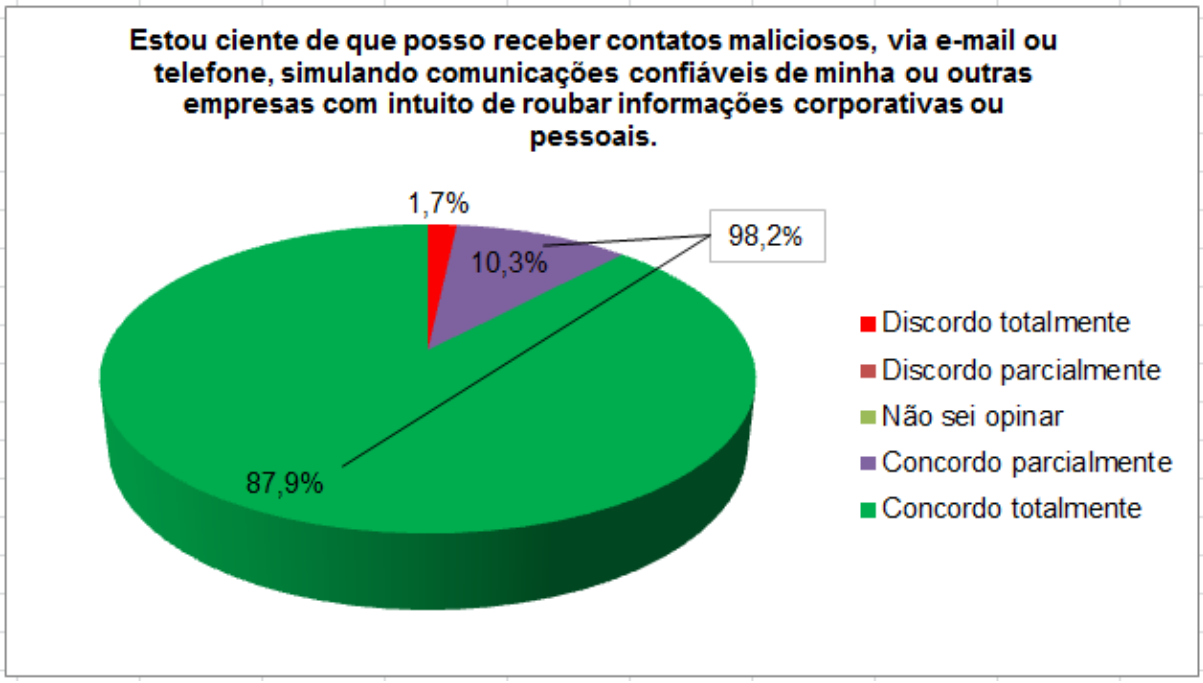

Figura 6: Sumarização das respostas da questão 2

A respeito da terceira questão, que tratava da percepção dos colaboradores sobre o envolvimento da direção em relação à segurança da informação, 39 colaboradores (67,2% dos entrevistados) reconheceram totalmente

ou parcialmente o comprometimento da direção. Em contrapartida 24,1% alegaram não detectar tal comprometimento da direção da corporação de forma total ou parcial.

A falta de apoio da alta administração, tratada no item 2.2.1, é um problema crítico, mas não incomum nos ambientes corporativos. O percentual de 24,1% dos entrevistados que assinalaram discordar totalmente ou parcialmente sobre a visualização do comprometimento da alta direção junto à segurança da informação é relativamente alto, porém esperado. A figura 7 ilustra o resultado obtido.

