UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO

Beatriz Menezes Machado

SEGURANÇA DA INFORMAÇÃO: ABORDAGEM DO TEMA COM FOCO NO USUÁRIO E SEU COMPORTAMENTO INFORMACIONAL SEGURO

Belo Horizonte

2013

Beatriz Menezes Machado

SEGURANÇA DA INFORMAÇÃO: ABORDAGEM DO TEMA COM FOCO NO USUÁRIO E SEU COMPORTAMENTO INFORMACIONAL SEGURO.

Monografia apresentada ao programa de Especialização do Núcleo de Informação Tecnológica e Gerencial – NITEG –, no curso de Gestão Estratégica da Informação da Escola de Ciência da Informação, da Universidade Federal de Minas Gerais, como requisito para a obtenção do certificado de Especialista em Gestão Estratégica da Informação.

Linha de Pesquisa: Segurança da Informação.

Orientador: Prof. Ricardo Barbosa.

Belo Horizonte
2013

Dedico este trabalho a todos aqueles que possuem sonhos, pois esse documento figura como prova de que eles podem se tornar realidade com esforço e fé.

AGRADECIMENTOS

A Deus, por me escolher, me permitir ser livre, me conhecer tão bem, me cuidar diariamente nos mínimos detalhes, enfim, pelo seu infinito amor.

A minha incrível mãe Célia e amada irmã Rackel, por todo o suporte e grande amor dedicado nos momentos mais complicados.

Ao meu querido namorado Lucas, o meu amor, por todo cuidado e ajuda nesse período.

Aos demais membros da minha família que sempre acreditou em mim e me incentivou.

Aos meus amigos especiais que me fortaleceram, apoiaram e colaboraram. Em especial à Silvinha, à Michele, ao Líbio, e mais especial ainda, à Lilian, ao Mateus e ao Paulo, porque, sem eles, definitivamente não teria conseguido.

À Sonda IT e aos seus colaboradores, meus colegas de trabalho, mais especificamente ao Mauro, ao Rafael, à Tatiane e ao Ivan pela compreensão nos momentos finais e mais cansativos.

Aos professores que fomentaram o interesse nessa área de conhecimento em mim. Desde a graduação com grande carinho à Silvia Calmon na área de segurança e amizade e ao Rodrigo Moreno por todo incentivo e crença em mim.

Agradeço aos mestres que me orientaram a um delicioso caminho pelo conhecimento específico na especialização.

Ao professor Ricardo Barbosa, meu orientador nesse trabalho pela oportunidade de trabalharmos em conjunto.

Ao professor Bax por aceitar o convite de composição da banca.

À Sônia, secretária do NITEG, pela atenção e sempre disponibilidade em me ajudar.

Aos 81 entrevistados do questionário que proporcionaram o material necessário a esse trabalho.

"A ciência humana de maneira nenhuma nega a existência de Deus. Quando considero quantas e quão maravilhosas coisas o homem compreende, pesquisa e consegue realizar, então reconheço claramente que o espírito humano é obra de Deus, e a mais notável."

Galileu Galilei

RESUMO

Os negócios estão cada vez mais interconectados, seja via Internet ou ainda sobre conexões de redes privadas na *Wide Area Network* (WAN). Dessa maneira, a informação está constantemente exposta a ameaças externas. Em função desse risco, grande parte das organizações possui sistemas que buscam reduzir esse tipo de ameaça. Mas não apenas ações tecnológicas são necessárias para que haja um procedimento adequado de proteção da informação, ainda é necessário intervenções sobre as pessoas e os processos organizacionais. Essa monografia tem como objetivo identificar o comportamento e avaliar o conhecimento dos funcionários de organizações, com atuação em diferentes nichos de mercado, em relação à segurança da informação. Para que esse objetivo fosse alcançado foi realizada uma pesquisa quantitativa através de questionário com questões que objetivaram analisar as políticas de segurança da informação existentes e também verificar o comportamento dos usuários da informação. O instrumento de coleta utilizado foi um questionário com perguntas objetivas aplicado via Internet.

Palavras-chave: acesso, segurança da informação, gestão do conhecimento, comportamento do usuário, normas de segurança, políticas de segurança.

ABSTRACT

Businesses are increasingly interlinked, either via Internet or private network connection on Wide Area Network (WAN). Thus, information is constantly exposed to external threats. Due to this risk, most organizations have systems that seek to reduce these threats. But not only technological actions are necessary for an adequate procedure to protect information, but interventions on people and organizational processes are also needed. The goal of this monograph is to identify the employees' behavior in these organizations and assess their knowledge while acting in different niche market, in relation to information security. For this goal to be achieved, a quantitative research was made through a questionnaire that aimed at analyzing existing security policies to protect information and at verifying users' behavior. This questionnaire, with objective questions, was the tool used to collect data and it was applied via Internet.

Key Words: access, information security, knowledge management, user behavior, security rules, security policies.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

EIC – *International Organization for Standardization*

ISO - *International Electrotechnical Commission*

SGBD - Sistemas de Gerenciamento de Banco de Dados Informacionais Digitais

WAN – *Wide Area Network*

LAN –*Local Area Network*

IDS – *Intrusion Detection Systems*

NAC - *Network Access Control*

PKI - *Public-key infraestructure*

CCSC - *Commercial Computer Security Centre*

RFC - *Request for Comments*

TSMC - *Taiwan Semiconductors Manufacturing Corp*.

SMIC – *Semiconductor Manufactoring Internacional*

DoS - *Denial of Service*

IC - Inteligência Competitiva

SCIP - *Society Competitive intelligence Professionals*

BYOD - Bring Your Own Device

SUMÁRIO

1 INTRODUÇÃO

Segundo a norma da ABNT NBRISO/IEC 17799:2005, da Associação Brasileira de Normas Técnicas, baseada na *International Organization for Standardization* (ISO) e na *International Electrotechnical Commission* (IEC), “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida”. Nos últimos 30 anos, principalmente após o surgimento dos Sistemas de Gerenciamento de Banco de Dados Informacionais Digitais (SGBD), as organizações têm se atentado ao valor da informação. O surgimento desses sistemas visava a organizar um mecanismo de busca e recuperação de dados de grandes massas de informações que são geradas pelas organizações. O uso dos SGBDs nas organizações a disponibilizou uma massa de dados com todo tipo de informações organizacionais. Esses dados organizados possuem diversas informações inerentes e importantes para o negócio. Tratar a segurança deles tende a ser um pensamento natural nos dias atuais.

Os negócios estão cada vez mais interconectados via Internet e demais conexões locais como as redes privadas *Wide Area Network* (WAN). Dessa maneira, toda informação está exposta a ameaças e conseqüentemente vulnerável. Passou-se então a uma busca tecnológica de meios que conseguissem garantir a inviolabilidade, por terceiros, dessas bases informacionais. Desde então, surgiram sistemas como o *firewall*, que é um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Utiliza-se também o *Intrusion Detection Systems* (IDS), que é um sistema de prevenção de intrusos que identifica tráfego suspeito e possíveis invasões de terceiros não autorizados via rede de dados. Existe também um dispositivo cuja ação é mais focada no usuário, o *Network Access Control* (NAC), que provisiona o controle de acesso à rede de dados por meio da validação de conformidade do perfil das máquinas e usuários de acordo com políticas de acesso pré-determinadas pelo administrador da rede local para aquele acesso. Os *Tokens* de acesso (chaves de criptografias individuais), *Public-key infraestructure* (PKI) que é a criptografia de chaves públicas visando garantir a troca de informações em ambientes inseguros de forma segura, além de outros métodos não citados aqui, procuram proteger a integridade dos dados organizacionais. Com essas tecnologias, as organizações

gastam milhares de dólares na esperança de que suas informações estejam seguras.

Visto isso, pode-se ainda observar que as empresas acabam, diminuindo outro lado importante das informações e dos seus ativos informacionais. Entende-se por ativo qualquer coisa que tenha valor para a organização conforme definido na norma ISO/IEC 13335-1:2004. A informação é gerada em diversos meios, não somente no meio digital. As pessoas ainda produzem muito papel e conversam bastante sobre assuntos profissionais em reuniões formais ou não. Seja qual for a maneira como essa informação circula, ela deve ser tratada com ações seguras.

De acordo com a norma brasileira ABNT NBR ISO/IEC 17799 (2005 p. IX):

> a 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.

Um contraponto que muitas vezes dificulta o processo de proteção das informações é que, segundo Fleury e Oliveira Júnior, (2001 p.17):

> o conhecimento organizacional constitui-se em ativo invisível que é acumulado vagarosamente ao longo do tempo e, desta forma, está impossibilitado de ser negociado ou facilmente imitado por concorrentes, uma vez que representa a base e os alicerces da história e da cultura da organização.

Entende-se por isso que a “chave” está nas mãos dos colaboradores, das pessoas envolvidas na produção diária, ou seja, não se pode revolver a questão da segurança da informação somente com a aplicação de um sistema da informação apenas tecnológico, a questão é muito mais abrangente do que isso.

Conforme Drucker (1994) os novos modelos econômicos precisam incorporar o conhecimento como o fator essencial do processo de produção e de geração de riqueza e não apenas figurarem como mais um fator de produção, pois o conhecimento tornou-se o recurso essencial da economia. Ainda sobre conhecimento, a gestão do mesmo que, de acordo com DAVENPORT e PRUSAK (1998), é um conjunto de atividades relacionadas com a geração, codificação e transferência do conhecimento, necessita ser realizado.