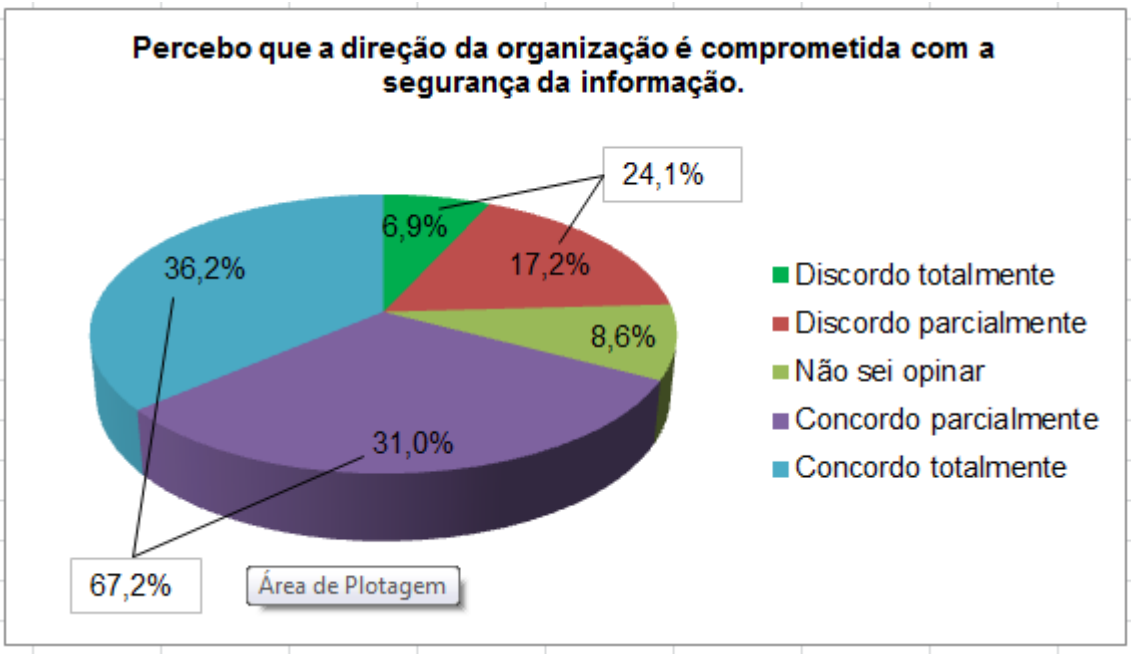

Figura 7: Sumarização das respostas da questão 3

Em relação à quarta questão, que abordava a satisfação dos colaboradores em relação aos serviços prestados pela área de tecnologia da informação, 72,4% dos entrevistados concordaram totalmente ou parcialmente que área de TI atende às demandas em tempo hábil. Porém, 24,1% dos entrevistados

negaram totalmente ou parcialmente que a área de TI atende às demandas em tempo hábil. Cita-se adicionalmente que 6,9% dos entrevistados não souberam responder a questão.

A questão 4, tratada pelo item 2.2.2 desse trabalho, explanou o porquê a TI é tão importante dentro do contexto da segurança da informação. Com base na dissertação e estudos realizados durante a execução desse projeto, considera-se alto o percentual de colaboradores satisfeitos com a área de Ti. A figura 8 explana o resultado.

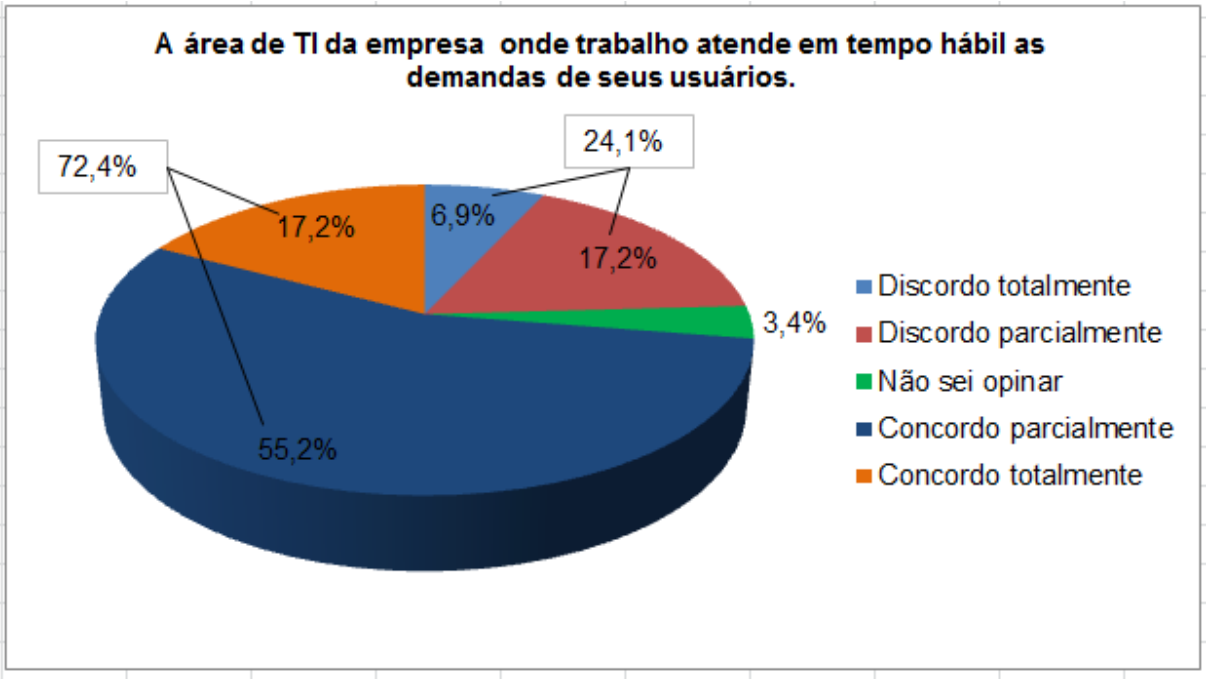

Figura 8: Sumarização das respostas da questão 4

Sobre a quinta questão, que avaliava o conhecimento da Política de Segurança da Informação por parte dos colaboradores, 55,2% afirmaram ter total ou parcial conhecimento sobre o documento. Entretanto 37,9% dos entrevistados

alegaram ter total ou parcial desconhecimento sobre ela e 6,9% dos entrevistados não souberam responder essa questão.

O percentual de colaboradores que alegaram ter total ou parcial desconhecimento sobre a Política de Segurança é significante, mas esperado. Adicionalmente, ressalta-se que esse percentual contempla o caso em que a empresa não possuía a Política. Veja-se o gráfico a seguir.

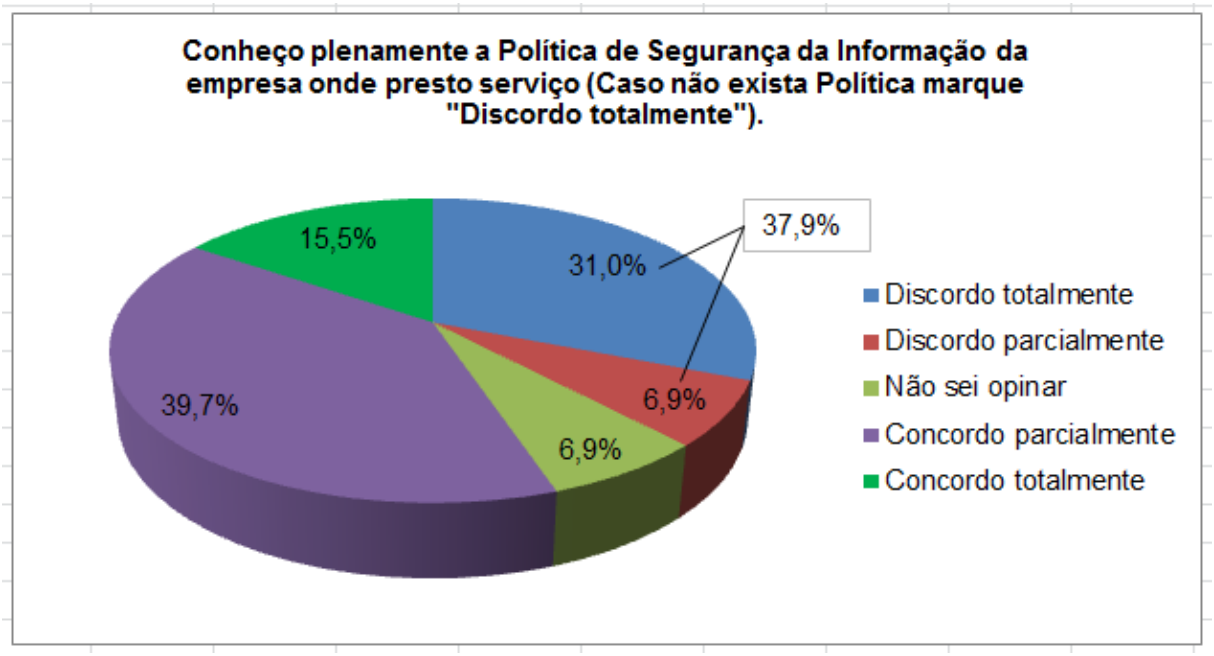

Figura 9: Sumarização das respostas da questão 5

Quanto à sexta questão, que abordava a dificuldade dos usuários em gerenciar suas respectivas senhas, 27,6% deles assinalaram possuir dificuldade ou muita dificuldade para administrar as senhas dos sistemas corporativos. Porém, 67,2% discordaram totalmente ou parcialmente mediante a afirmação “Tenho muita dificuldade de criar e gerenciar as senhas de acesso aos sistemas corporativos”. Por fim, 3 entrevistados, o que corresponde à 5,2%, não souberam opinar.

Com base na dissertação localizada no item 2.2.4 desse trabalho, o alto percentual de colaboradores com dificuldade ou multa dificuldade de administrar as senhas pessoais era esperado. A figura 10 aclara o resultado.