Dentro de um contexto de competição, o valor da informação tende a crescer exponencialmente. Portanto, faz-se necessário analisar o ponto de vista do usuário, dos colaboradores das organizações, visando a reduzir os custos com perdas informacionais e ainda fornecer uma orientação adequada quanto aos conceitos básicos que muitas vezes não recebem a atenção devida.

Comportamentos inadequados, ditos não seguros, dos funcionários das organizações podem ocasionar perdas financeiras para as suas respectivas empresas. O grande desafio é como fazer com que eles compreendam o valor da informação e a tratem de maneira segura.

Historicamente, a segurança da informação já foi estudada e aplicada inclusive durante as guerras mundiais. Um dos casos mais conhecidos envolve pessoas e técnicas de segurança da informação. Trata-se da criptografia das máquinas de escrever utilizadas pelos alemães, a Enigma. Ela começou a ser estudada por Marian Rejewski em 1932, que deduziu a estrutura detalhada do código do exército alemão, usando modelos matemáticos e a pouca documentação fornecida pelo capitão Gustave Bertrand da inteligência militar francesa oriunda de espionagem.

Mais recentemente, o poder da informação relacionado à ética pessoal ganhou destaque na mídia como no caso da General Motors e da Volkswagen no ano 2000, quando um executivo da GM aceitou um convite da Volkswagen para trocar de empresa, levando consigo planos de trabalhos confidenciais da concorrente (Cook & Cook, 2000). Cita-se também o caso da Oracle com a Microsoft, quando a primeira admitiu revirar o lixo da segunda em busca de informações relevantes. Esses são exemplos com resultados negativos derivados da aplicação inadequada do uso da informação em que o foco da questão é as atitudes das pessoas. Nesses casos, encontram-se colaboradores com problemas em seus valores intrínsecos, como, ética e moral, mas ainda há exemplos de funcionários que não agiram de “má-fé”, apenas foram inocentes e/ou mal orientados por seus empregadores. Exemplo dessa afirmação é o caso da Procter & Gamble (P&G) X Unilever em 2001. Nessa época, a P&G conseguiu informações confidenciais importantes da Unilever. Para tal, a P&G contratou uma empresa terceirizada para se passar por analistas de mercado, que realizou entrevistas com os funcionários da Unilever os quais, simplesmente, cederam informações à concorrente sem saber do que se tratava.

Adequações para esse tipo de comportamento, de uma forma comercial no que tange as organizações com fins lucrativos, começou de fato a ser padronizado na origem da ISO/IEC 17799, que data do final da década de 1980, quando no Reino Unido publicou-se em 1987 o *Comercial Computer Security Centre* (CCSC) que objetivava criar critérios de avaliações de segurança comercial para os usuários na área de tecnologia da informação. Esse sofreu diversas atualizações até a revisão final do ano 2005 que resultou na publicação da norma padrão ISO/IEC 17999.

Desde o ano 2000 até os dias atuais, constitui a época com maiores investimentos em segurança da informação nas organizações. Segundo a consultoria IDC, no Brasil, em 2011, o mercado atingiu US$ 779 milhões, sendo destinados 32% para *software*, 25% para *hardware* e 43% para serviços. Ainda segundo o IDC, apenas 15% das empresas sabem o que desejam contratar, contra 40% de empresas que têm alguma noção do que querem contratar, mas que precisam de orientação, e outros 40% de empresas que realmente não sabem nem por onde começar quando o assunto é segurança da informação. Mas é notado que, para haver uma quebra na segurança da informação, basta a quebra de um dos elos conforme declarou à Reuters o especialista da Agência de Segurança da Informação Européia, Steve Purser: “Você só precisa quebrar um dos componentes (pessoas, processos ou tecnologias) para atacar o sistema”.

Passa-se então a ter que focar em um sistema que contemple não somente equipamentos de tecnologia e sim uma política de segurança completa que, como pontuam as *Request for Comments* (RFCs) 2196 e 2828, a “Política de Segurança é um documento que deve descrever as recomendações, as regras, as responsabilidades e as práticas de segurança.” O que visivelmente não se limita a equipamentos tecnológicos e sim ao comportamento pessoal seguro.

Face ao exposto, o principal problema desse trabalho é identificar o comportamento dos colaboradores das organizações, nos mais diversos nichos de mercado, para verificar se as atitudes são tomadas com consciência de um comportamento informacional seguro.

Diante do cenário apresentando e do problema supracitado, a pergunta que norteia esse estudo é: o que é necessário para que os funcionários das organizações compreendam o valor a informação e a tratem de maneira segura? O objetivo primordial é: Identificar o comportamento dos funcionários de algumas

organizações com atuação em diferentes nichos de mercado em relação à segurança da informação.

Para auxílio nesse objetivo principal elencam-se os seguintes objetivos específicos:

a) analisar a existência de políticas de segurança da informação nas organizações estudadas; e
b) propor, com base na literatura, um programa de conscientização para as organizações no formato de construção de uma política de segurança;

Visto isso, a pesquisa ainda visa contribuir com as organizações no sentido de:

a) identificar o grau de entrevistados com relação à importância da informação dentro das organizações e sua participação nessa equação;
b) propor uma reflexão em todos os âmbitos de segurança informacional: pessoas, processos e tecnologia;
c) propor aplicações da norma ISO/IEC 17799 para as organizações no quesito treinamento dos seus funcionários rumo ao comportamento informacional seguro;
d) propor a capacitação dos colaboradores para compreender o contraponto de compartilhar a informação e de fornecê-la de maneira inadequada; e
e) justificar o investimento em tecnologia da informação, pois o usuário será capacitado a usar adequadamente a informação.

Além das justificativas e aspectos apresentados deseja-se, com esse trabalho, fomentar a discussão sobre segurança da informação do ponto de vista comportamental por entender-se a importância de levar esse assunto a um patamar em que todas as organizações entendam o quão relevante são os pilares dela: pessoas, tecnologia e processos, mas principalmente com foco nas pessoas.

2 REFERENCIAL TEÓRICO

Este capítulo tem como objetivo apresentar a base conceitual utilizada para executar a pesquisa. Será divido em seis partes. Todas elas visam definir os conceitos estudados para o presente documento, fundamentados pelos autores de maior renome no que tange a segurança da informação inclusive os conceitos de segurança da informação, padrões e normas de tecnologia da informação, organização da informação, proteção da informação, inteligência competitiva e gestão do conhecimento.

2.1 Conceitos de segurança da informação

Os conceitos abaixo são necessários para a compreensão do trabalho que se segue. Esses conceitos conforme definidos na norma ISO de segurança Internacional ISO/IEC 17799:2005 para atributos básicos da informação, são:

- ✓ confidencialidade: propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- ✓ integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição);
- ✓ disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- ✓ irretratabilidade: propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

Existem ainda duas outras definições introduzidas principalmente por Sêmola (2003) e Fontes (2006) que complementam a norma e que tratam como características importantes da informação como:

- ✓ legalidade: garante que a informação foi produzida dentro da conformidade da lei;
- ✓ autenticidade: permite que desde o momento de concepção da informação, no seu emissor, até a chegada da mesma no receptor a informação não sofreu nenhum tipo de alteração.

Os conceitos acima são amplamente conhecidos e divulgados pelos estudiosos e profissionais das áreas de segurança da informação das empresas em todo o mundo já que esses se tratam de características da informação segura.

Para definição do termo, segurança da informação, Fontes (2006 p.11) declara que:

> Segurança da informação é um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

A definição acima complementa a visão apresentada por Beal (2005) que trata segurança da informação como um processo de proteção da informação frente a ameaças de sua integridade, disponibilidade e confidencialidade.

Uma definição mais progressiva, um pouco mais focada na tecnologia, fez Sêmola (2003): “podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”. Sêmola reforça o acesso as essas informações como principal ponto de referência à segurança da informação e não pontua claramente a questão do ativo pessoa nesse processo.

É inegável que a informação passa a figurar como um grande fator de sucesso das organizações. Elas são instrumentos que devem ser organizados, classificados, analisados, protegidos e compartilhados.

As organizações enfrentam algumas questões que necessitam ser adequadas, já que o mercado demanda algumas mudanças. De acordo com Fugini e Bellettini (2001) segurança é um problema de negócio já que no ambiente mercadológico atual o foco está na segurança da informação e os desafios nessa área só tem feito crescer. Ressaltam ainda que outros desafios encontram-se na busca de tecnologias para proteger as informações, que padrões e regulamentos

ainda são muito recentes e complexos para o entendimento e aplicações corretos pelas organizações e que, ainda estamos apenas no começo das adequações legais de proteção a informação.

Uma vez conceituados os valores acima, passa-se a uma análise mais aprofundada dos caminhos adequados para a informação visando à segurança dos dados.

2.2 Organização da informação

Segundo Nonaka e Takeuchi (1997) o conhecimento está disseminado entre pessoas e processos de forma tácita e explícita, definidos conforme segue:

- ✓ conhecimento explícito: é o conhecimento que pode ser transferido de maneira formal por via de livros, repositório de dados, apresentações que proporcionem essa transferência por meio de aprendizado direto entre outros;
- ✓ conhecimento tácito: é o conhecimento intrínseco ao individuo, difícil de ser transferido para outrem. Está ligado as experiências pessoas de cada um, não somente isso mas também as crenças e ao sistema de valor do indivíduo. Ele é extremamente valioso e pode fazer com que uma organização se difira da outra devido à capacidade dos colaboradores que possuem um conhecimento tácito de acordo com o necessário ao negócio organizacional. Para transferi-lo é necessário observação e relacionamento.