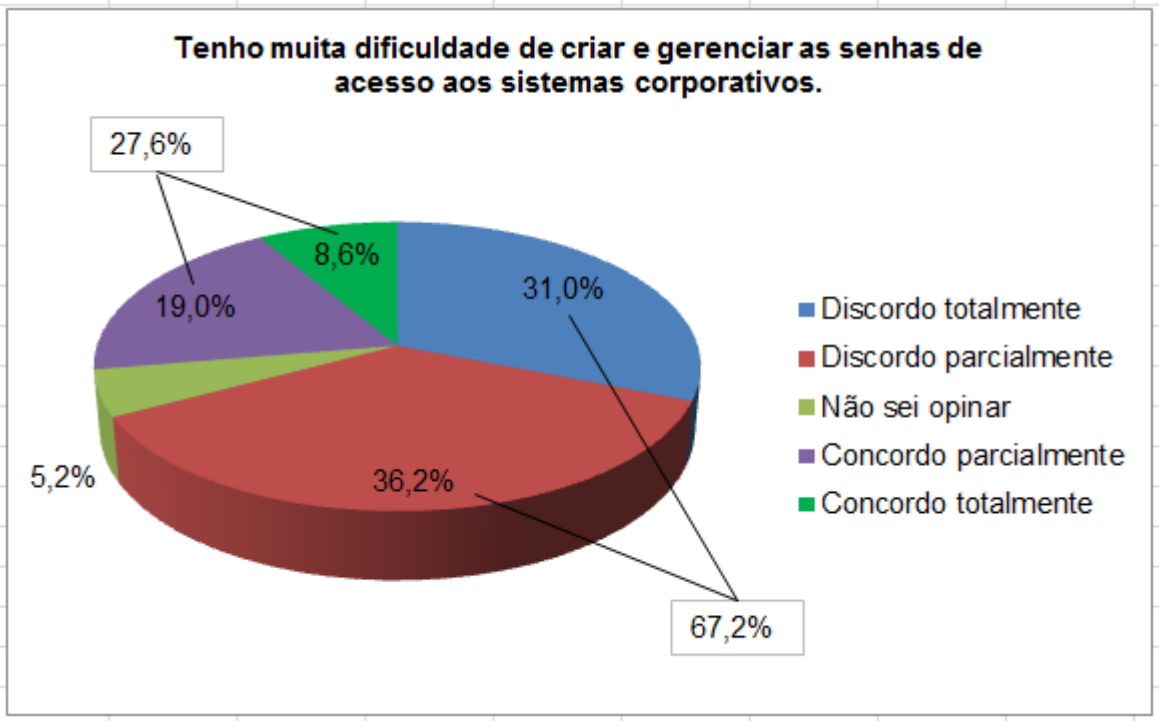

Figura 10: Sumarização das respostas da questão 6

A sétima questão questionou ao entrevistado sobre a existência de eventos e campanhas periódicos sobre a segurança da informação na empresa em que trabalha. Como resultado, 37,9% dos entrevistados concordaram totalmente ou parcialmente sobre a existência das citadas ações. Porém, 67,2% negaram totalmente ou parcialmente sobre a existência das referidas ações de endomarketing. Adicionalmente, informa-se que 5,2% dos entrevistados não souberam opinar.

A alta taxa de entrevistados, superior a dois terços, que negaram totalmente ou parcialmente sobre a existência das referidas ações de endomarketing

ilustra como as empresas de uma forma geral ainda pecam na disseminação da cultura da segurança da informação.

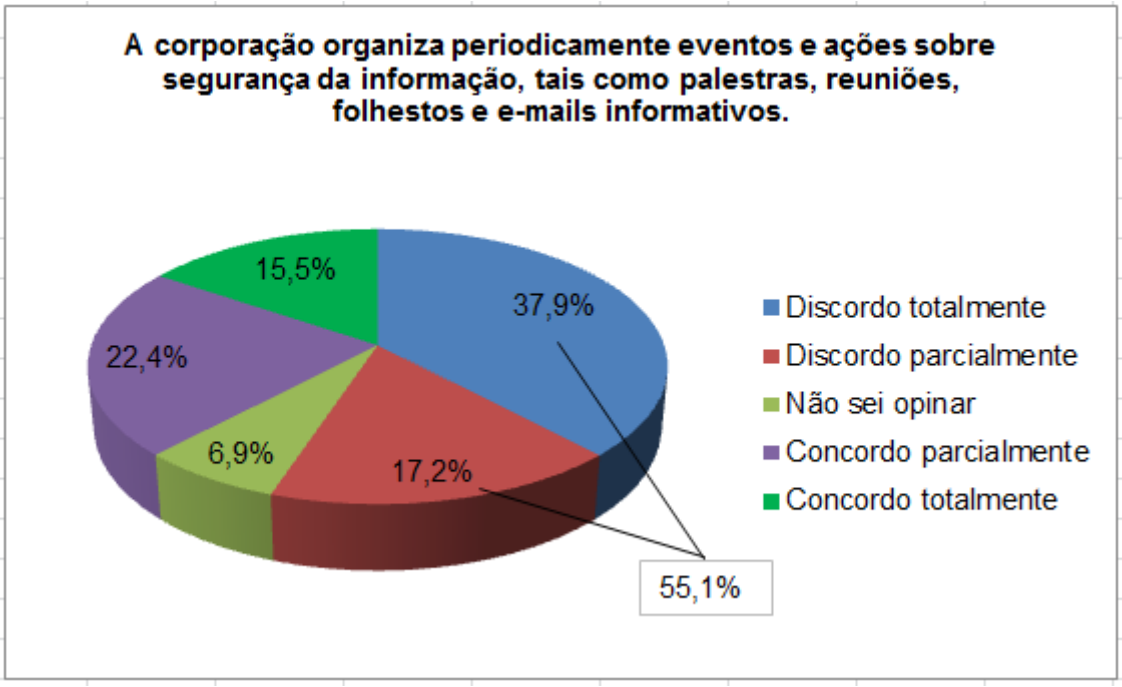

Figura 11: Sumarização das respostas da questão 7

A última questão do formulário tinha como meta avaliar o quanto os entrevistados consideravam a segurança da informação algo importante para o sucesso do negócio. Como resposta, 57 dos 58 entrevistados, assinalaram “Concordo totalmente” ou “Concordo parcialmente” quando indagados se consideravam a segurança da informação importante para o negócio, apesar de alguns contratempos gerados por ela. Por fim, 1 entrevistado, o que corresponde à 1,7% da amostra, discorda parcialmente sobre a importância da segurança da informação para o negócio.

Os resultados dessa questão mostraram que os usuários sabem o valor da segurança da informação, entretanto o percentual de praticamente 100% chega a

ser surpreendente. Essa surpresa existe, pois apesar da cultura de segurança da informação ser relativamente nova na sociedade ela já tem a sua importância. A figura 12 ilustra o resultado.

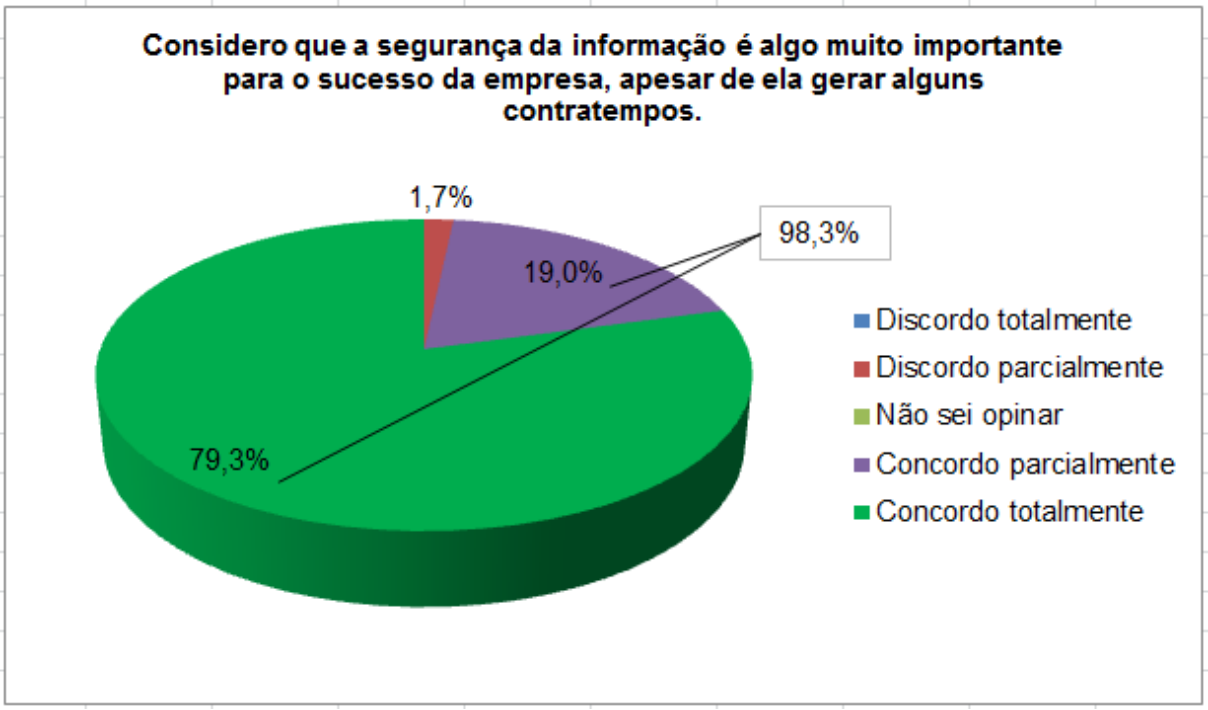

Figura 12: Sumarização das respostas da questão 8

3.3.1 Nível gerencial x Nível operacional

A primeira questão do questionário tinha como objetivo detectar se o funcionário possuía carga de nível gerencial ou operacional. Esse item possibilitou filtrar as respostas e avaliar se os colaboradores detentores de cargo gerencial têm o mesmo nível de conhecimento, entendimento e dificuldades em comparação aos colaboradores de nível operacional. Essa questão proporcionou a elaboração do quadro 2 que confronta as respostas dos entrevistados que afirmaram possuir cargo

gerencial com as respostas dos entrevistados que afirmaram não possuir cargo de tal nível.

Item	Cargo em nível gerencial					Cargo em nível operacional / técnico				
	DT	DP	NS	CP	CT	DT	DP	NS	CP	CT
2	0%	0%	0%	4,5%	95,5%	2,8%	0%	0%	13,9%	83,3%
	0%			**100%**		**2,8%**			**97,2%**	
3	9,1%	22,7%	9,1%	27,3%	31,8%	5,6%	13,9%	8,3%	33,3%	38,9%
	31,8%		**9,1%**	**59,1%**		**19,5%**		**8,3%**	**72,2%**	
4	9,1%	27,3%	4,5%	54,5%	4,5%	5,6%	11,1%	2,8%	55,6%	25%
	36,4%		**4,5%**	**59%**		**16,7%**		**2,8%**	**80,6%**	
5	31,8%	4,5%	4,5%	40,9%	18,2%	30,6%	8,3%	8,3%	38,9%	13,9%
	36,3%		**4,5%**	**59,1%**		**38,9%**		**8,3%**	**52,8%**	
6	18,2%	50%	9,1%	18,2%	4,5%	38,9%	27,8%	2,8%	19,4%	11,1%

Item	Cargo em nível gerencial					Cargo em nível operacional / técnico				
	68,2%		**9,1%**	**22,7%**		**66,7%**		**2,8%**	**30,5%**	
7	31,8%	31,8%	4,5%	27,3%	4,5%	41,7%	8,3%	8,3%	19,4%	22,2%
	63,6%		**4,5%**	**31,8%**		**50%**		**8,3%**	**41,6%**	
8	0%	4,5%	0%	22,7%	77,7%	0%	0%	0%	16,7%	83,3%
	4,5%		**0%**	**95,5%**		**0%**		**0%**	**100%**	

Quadro 2: Comparação das respostas entre os colaboradores de nível gerencial e operacional

Legenda: DT = Discordo totalmente; DP = Discordo parcialmente; NS = Não sei responder; CP = Concordo parcialmente e CT = Concordo totalmente.