Para armazenamento do conhecimento explicito dos colaboradores de uma organização nos dias atuais faz-se uso dos bancos de dados informacionais digitais (SGBDs). Esses sistemas visam, dentro do foco em segurança da informação, garantir a proteção dessas, fazendo com que algumas características seja garantidas. A norma ISO/IEC 17799 (2005), Sêmola (2003) e Fontes (2006) pontuam disponibilidades, integridade, confidencialidade, legalidade. Fontes (2006) ainda cita a auditabilidade como ponto a ser garantido, já que “significa que o acesso da informação deve ser registrado, possibilitando a identificação de quem fez o

acesso e o que foi feito com a informação". Abaixo se listam os níveis de acesso informacional citados por Fontes (2006):

- ✓ leitura: permite ao usuário acesso de leitura da informação apenas. Exemplo: retirada de um relatório de um SGDB de gestão de pagamentos da organização que demonstra o que foi creditado aos funcionários, permitindo apenas a visualização dos valores;
- ✓ escrita: permite que o usuário possa inserir informações no sistema. Exemplo: no mesmo SGBD do exemplo anterior, é permitido que o usuário insira os valores dos pagamentos da folha de colaboradores;
- ✓ remoção: permite ao usuário que remova informações do sistema. Exemplo: caso algum colaborados do exemplo anterior seja demitido e seja necessária sua retirada da folha de pagamento este usuário de sistema poderá retirá-lo;
- ✓ criação: permite ao usuário do sistema a criação de novas informações. Exemplo: da mesma maneira que no exemplo anterior no caso de inclusão de um novo colaborador este usuário poderia incluí-lo para sua aparição nos relatórios de listagem de folha de pagamento.

Criando classificações de usuários faz-se com que a informação se torne mais segura.

Um ponto que deve ser considerado também se refere à integração das informações disponíveis em uma organização. As organizações em sua grande maioria não possuem apenas um sistema local de armazenamento de informações. Já se verificou que as informações estão em diversos tipos de repositórios, sejam eles tecnológicos ou não. Fugini e Bellettini (2001) revelam alguns aspectos que devem ser analisados quando busca-se organizar e conseqüentemente integrar sistemas, como a seguir:

- ✓ autenticidade das informações;
- ✓ definição de acessos com permissões e bloqueio adequados;
- ✓ criptografia da informação caso ela seja migrada de local ou apenas armazenada;
- ✓ tratar de forma respeitosa e confidencial as informações disponíveis;

- ✓ gerenciar de maneira uniforme políticas heterogêneas em matéria de proteção de dados;
- ✓ preservar os dados de ataques externos (Internet).

Nesse ponto introduza-se uma das características mais relevantes do momento nas organizações e foco do trabalho, a proteção da informação.

2.3 Proteção da Informação

A proteção da informação é o fundamento do pensamento de segurança da informação. Proteger a informação é proteger a organização.

Qualquer empresa está sujeita a danos informacionais, sejam eles de vazamento por meio de seus colaboradores, por políticas inadequadas, invasões externas a sistemas externos, enfim, existem diversos pontos de atenção e meios pelos quais podem ocorrer uma disponibilização inadequada da informação. Dependendo do valor dessa informação, de quão sensível ela for para os concorrentes haverá um impacto financeiro na organização. Segundo Fontes (2006) “toda informação tem valor para a organização, para a concorrência e para o mercado em que ela atua”. Portanto, verifica-se uma necessidade de proteção que abranja todos os elos de segurança da informação: pessoas, processos ou tecnologias (Purser, 2004). A figura 1 explicita a relação entre os pilares e suas ações fundamentadas na estratégia da organização e sob o ponto chave, que é a conscientização.

Figura 1– Relação dos componentes de uma empresa: pilares e ações fundamentais de segurança da informação: pessoas, processos e tecnologia.

Fonte: Gestão de Segurança da Informação (LAUREANO, 2005, p. 113)
http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf

i) Pessoas

No âmbito de pessoas temos o mais abrangente campo, pois devemos tratar a segurança física, lógica e comportamental.

A segurança física está relacionada ao acesso das pessoas ao local de trabalho por meio de identificação de crachás, por exemplo. A inexistência de controle de acesso pode ter resultados indesejados, como no caso de uma das maiores fabricantes de chips de computadores do mundo de Taiwan, a *Taiwan Semiconductors Manufactoring Corp.* (TSMC). Em 2001 quando um colaborador, que não costumava ir à empresa aos finais de semana, foi e, permaneceu por horas fazendo cópias de documentos. Uma semana depois, esse funcionário pediu demissão e migrou para a empresa *Semiconductor Manufactoring Internacional* (SMIC), tida como uma empresa promissora no ramo com sede em Shangai. A proteção da informação falhou nos três âmbitos nesse exemplo, mas o início se deu no acesso físico ao local de trabalho. Quando não se tem o controle mínimo, como o acesso.Podem ocorrer casos ainda piores do que esse, sem mesmo que a

organização consiga detectá-los. Muitas vezes, são as evidências que se encontram no mercado que despertam a organização onde houve a falha, para que a mesma investigue o que pode ter ocorrido.

Existem algumas normas técnicas, ainda que desatualizadas, ABNT/NBR 11584 (1991) e a ABNT/NBR 11514 (1990) que trazem algumas definições sobre segurança física da área de trabalho dos colaboradores das organizações e referentes ao controle de acesso físico as instalações de processamento de dados.

A segurança lógica abrange níveis de acesso por meio de *software*s que buscam aumentar a segurança da informação. A primeira etapa se dá na identificação do usuário e autenticação desse. Segundo Fontes (2006) “a identificação informa ao ambiente computacional quem é a pessoa que está acessando a informação”. Esse identificação geralmente se dá por uma informação pessoal e única, como por exemplo o *login* de rede que é o nome e sobrenome ou então o Cadastro de Pessoa Física (CPF). Após a identificação é necessário que haja uma autenticação, ou seja, deve ocorrer a garantia que o usuário inserido é de fato aquele indivíduo, portanto essa informação que autentica o usuário deve ser sigilosa e de conhecimento pessoal e intransferível. Caso essa afirmação não seja verdadeira perde-se o valor da autenticidade.

Para ocorrer a autenticação de usuários existem alguns meios, que podem ser biométricos via impressão digital, verbalização para identificação de voz, reconhecimento facial, senha pessoal, *token* de acesso, equipamento que gera senhas automaticamente de forma aleatória sempre que solicitado, entre outros. Podendo ser utilizados individualmente ou como uma combinação como, por exemplo, identificação facial mais senha de acesso pessoal. O método mais utilizado atualmente pela maioria das organizações é o uso da senha pessoal, provavelmente porque ele possui o custo mais baixo de implementação de todas as outras opções disponíveis no mercado.

Muitas organizações não possuem apenas um sistema com senhas, o que faz com que sejam verificados o uso de senhas muito obvias para que elas não sejam esquecidas ou mesmo confundidas pelos colaboradores. Fontes (2006) e Fugini e Bellettini (2004) recomendam que não se use senhas óbvias como: datas de aniversário, seqüências conhecidas, muito curtas com menos de seis caracteres, apenas numéricas entre outras que sejam de fácil dedução. Recomendam-se senhas fortes e que sejam trocadas periodicamente de acordo com a norma

ISO/IEC17799 e dos autores supracitados. Um exemplo da importância de uma senha segura e protegida encontra-se em Moraes (2005). O autor conta a história ocorrida no instituto de criminalística de São Paulo, quando a polícia apreendeu muitos *notebooks* de uma quadrilha. Todos os equipamentos estavam protegidos por uma senha que era desconhecida e os criminosos não a divulgaram. Após o uso de alguns sistemas para descobrir a senha dos equipamentos eles verificaram que a senha possuía 8 (oito) dígitos mas não conseguiram mais informações. Os policiais especialistas tentaram todas as opções óbvias, datas de aniversário, nomes invertidos, combinações de nomes de pais e não conseguiram acessar os computadores. Os técnicos então observaram e perceberam que todos os criminosos tinham algo em comum, eles gostavam muito de futebol. Deduziram que seria o time deles, *Colo-Colo* (um time de futebol do Chile). A senha foi descoberta. O exemplo é de uma organização criminosa, mas podemos aplicar a facilidade de descoberta de senha no ambiente corporativo. No caso acima a polícia descobriu dados de seqüestros arquitetados que não ocorreram, calcular o impacto financeiro decorrente da descoberta da senha de um computador de um gestor da área de desenvolvimento de produtos de uma organização por terceiros é incalculável.

O ponto comportamental tem importante valor frente à senha individual. A senha passa a ser irrelevante a partir do momento em que a informação que deveria aferir autenticidade não é mais exclusiva e pessoal. Ocorre uma quebra de princípios quando a senha perde o seu sigilo e, portanto, o colaborador a compartilha com outros indivíduos. Para diminuir esse tipo de comportamento faz-se necessário a definição de processos e políticas informacionais adequadas, além de treinamentos para plena assimilação e convencimento aos colaboradores da importância de proteger a informação.

ii) Processos

Este estudo não pretende aprofundar a administração moderna com origem em Taylor (1970) e Fayol (1994). Apenas definiremos processo organizacional para compreensão do trabalho. Uma das melhores definições encontradas trata os processos de uma organização como uma série de tarefas ou etapas que recebem insumos (materiais, informações, pessoas, máquinas, métodos)

e geram produtos (produto físico, informação, serviço), usados para fins específicos, gerando os resultados esperados às organizações.