A linha da tabela relativa à análise da questão 2 do questionário explana que 100% dos entrevistados pertencentes ao nível gerencial têm ciência da possibilidade do ataque de Engenharia Social. Enquanto isso, 97,2% dos entrevistados de nível operacional possui tal ciência. Pode-se afirmar que não houve diferença significa na comparação das respostas dos entrevistados de nível gerencial *versus* técnico.

A linha da tabela vinculada à apreciação da questão 3 do questionário mostra que 59,1% dos entrevistados da classe gerencial reconhecem total ou

parcialmente o comprometimento da direção em relação à segurança da informação. Adicionalmente, 72,2% dos entrevistados pertencentes ao grupo de funcionários operacionais reconhecem o comprometimento da direção em relação à segurança da informação. Há uma diferença de aproximadamente 13% entre as respostas dos dois grupos.

A linha da tabela relacionada à análise da questão 4 mostra que praticamente 60% dos entrevistados do grupo de funcionários de nível gerencial responderam que área de TI atende em tempo hábil às demandas de forma total ou quase total. Em contrapartida, 80,6% dos entrevistados pertencentes ao grupo de funcionários operacionais responderam que área de TI atende em tempo hábil às demandas de forma total ou quase total. Há uma diferença de 20,1% na comparação das respostas dos dois grupos.

Adicionalmente, a linha da tabela relativa à apreciação da questão 5 explana que mais de 59% dos entrevistados do grupo de funcionários de nível gerencial responderam que conhecem totalmente ou quase totalmente a Política de Segurança da Informação da empresa onde trabalham. Por outro lado, 52,8% dos entrevistados pertencentes ao grupo de funcionários operacionais responderam da mesma forma que os funcionários de nível gerencial.

A linha da tabela vinculada à análise da questão 6 explana que mais de 22,7% dos entrevistados pertencentes ao grupo de funcionários de nível gerencial concordaram totalmente ou quase totalmente na dificuldade de administrar suas respectivas senhas pessoais. Por outro lado, 30,5% dos entrevistados pertencentes ao grupo de funcionários operacionais responderam de forma similar.

A linha da tabela coerente à questão 7 mostra que 31,8% dos entrevistados do grupo de funcionários de nível gerencial responderam que sua empresa costuma realizar atividades de endomarketing sobre segurança da informação. Porém, 41,6% dos entrevistados pertencentes ao outro grupo de concordam totalmente ou parcialmente que suas empresas possuem atividades de endomarketing sobre segurança da informação.

Finalmente, a linha da tabela relativa à questão 8 explana que 95,5% dos entrevistados pertencentes ao grupo de funcionários de nível gerencial reconhecem totalmente ou parcialmente a importância da segurança da informação para o sucesso do negócio. Adicionalmente, 100% dos entrevistados pertencentes ao grupo de funcionários operacionais reconhecem totalmente ou parcialmente a importância da segurança da informação. Nessa questão, ficou claro que, independentemente do nível funcional do colaborador, é quase uma unanimidade o saber de importância da segurança da informação para o sucesso de qualquer negócio.

CONCLUSÃO

A segurança da informação, área do conhecimento dedicada à proteção dos ativos de informação, faz-se de extrema importância para o negócio e é sustentada pelo tripé disponibilidade, integridade e confidencialidade.

Para alcançar os níveis aceitáveis de segurança da informação para o negócio, várias medidas de proteção devem ser aplicadas. Essas medidas envolvem aspectos tecnológicos, jurídicos, processuais, corporativos e principalmente humanos.

Pode-se afirmar que, considerando todos os aspectos envolvidos na criação e manutenção da segurança da informação num determinado ambiente, o fator humano é o elo mais frágil e o mais complexo de ser tratado. Não são raros os casos de incidentes de segurança envolvendo o fator humano. Como exemplos clássicos de ataques que procuram explorar a fragilidade do fator humano destacam-se o *phishing*, a engenharia social e a espionagem industrial.

Implantar um sistema de gestão de segurança que contenha controles efetivos sobre o fator humano não é uma missão simples. De acordo com a pesquisa de campo realizada durante a produção desse trabalho, a não realização de eventos e campanhas periódicas sobre segurança é a falha mais comum no meio pesquisado. Em seguida citam-se a inexistente ou inadequada divulgação e implantação da Política de Segurança e a dificuldade dos usuários em administrar as próprias senhas.

Em sequência, a falta de percepção de comprometimento da direção em relação à segurança da informação, sob a ótica dos usuários, é outro problema

grave que acontece em razoável escala no meio pesquisado. Adicionalmente, o nível de insatisfação com a área provedora de TI, setor fundamental na gestão da informação, é alto.