Segundo Davenport (1994) os processos de gerenciamento envolvem planejamento, metas, monitoramento, tomada de decisões e comunicação. O conhecimento desses processos é fundamental, visto que, conforme Chiavegatto (1999) o processo pode se tornar oneroso em demasia devido a lentidão que pode ocorrer em função do não conhecimento adequado da informação. Esses processos, também conhecidos como processos de responsabilidade de gestores, terminam por suportar todos os demais processos de uma organização. São esses processos que estão mais envolvidos com a gestão da informação e conseqüentemente sua segurança.

A todo o momentos negócios, os processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças que buscam identificar um ponto fraco, uma falha ou vulnerabilidade capaz de romper um dos pontos de segurança da informação. Quando isso acontece com sucesso, a quebra de segurança é consumada. (SÊMOLA, 2001).

A norma ABNT NBR ISO/IEC 17790:2005 cita alguns processos necessários para a segurança da informação. O principal é a análise a avaliação de riscos e suas aplicações aos processos específicos de negócio já existentes. Os processos de segurança da informação devem ser aderentes aos processos de gestão do negócio. A Norma ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação apresenta 133 controles para o Processo Organizacional da Segurança da Informação. Essa também, não explica como fazer para desenvolver ou mesmo implantar os controles e processos, mas pontua um caminho que pode ser seguido para conseguir o início de definição desses.

Para adequar a segurança da informação, após os processos organizacionais estarem adequados, as tecnologias figuram como o meio mais eficiente para o sucesso da segurança dos dados.

iii) Tecnologias

Segurança não é tecnologia, não é possível comprar um dispositivo que torne a sua empresa segura, assim como não é possível comprar ou criar um *software* capaz de tornar seu computador seguro (Wadlow, 2000).

As tecnologias auxiliam na segurança da informação em todos os tipos de segurança. Do acesso biométrico de entrada física ao local de trabalho, passando pelas senhas digitadas nos *software*s, nas câmeras de vigilância que atual sobre tecnologia IP, entre outros. Houve um ganho significativo com o uso da tecnologia nos processos produtivos. Desde a origem das máquinas na Revolução Industrial ocorrida na Inglaterra no século XVIII, a produção cresceu e precisou ser padronizada até os dias atuais com *smartphones*, que executam tudo que uma estação de trabalho tradicional possui,sendo assim uma grande evolução.

A Internet faz com que um novo mundo de oportunidades fosse explorado. Inicialmente utilizada para fins exclusivamente militares durante a Guerra Fria, foi-se expandindo, a princípio para a área acadêmica a partir dos anos 1970. Passou-se apenas a utilizar a Rede para fins comerciais na década de 1990. Hoje em dia é impossível imaginar que alguma organização consiga operar sem o uso da Internet de maneira adequada.

O ponto negativo do uso da rede, é que, a partir do momento em que se tem uma conexão externa à sua *Local Area Network* (LAN), fazendo com que ela se conecte a *Wide Area Network* (WAN), encontram-se alguns pontos de atenção que deve ser observados visando à proteção da informação. Onde se era limitado ao tráfego interno das informações agora se tem os programas em rede, envio de *e-mails*, servidores em nuvem, entre outros tipos de serviços que fazem com que o fluxo de informação não seja apenas local, e sim globalizado.

De acordo com a NIC BR *Security Office* (NBSO), o grupo de resposta a incidentes para a Internet brasileira, mantido pelo comitê gestor de Internet no Brasil, registrou 75.722 ataques de usuário final, de navegação de serviço do tipo *Denial-of-Service* (DoS) e a servidores Web em dezembro de 2004. O crescimento desse tipo de ameaça de segurança cresce a cada ano no Brasil e os dados que eles causam são alarmantes. Isso significa que as organizações estão ano após ano mais expostas aos danos que esses ataques podem causar. Para fazer com que as organizações não sejam vitimas desse tipo de ataque externo é necessário manter um processo de segurança da informação independente do tamanho da organização e do tipo de negócio, e para que esses processos tecnológicos funcionem é

fundamental a conscientização dos colaboradores. Abaixo se apresenta algumas soluções tecnológicas para proteção da informação nas organizações.

As organizações precisam definir claramente nos seus processos tecnológicos quais são os produtos homologados para lidar com cada tipo de ameaça. Um dos sistemas mais utilizados dentro de uma organização para se proteger os dados de ataques externos é o antivírus. Segundo Fontes (2006): “os vírus são programas que penetram no computador que utilizamos sem a nossa autorização e executam ações que não solicitamos”. Para evitar que esse tipo de ameaça roube informações indesejadas as organizações devem manter em seus servidores externos programas antivírus assim como também nas estações de trabalho de seus colaboradores.

Como já visto anteriormente o conhecimento possui grande valor para as organizações já que figura como grande parte do valor delas. Observamos que as pessoas, processos e tecnologia nos auxiliam para a gestão desse conhecimento. Tendo isto visto verifica-se a necessidade de discussão de mais alguns pontos, como a gestão do conhecimento propriamente dito e a inteligência competitiva.

2.4 Inteligência Competitiva

A inteligência competitiva (IC) é entendida como um processo organizacional, que tem o propósito de descobrir oportunidades e reduzir riscos, bem como conhecer o ambiente interno e externo da organização, visando o estabelecimento de estratégias de ação a curto, a médio e longo prazo (VALENTIM et al., 2003, p.2). Starec, Gomes e Bezerra (2006) e Sêmola (2003) extrapolam um pouco o conceito definido anteriormente ao afirmarem que a definição do conceito não é clara nem unânime entre os principais autores na área e que portanto, o ponto em que todos concordam, é que IC trata-se da análise de informações que são ativos críticos.

Dispor da informação correta, no momento adequado, significa tomar uma decisão de forma eficiente. A informação é o substrato da inteligência competitiva.

O que acontece com a inteligência competitiva é que, pode ser muito fácil para um profissional da área de IC sair do definido pela *Society Competitive intelligence Professionals* (SCIP) como suas atribuições que diz que:

> (...) trata-se de um programa sistemático e ético de coleta, análise, disseminação e gerenciamento das informações sobre o ambiente externo, que podem afetar os planos, as decisões e a operação das organizações.

A associação no Brasil também lista os seguintes pontos a serem respeitados pelos seus associados:

- ✓ exercer a profissão com zelo diligencia e honestidade;
- ✓ preservar a dignidade, prerrogativas e independência profissional;
- ✓ esforçar-se continuamente para aumentar o reconhecimento e o respeito à profissão;
- ✓ cumprir as leis aplicáveis, tanto no país quanto no exterior;
- ✓ manter sigilo sobre o que souber, em função de sua atividade profissional;
- ✓ evitar envolver-se em conflitos de interesse no cumprimento de seus deveres;
- ✓ assegurar as condições mínimas para o desempenho ético-profissional;
- ✓ emitir opinião, dar parecer e sugerir medidas somente depois de estar seguro das informações produzidas e de sua confiabilidade.

Fica explicita a preocupação, não apenas no Brasil, que cerca esses profissionais que tratam a inteligência competitiva já que o instrumento de trabalho deles é a informação muitas vezes sigilosa.

Existem muitos casos onde a IC é avaliada e tida como espionagem industrial. Quando uma pessoa não autorizada consegue acesso a uma informação que a organização está tentando proteger, esse ato se caracteriza como espionagem ou trapaça de acordo com Whitman e Mattord (2011). Os autores ainda afirmam que os invasores usam diversos métodos para acessar a informação armazenada e um sistema informacional. Definem como ato de inteligência competitiva um caso onde se consegue esse tipo de informação por meio de um *web browser*, para uma pesquisa de mercado na Internet. Mas muitas vezes faz-se uso de ações não éticas, e até mesmo ilegais.

Existe um caso recente que exemplifica o referido fato. Ocorreu no início do ano 2009 e foi resolvido no ano 2013. O caso envolveu duas grandes redes

hoteleiras americanas, a *Hilton* e *Starwood*. A *Hilton* foi condenada por roubar documentos da *Starwood* e copiar um empreendimento conceitual que estava contido neles. A informação fez com que a *Hilton* construísse mais rápido que a *Starwood* um novo conceito de hotel fazendo com que ela parecesse inovadora e obtivesse lucros inesperados. O valor da informação é de fato irrefutável e existem níveis de classificação dessas informações. Segundo Laureano (2005):

- ✓ pública, informação que podem ser conhecidas sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
- ✓ interna, o acesso a esse tipo de informação deve ser evitado, embora as conseqüências do uso não autorizado não possuam conseqüências graves. Sua integridade é importante, mesmo que não seja vital;
- ✓ confidencial, informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional. Eventualmente pode ocasionar perdas financeiras, ou de confiabilidade perante o cliente externo e permitir vantagem expressiva ao concorrente;
- ✓ secreta, informação crítica para as atividades da empresa, cuja integridade deve ser preservada. O acesso deve ser restrito a um número reduzido de pessoas. A manipulação desse tipo de informação é vital para a organização.