Apesar da dificuldade de se criar e manter um ambiente seguro, a segurança da informação ganha cada vez mais importância para os usuários corporativos. Isso pode ser ilustrado pelas respostas à pergunta 8 do questionário: 98,3% dos entrevistados concordaram com a importância da segurança da informação para o sucesso do negócio, apesar de ela gerar alguns transtornos.

Com intuito de minimizar as vulnerabilidades e prover a implantação de um ambiente seguro, algumas ações podem ser adotadas nas corporações. Primeiramente, o trabalho de endomarketing voltado para a segurança da informação deve ser reforçado. Ações como o envio de *e-mails* informativos e realização de palestras podem ser muito úteis.

Outro ponto importante é a criação e a implantação da Política de Segurança. Ela é fundamental, pois detém as diretrizes da segurança da informação e sem elas qualquer outra ação está fadada ao fracasso. Observe-se que as empresas devem promover também ações para facilitar a administração pelos usuários de suas próprias senhas, como disponibilizar *softwares* de armazenamento de senhas pessoais e prover sistemas com senha e usuário unificados.

Ademais, recomenda-se que a alta administração das empresas se comprometa com a segurança da informação. Isso pode ser feito, por exemplo, mediante a criação e a participação de comitês de segurança. Além disso, tão importante quanto o comprometimento é a divulgação das ações definidas nos comitês para os demais funcionários. Qualquer programa de segurança da

informação terá maior probabilidade de sucesso se os colaboradores estiverem motivados por perceberem que a alta administração está engajada e empenhada para o sucesso do programa.

Adicionalmente, considerando a importância da área de TI na gestão das informações, é muito importante que ela atenda às necessidades do negócio de forma organizada, estruturada e tempestiva. É imprescindível a compreensão pelo grupo dirigente da corporação de que a área de TI não é uma simples área meio, mas sim uma área estratégica. Ela deve prestar serviço de forma eficiente e sempre que possível em *compliance* com as melhores práticas, tais como as normas NBR ISO 27001, NBR ISO27002, COBIT (*Control Objectives for Information and Related Technology*) e ITIL (*Information Technology Infrastructure Library*).

Por fim, como continuidade desse trabalho, sugere-se a produção de dissertações e pesquisas sobre a diferença do nível da cultura da segurança da informação entre ambientes corporativos de empresas públicas e empresas privadas. Adicionalmente, outra sugestão é a realização de pesquisa de campo no mesmo âmbito, mas com relevância estatística.

REFERÊNCIAS

10 Casos de Espionagem Industrial. Revista Exame. Disponível em: http://exame.abril.com.br/ negocios/gestao/noticias/10-casos-de-espionagem-industrial?p=9#link, 2011. Acesso em 8 de fev. de 2012.

BASTOS, Alberto; CAUBIT, Rosângela. *Gestão de Segurança da Informação – ISO 27001 e 27002 Uma Visão Prática*. Porto Alegre: Módulo, 2009.

BEAL, Adriana. *Segurança da Informação – Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações*. São Paulo: Atlas, 2003.

CARSTENS, Deborah Sater et al. Evaluation of the Human Impact of Password Authentication Practices on Information Security. *Informing Science Journal*, v. 7, 2004. Disponível em: http://www.inform.nu/Articles/Vol7/v7p067-085-229.pdf. Acesso em: 1 de jan. de 2012.

Cert BR. Disponível em: http://cartilha.cert.br/fraudes/sec2.html #subsec2.2. Acesso em: 8 de dez. de 2011.

Computer World. Disponível em: http://computerworld.uol.com.br/seguranca /2011/11/14/seguranca-maioria-das-fraudes-e-cometida-por-funcionarios/. Acesso em: 8 de dez. de 2011.

DIAS, Cláudia. *Segurança e Auditoria da Tecnologia da Informação*. Rio de Janeiro: Axcel Books, 2000.

FONTES, Edison. *Vivendo a Segurança da Informação – Orientações Práticas para Pessoas e Organizações*. São Paulo: Sicurezza, 2000.

GOMIDE, Tito L. Ferreira. *Segurança Documental nas Empresas*. São Paulo: LTR, 2005.

IDG NOW:

a. Disponível em: http://idgnow.uol.com.br/seguranca/2006 /05/23/idgnoticia.2006-05-3.9981651856/IDGNoticia_view/. Acesso em: 6 de dez. de 2011.

b. Disponível em: http://idgnow.uol.com.br/mercado/2011/09/27/ex-funcionario-da-microsoft-e-preso-por-desfalque-de-meio-milhao-de-dolares/. Acesso em: 6 de dez. de 2011.

c. Disponível em: http://idgnow.uol.com.br/computacao_corporativa /2010/11/23/sete-em-cada-dez-funcionarios-ja-roubaram-dados-de-seus-empregadores/. Acesso em: 6 de dez. de 2011.

d. Disponível em: http://idgnow.uol.com.br/seguranca/2011/05/10/mais-sofisticados-ataques-de-phishing-viram-ameaca-corporativa/. Acesso em: 8 de dez. de 2011.

e. Disponível em: http://idgnow.uol.com.br/seguranca/2011/09/21/ataques-de-engenharia-social-custam-caro-as-empresas-diz-estudo/. Acesso em: 8 de dez. de 2011.

f. Disponível em: http://idgnow.uol.com.br/seguranca/2011/06/30/*hacker*-invade-e-mail-de-dilma-rousseff-e-jose-dirceu/. Acesso em: 14 de dez. de 2011.

g. Disponível em: http://idgnow.uol.com.br/seguranca/2011/06/17/divulgacao-de-senhas-por-*hacker*s-leva-a-enxurrada-de-golpes-online. Acesso em: 10 de jan. de 2012.