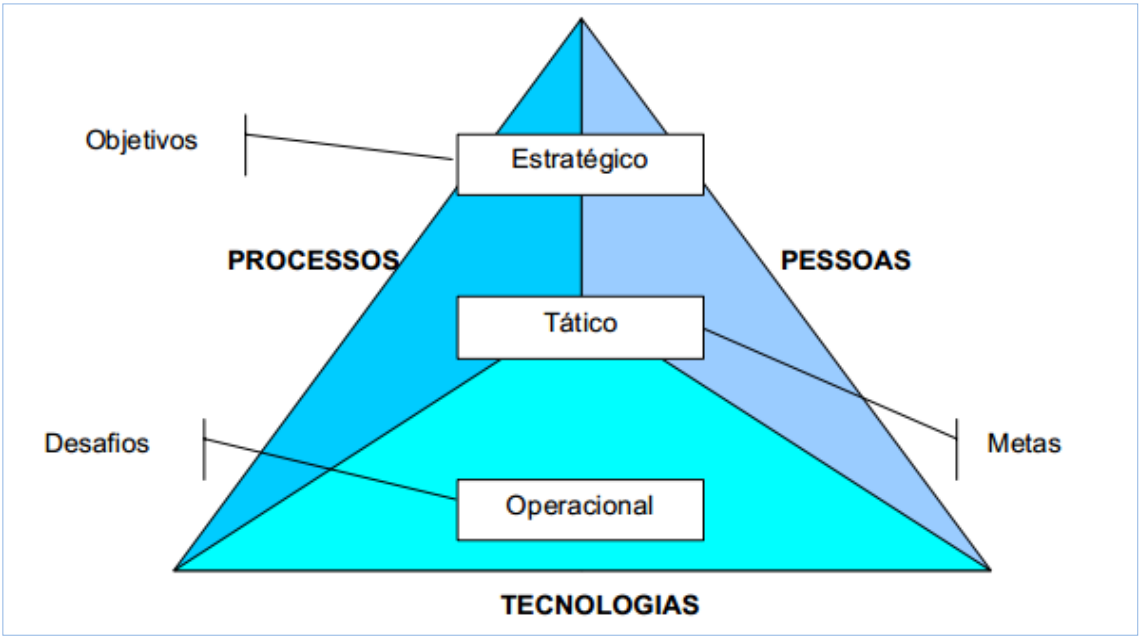
Para o adequado controle e gerenciamento das informações de uma organização faz-se necessária a gestão do conhecimento da informação.

2.5 Gestão do Conhecimento

Entende-se gestão do conhecimento como um conjunto de estratégias para criar, adquirir, compartilhar e utilizar ativos de conhecimento, bem como estabelecer fluxos que garantam a informação necessária no tempo e formato adequados, a fim de auxiliar na geração de ideias, solução de problemas e tomada de decisão (VALENTIM, 2003,p.1).

A informação trafega nos três pilares de acordo como mostra a figura 2:

Figura 2 – Tecnologias: níveis organizacionais em contraponto com os pilares de segurança da informação.



Fonte: Gestão de Segurança da Informação (LAUREANO, 2005, p. 4)
http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf

De acordo com Bateman e Snell (1998), as organizações podem ser divididas em três níveis: estratégico, tático e operacional. Cada um desses níveis são bem divididos no que tange ao fluxo de informações. As informações estratégicas, mais valiosas, tendem a circular no nível estratégico e algumas vezes são pontuadas no tático. Segundo Freitas e Kladis (1995) em todos os níveis da organização a informação é um recurso fundamental.

Do ponto de vista organizacional, Barclay e Murray (1997) consideram a gestão do conhecimento uma atividade de negócios com dois aspectos básicos:

- ✓ tratar o componente de conhecimento das atividades de negócios explicitamente como um fator de negócios refletido na estratégia, política e prática, em todos os níveis da empresa; e
- ✓ estabelecer uma ligação direta entre as bases intelectuais da empresa explícitas (codificadas) e tácitas (conhecimento pessoal) – e os resultados alcançados.

A informação transformada em conhecimento é o componente mais importante das organizações, sendo diretamente responsável pelo seu sucesso. De acordo com Handy (1995), a inteligência é o novo tipo de ativo. Não se comporta

como os outros tipos de ativos e nisso reside o paradoxo. Ao contrário dos outros bens, a inteligência não pode ser dada de presente e será sempre conservada, mesmo que compartilhada. Também não é possível possuir a inteligência de outra pessoa. Se o colaborador sair da empresa e for para outra, levará consigo a inteligência.

Gerir ativos de conhecimento intangíveis é um dos grandes desafios dos gestores da atualidade. Fontes (2006) ressalta que a proteção da informação é responsabilidade de cada pessoa na organização, independente do seu nível hierárquico.

Dentro da gestão do conhecimento existem algumas ações que devem ser realizadas para que possam ser reduzidas as perdas informacionais.

Barclay e Murray (1997) adotaram uma classificação de abordagem de gestão do conhecimento em três grupos:

- ✓ abordagens mecanicistas: focada na tecnologia para trazer melhores resultados. Exemplo: melhor meio de acesso a informação;
- ✓ abordagens culturais/comportamentais: são os processos de reengenharia e gestão de mudanças da cultura organizacional. O foco é o processo e a ação dos gestores;
- ✓ abordagens sistemáticas: o foco está na análise do problema o que necessita é uma mudança de pensamento. Questões culturais são analisadas.

Após essa análise passa-se para a aplicação de alguns conceitos com a criação de políticas de segurança da informação.

2.6 Políticas de segurança da informação

Atualmente existe uma *request for comments* (RFC) 2196, também conhecida como *Site Security Handbook*, que descreve, que “uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização”. De acordo com a afirmação anterior pode-se aferir que sem regras adequadas sendo aplicadas e executadas adequadamente pelos colaboradores da organização não se consegue uma política

de segurança consistente. De acordo com Fontes 2006, é necessária uma definição e implementação clara das políticas e das regras, explicitando inclusive a filosofia delas, para a compreensão e conseqüente comportamento adequado dos colaboradores.

Políticas de segurança para o usuário, ainda nos dias de hoje, são praticamente inexistentes dentro das organizações. As políticas de senhas e orientações de uso de tecnologia são as mais presentes e definidas claramente na ISO 27001 de 2005 que figura inclusive, como certificação de padrão de qualidade em diversas organizações.

Martins e Santos, (2005) de maneira mais prática do que as normas de segurança presentes atualmente, recomendam que a política de segurança deva abranger os seguintes tópicos:

- ✓ propriedade da informação: é interessante determinar o responsável pela informação, pessoa que poderá definir quem poderá ter acesso às informações e que nível de acesso é permitido, e qual a periodicidade necessária para a realização do backup desta informação;
- ✓ classificação da informação: o gestor deverá classificar a informação quantos aos princípios de disponibilidade, confidencialidade e integridade;
- ✓ controle de acesso: deve atender ao princípio de menor privilégio. Todo pedido de acesso deve ser documentado. Deve-se evitar a segregação de função, por exemplo, um mesmo usuário não deve ter acesso à geração de pagamento e liberação do mesmo. É importante, também, que se mantenham as trilhas de auditoria no sistema;
- ✓ gerência de usuários e senhas: As senhas devem ser únicas e individuais, seguindo critérios de qualidade, isto é, senhas fortes com trocas periódicas. A responsabilidade da senha é do usuário proprietário da mesma;
- ✓ segurança física: Os acessos a áreas de servidores devem ser consentidos mediante autorização. Deve-se ter controle quanto à entrada e saída de equipamentos e pessoas, recomendando-se a

criação de normatizações de controles internos referentes à segurança física, os quais deverão ser auditados periodicamente;

- ✓ desenvolvimento de sistemas ou compra de sistemas/*software*: é importante definir uma sistemática interna com ênfase nos requisitos de segurança;
- ✓ plano de continuidade de negócios: é um dos mais importantes tópicos na política de segurança, sendo recomendada a geração de controles e padrões especificando detalhes quanto ao plano de contingência e continuidade dos negócios.

Assim, baseando-se no que foi visto até o momento e com o objetivo de estudar a segurança da informação com foco no usuário, são apresentados abaixo mais alguns pontos relevantes que foram utilizados na elaboração do questionário utilizado na presente pesquisa.

Purser (2004) ressalta em seu livro que a atenção nos últimos anos está sobre a tecnologia, metodologias e técnicas e que de fato esses conseguem reduzir os riscos de perdas informacionais.

Algumas ações são propostas por Fontes (2006) visando o reduzir os riscos e combater os problemas que podem ocorrer devido a falhas. Lista-se abaixo algumas dessa ações:

- ✓ ações preventivas: são ações que geralmente são mais simples e fáceis de assimilar cujo objetivo é evitar que a falha aconteça. Para isto toma-se pedidas simples, como manter o *notebook* do seu trabalho fixo a mesa enquanto o colaborar se encontra na organização até mais complexas com *software*s especializados em segurança que analisam o tráfego procurando por falhas, identificando acessos não autorizados entre outros;
- ✓ ações detectivas: o segundo nível de ação são as detectivas. Essas passam a vigorar quando as preventivas não obtiveram sucesso. Cita-se o sistema de detecção de incêndio como exemplo claro dessas ações. O ideal era que não ocorresse fogo no local, mas como ocorreu, o sistema entra em ação para avisar que o problema aconteceu. No meio virtual dentro de uma organização um exemplo

claro de políticas detectivas é o bloqueio de uma senha após a mesmas ser digitada incorretamente mais de três vezes;

- ✓ ações corretivas: o principal objetivo desse tipo de ação é minimizar o problema. Um exemplo aplicado ao contexto organizacional é quando ocorre um ataque na rede de dados, seja ele interno ou externo, que faz com que a rede principal fique inoperante. O caminho alternativo, ou a ação corretiva, é utilizar o caminho redundante que muitas vezes passa por outros equipamentos menores. Dessa maneira a organização passa a operar de forma alternativa, mas operante.