ISO IEC 27002 – *Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação – Código de Práticas para Gestão de Segurança da Informação*.

IT Web. Disponível em: http://itweb.com.br/voce-informa/apenas-40-dos-funcionarios-levam-a-serio-a-seguranca-de-ti-da-empresa-onde-trabalham/. Acesso em: 8 de dez. de 2011.

LACEY, David. *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. West Sussex, England: Wiley, 2009.

LAVILLE, Christian; DIONNE, Jean. *A Construção do Saber. Manual de Metodologia da Pesquisa em Ciências Humanas*. Belo Horizonte: UFMG, 1999.

MITNICK, D. Kevin; SIMON, William L. *A Arte de Enganar – Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação*. São Paulo: Pearson Makron Books, 2003.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. *Segurança de Redes em Ambientes Cooperativos*. São Paulo: Novatec, 2007.

Neowin.net. Disponível em: http://www.neowin.net/news/microsoft-accuses-former-manager-of-stealing-600mb-of-data. Acesso em 7 de dez. de 2011.

SÊMOLA, Marcos. *Gestão da Segurança da Informação - Uma Visão Executiva*. Rio de Janeiro: Campus, 2003.

VROOM Cheryl (cherylv@webmail.co.za); SOLMS Rossouw (rossouw@petech.ac.za). Artigo *Towards Information Security Behavioural Compliance*. Publicado no *site* sciencedirect.com em 2004. Disponível em: http://www.sciencedirect.com/science/article/pii/S016740480400032X, acessado em 30 de janeiro de 2012.

WAINER Jacques. Métodos de Pesquisa Quantitativa e Qualitativa para a Ciência da Computação, 2007. Disponível em: http://www.ic.unicamp.br/~wainer/ papers/metod07.pdf. Acesso em: 15 de mar. de 2012.

Wired. Disponível em: http://www.wired.com/threatlevel/2011/09/ diginotar-*hacker*/). Acesso em 31 de jan. de 2012.

APÊNDICE

Apresentação

Esta pesquisa faz parte do trabalho de conclusão do curso do aluno Winícius Ferraz Neres na pós-graduação latc sensu em Redes de Computadores com ênfase em Segurança do Centro Universitário de Brasília - UniCEUB.

Tema do Projeto: A Importância do Fator Humano e Cultura da Segurança da Informação nos Ambientes Corporativos.

Público: Todas as pessoas que exercem atividade profissional remunerada.

Importante:
1- Procure responder o questionário com sinceridade.
2- Sua identificação não é necessária.

Agradeço pela participação!

***1. Possuo cargo de nível gerencial na empresa onde sou colaborador.**

○ Sim ○ Não

***2. Eu estou ciente de que posso receber contatos maliciosos, via e-mail ou telefone, simulando comunicações confiáveis de minha ou outras empresas com intuito de roubar informações corporativas ou pessoais.**

○ Discordo totalmente ○ Discordo parcialmente ○ Não sei opinar ○ Concordo parcialmente ○ Concordo totalmente

***3. Percebo que a direção da organização é comprometida com a segurança da informação.**

○ Discordo totalmente ○ Discordo parcialmente ○ Não sei opinar ○ Concordo parcialmente ○ Concordo totalmente

***4. A área de TI da empresa onde trabalho atende em tempo hábil às demandas de seus usuários.**

○ Discordo totalmente ○ Discordo parcialmente ○ Não sei opinar ○ Concordo parcialmente ○ Concordo totalmente

***5. Conheço plenamente a Política de Segurança da Informação da empresa onde presto serviço (Caso não exista a política, marque "Discordo totalmente").**

○ Discordo totalmente ○ Discordo parcialmente ○ Não sei opinar ○ Concordo parcialmente ○ Concordo totalmente

***6. Tenho muita dificuldade de criar e gerenciar as senhas de acesso aos sistemas corporativos.**

○ Discordo totalmente ○ Discordo parcialmente ○ Não sei opinar ○ Concordo parcialmente ○ Concordo totalmente

***7. A corporação organiza periodicamente eventos e ações sobre segurança da informação, tais como palestras, reuniões, folhetos e e-mails informativos.**

Discordo totalmente | Discordo parcialmente | Não sei opinar | Concordo parcialmente | Concordo totalmente

***8. Considero que a segurança da informação é algo muito importante para o sucesso da empresa, apesar de ela gerar alguns contratempos.**

Discordo totalmente | Discordo parcialmente | Não sei opinar | Concordo parcialmente | Concordo totalmente