O questionário avaliou ainda os seguintes itens:

a) segurança física: com questionamentos nessa área visa-se a abranger o cotidiano do trabalhador em sua empresa no que tange a parte física do processo. Definiu-se, por segurança física, itens de acesso ao local de trabalho como catracas e crachás de identificação. Com essas questões verificou-se o nível de segurança das organizações num quesito que se compreende como elementar de segurança, a parte não lógica do processo;
b) segurança lógica: as organizações disponibilizam, na grande maioria das vezes, equipamentos eletrônicos para seus funcionários trabalharem. Esses equipamentos, usualmente computadores, tendem a funcionar interligados em rede, o que permite acesso aos dados da organização. Portanto, medir o grau de segurança lógica, ou seja, como o funcionário lida com a segurança informação no seu meio digital, torna-se imprescindível. Avaliou-se nas questões desse item a interação do funcionário com o equipamento, se lhe é permitido acesso sem senha ou se pode retirar informações do mesmo sem auxílio e/ou controle;
c) comportamento seguro: nesse tópico buscou-se identificar o comportamento do usuário propriamente dito. O item é amplo e abrange questões típicas como se ocorre bloqueio da tela do computador na ausência do usuário até questões como abordagens fora do local de trabalho por terceiros sobre assuntos pertinentes à

empresa também foram investigadas. A ideia central desse tópico é verificar a interação entre os funcionários do ponto de vista comportamental e pessoal, independente de políticas de segurança da informação e/ou normas internas;

d) controle da informação: as organizações possuem geralmente um nível hierárquico, que segundo Stoner (1992) é a forma pela qual as atividades de uma organização são divididas, organizadas e coordenadas. Nesse item, buscou-se verificar como a informação é tratada sob esse ponto de vista. Questões de conhecimento de senha de superiores e criações de níveis de confidencialidade foram abordadas;
e) políticas de segurança da informação: buscou-se apurar a maturidade das organizações no que tange à existência de políticas de segurança da informação. Propondo questões como desde se elas existem, até se ocorrem treinamentos e se estão disponíveis para os funcionários as consultarem sempre que houver dúvidas de procedimento;
f) conhecimento de normas organizacionais de segurança da informação: as questões levantadas nessa subdivisão buscam aferir o conhecimento dos participantes da pesquisa sobre as normas de segurança da informação adotadas pela organização na qual trabalha;
g) acesso móvel: questões de acessos a dados corporativos em dispositivos móveis, como *tablets* e *smartphones*;
h) acesso remoto: questões quanto à maturidade das organizações para prover acesso aos dados da mesma quando o funcionário não está fisicamente no local de trabalho;
i) informações gerais: sexo dos entrevistados e dados da organização foram pesquisados.

3 PROCEDIMENTOS METODOLÓGICOS

A primeira parte do estudo realizado foi a pesquisa bibliográfica e estudos de documentos acadêmicos publicados sobre o assunto. Segundo Lima (1997) pesquisa bibliográfica é a tarefa de consultar fontes de informação escritas com o objetivo de obter dados em relação ao tema pesquisado. O autor define, ainda, livros, dicionários, periódicos, monografias, dissertações, artigos, entre outros, digitalizados ou em papel, como fontes formais da pesquisa bibliográfica. A pesquisa bibliográfica tem o objetivo de fundamentar a base para os objetivos específicos e secundários como compreender o comportamento informacional, a segurança da informação e as informações organizacionais.

No que diz respeito à classificação da pesquisa, conforme Vergara (2000), trata-se de uma pesquisa descritiva, cujo objetivo final é identificar as características da população investigada. O questionário foi aplicado de forma que tornasse possível verificar dentro da população analisada os comportamentos amplos e não somente um grupo específico fazendo com a pesquisa seja mais abrangente e permita uma visão do todo.

3.1 Universo e População

Uma vez que o objetivo principal desta pesquisa é identificar o comportamento dos funcionários de diversas organizações com atuação, em diferentes nichos de mercado, em relação à segurança da informação, o foco da pesquisa está no comportamento informacional dos trabalhadores.

Devido a não especificidade de uma população, o critério adotado para determinar o público a ser pesquisado foi limitar apenas as áreas de atuação das organizações por meio de direcionamento e envios direto de *e-mails*. A pesquisa não se limitou ao envio específico de *e-mails* individuais, já que ficou disponibilizada em *blog* na Internet. De qualquer maneira, buscou-se limitar as organizações por área de atuação como serviços financeiros, educação e tecnologia da informação. No conjunto das empresas do setor financeiro encontram-se os bancos, no de educação as universidades, enquanto no setor de tecnologia da informação são enquadradas as empresas de tecnologia.

O estudo também contemplou uma comparação entre empresas públicas e privadas para verificar o comportamento do mercado em relação à segurança, tomando esse posicionamento como ponto interessante a se observar.

O questionário foi respondido por 81 pessoas durante 2 (duas) semanas de exposição. Um dos meios escolhidos para aplicação do questionário foi uma ferramenta *online* do *Google*, o *Google Docs*[1], permitindo que dessa forma fosse mantida a acessibilidade e segurança dos dados.

Ressalta-se ainda que o questionário passou por um período de testes antes de sua divulgação, durante o qual foram obtidas cinco respostas de pessoas escolhidas com experiência na área de informação para validação do mesmo. Essas cinco respostas prévias serviram para validar o conteúdo, entendimento adequado e tempo de resposta. Essas respostas iniciais foram desconsideradas na análise final, que será apresentada a seguir.

A análise apresentada a seguir, em forma de gráficos, também se baseia na referida ferramenta, o *Google Docs*[1]. O questionário aplicado, exatamente da maneira que estava disponibilizado na Internet, é apresentado no Anexo 1.

Segue análise exploratória de dados qualitativa com análise de freqüência das respostas e gráficos. O documento objeto do estudo são as respostas do questionário aplicado. Esse questionário tem 57 perguntas divididas em 12 assuntos relacionados à segurança da informação no ambiente organizacional. Esses assuntos ou temas são os seguintes:

1. acesso físico ao local de trabalho;
2. controle de documento físico: impressões, descarte de material, etc.;
3. controle do uso da estação de trabalho;
4. senhas;
5. compartilhamento de informação;
6. uso da Internet;
7. políticas de segurança da organização;
8. comportamento seguro;
9. acesso remoto e móvel;

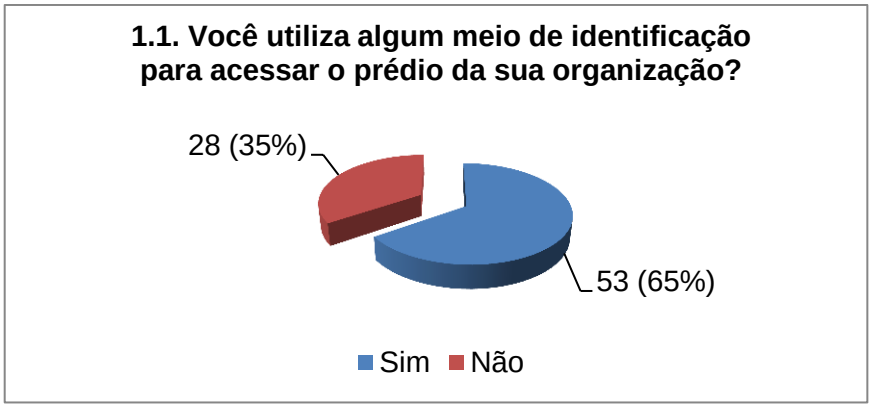
[1]https://docs.google.com/spreadsheet/viewform?formkey=dDFFbnpfbzNWNldRYmotSE5IbFNId2c6MQ#gid=0. A outra forma de divulgação do questionário foi via blog, disponível em: http://daydreamschristians.blogspot.com.br/2012/09/pesquisa-especializacao-ufmg.html.

10. sexo;
11. natureza da organização; e
12. setor de atuação da organização.

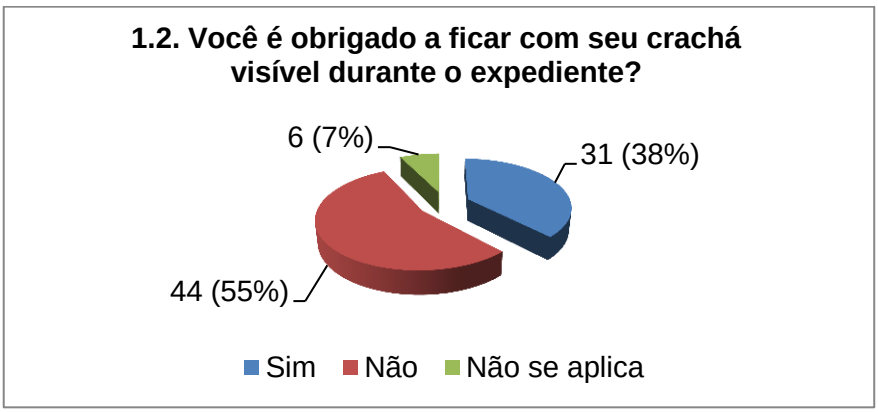
A subdivisão acima apresentada não fica explicitada para o entrevistado, à medida que ele progride no formulário, o questionário se adequa conforme as respostas, mudando assim de item e subitem. Algumas dessas mudanças serão detalhadas durante a análise individual das questões, visto que, as amostram podem ter sua quantidade alterada devido ao desdobramento e/ou evolução de uma questão em outra. Por exemplo, com uma questão principal de sim e não e a secundária que analisa apenas os respondentes de sim. Os valores apresentados na análise que se segue serão apresentados em freqüência de valores absolutos (quantidade de pessoas) e relativos (porcentagem).

4 ANÁLISES DE RESULTADOS

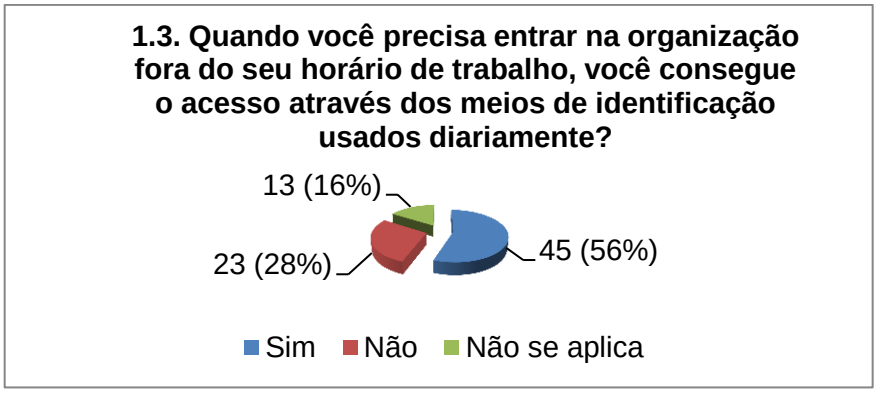
A seguir apresento gráficos que elaborei, apresentando o resultado e a análise das respostas de cada questão, de acordo com os referidos temas.



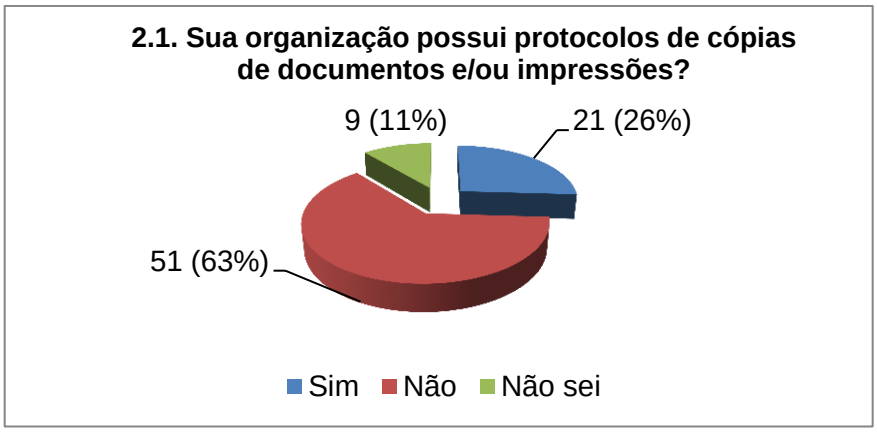
A questão acima procurou identificar se as questões de segurança física estavam sendo abordadas. Verificou-se que 65% dos funcionários das organizações utilizam algum meio de identificação para acessar o local de trabalho. Esses dados revelam que as organizações, em sua maioria, se importam com o acesso físico ao local de trabalho, garantindo assim um nível básico de segurança física de acesso.



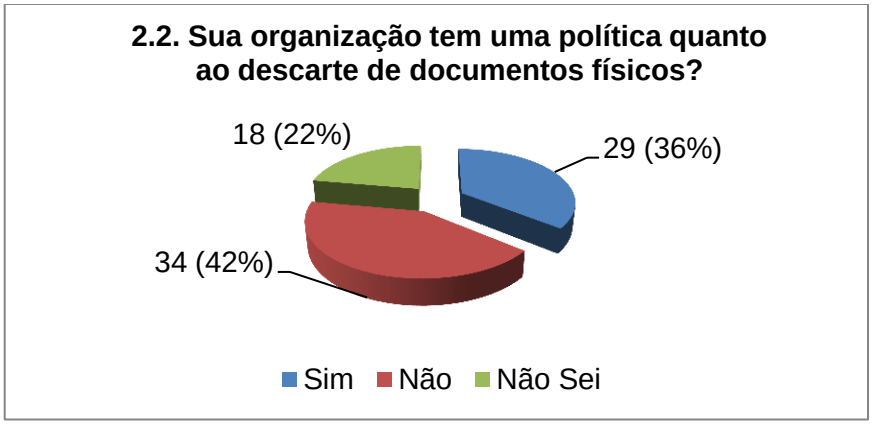
Os dados acima demonstram uma falha nos sistemas de segurança das organizações estudadas que, em sua grande maioria, não exigem que os funcionários deixem sua identificação à vista para identificação sempre que necessário.



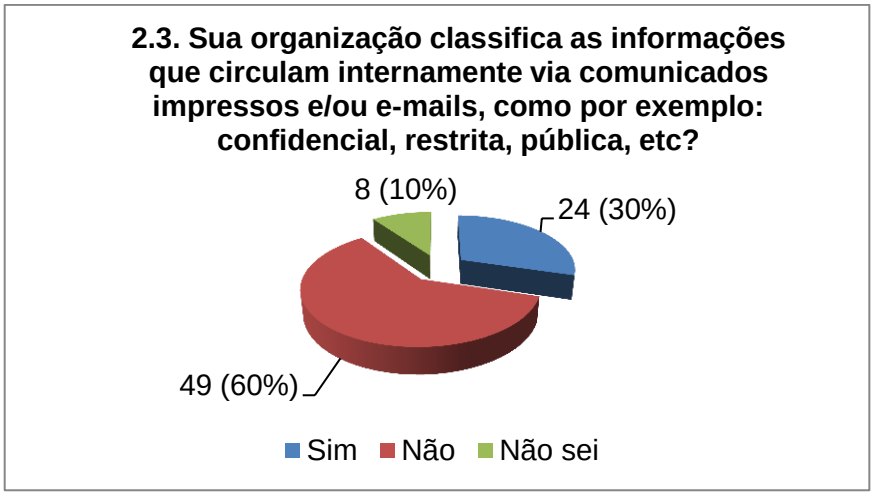
Com esse questionamento buscou-se verificar se os acessos dos colaboradores podem ocorrer fora do horário comercial com os mesmos critérios de acesso de horário de expediente diário. Mais da metade deles pode acessar o local de trabalho sem autorização prévia, apenas com o acesso diário o que é um ponto de atenção de segurança informacional.



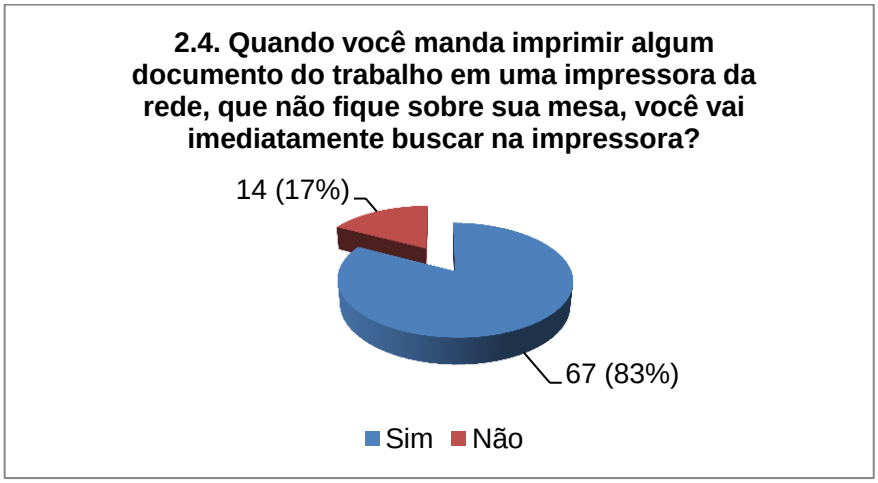
A verificação nessa questão se referia a proteção da informação não digitalizada e ainda amplamente produzida conforme vimos nos referenciais anteriores neste trabalho. Constatou-se que na maioria das organizações não existe nenhum controle de cópias ou impressões, o que configura-se como grande ponto de falha de segurança.



Verifica-se nessa questão, que a maioria das organizações não possui políticas de descarte de documentos. Ressalta-se que uma parte considerável delas, 36% buscaram o controle de descarte e portanto possuem políticas adequadas para essa questão. E outra parte significativa, 22% desconhecem a existência dessa política em suas organizações. Essa questão chama a atenção pelo fato de ter suas opções equilibradas, distinguindo-se da anterior onde o fundamento tem origem semelhante, a segurança da informação física. Pode-se afirmar que não existe controle de cópias e impressões na maioria das organizações, mas que também há uma dificuldade de entendimento dos fundamentos da segurança informacional já que houve um equilíbrio nas repostas referentes ao descarte dessa informação que pode ter sido impressa sem controle.

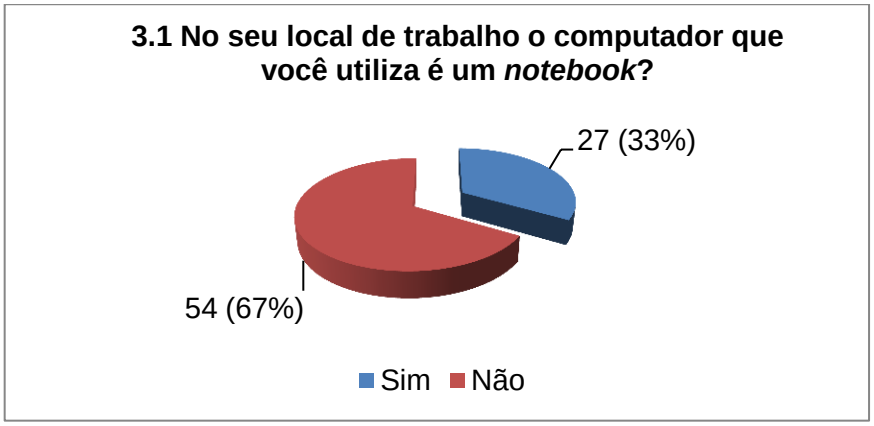


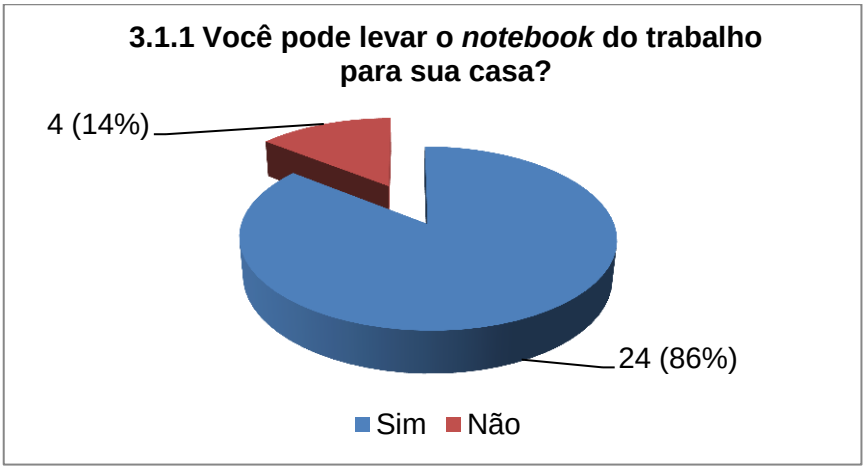
O intuito dessa questão era avaliar se a informação que trafega dentro da organização é classificada. Como ficou constatado a grande maioria das empresas ainda não classificam a informação o que permite que elas sejam acessadas por qualquer colaborador.



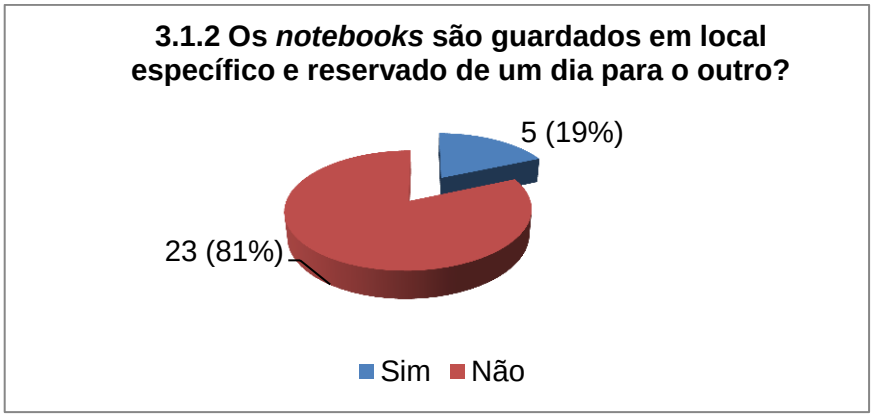
Aqui a segurança física é avaliada em conjunto com o comportamento do usuário. A maioria dos colaboradores respondeu afirmativamente a questão, o que revela colaboração e ainda cuidado com a informação que foi impressa para que outros não possuam acesso ao documento.

A série de perguntas que vem a seguir buscou identificar o comportamento do usuário de informação que possui dispositivo móvel para uso profissional.

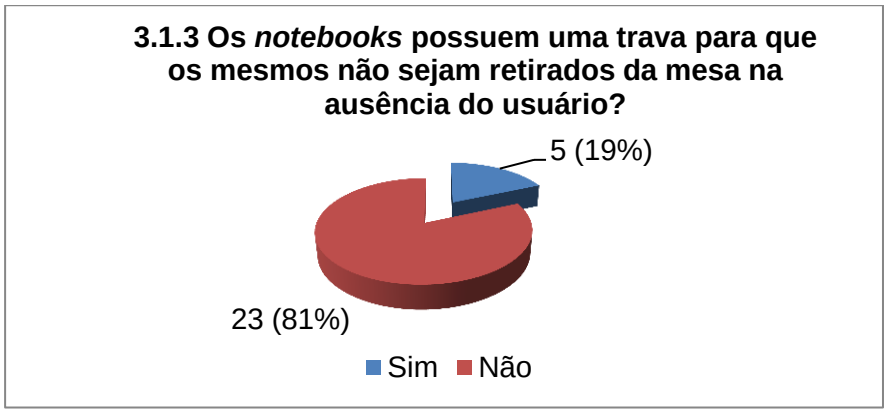




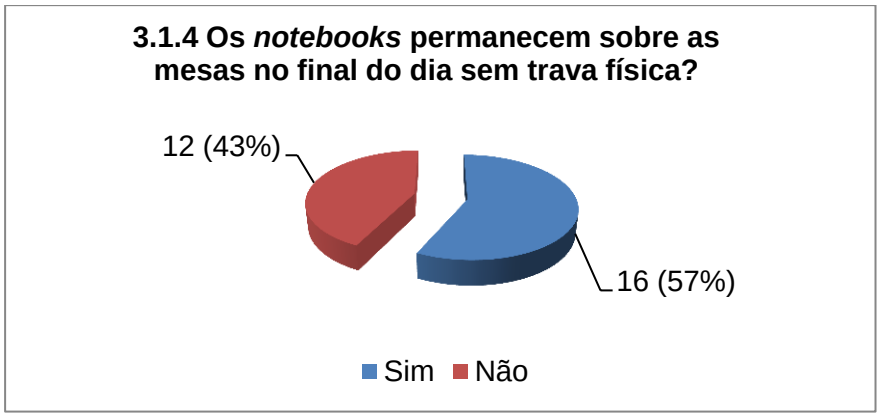
Do universo de 81 pesquisados apenas 28 deles, ou 33%, possuíam *notebook* de trabalho sendo que a enorme maioria 86% tem permissão de levar o dispositivo para sua residência. Ressalta ainda que a amostra se reduz nas perguntas que se seguem: 3.1.1, 3.1.2, 3.1.3, 3.1.4 e 3.1.5, visto que elas retratam um aprofundamento dos respondentes de sim da resposta da pergunta principal, a 3.1. Por isso a amostra é reduzida para 28 colaboradores no bloco que se segue.



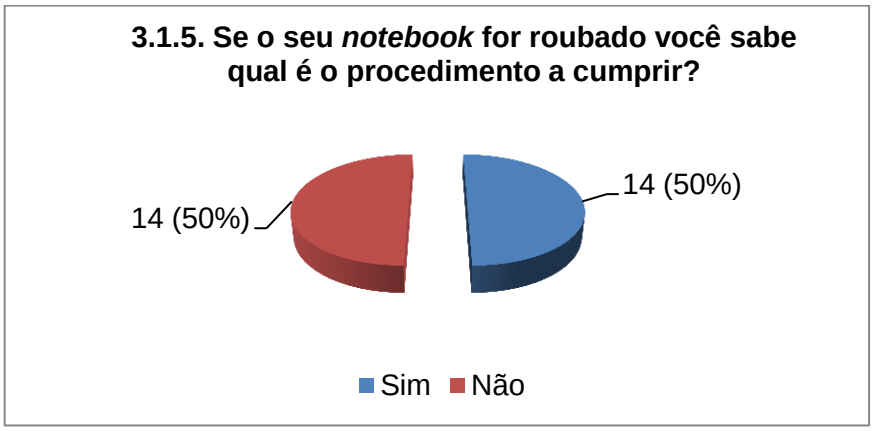
Quanto a segurança física dos *notebooks*, a pesquisa revelou que apenas 19% das organizações fazem com que os colaboradores guardem o dispositivo no final do dia para que o mesmo fique protegido, fora do acesso de terceiros como ação preventiva, reduzindo as falhas de segurança informacional.



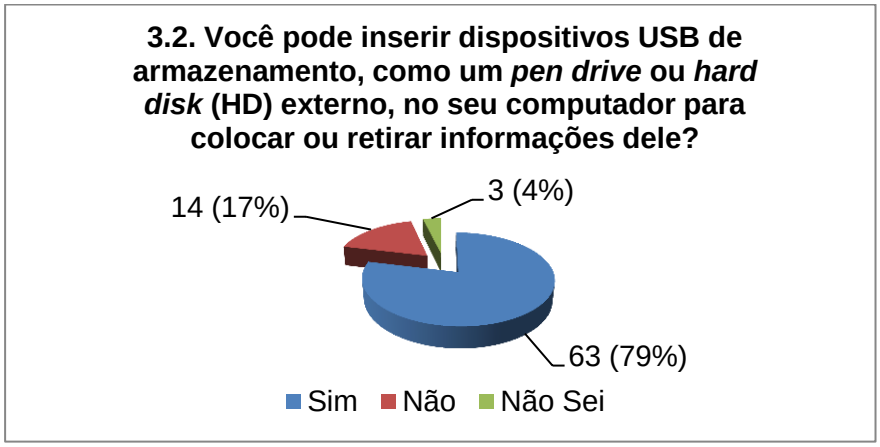
A trava física figura como outra ação preventiva já mencionada anteriormente neste trabalho. Verificou-se que a mesma porcentagem dos colaboradores que recebem diretrizes para guardar o *notebook* em local adequado, o prende à trava. O objetivo é o mesmo, proteger a informação de maneira física.



Já essa questão aprofunda a pesquisa das questões anteriores. Os mesmo colaboradores que guardam o *notebook* nos dias de semana não o guarda nos finais de semana. Essa diferença se dá primeiro porque alguns levam o equipamento para a casa e outros tem a política válida apenas para o final de semana.

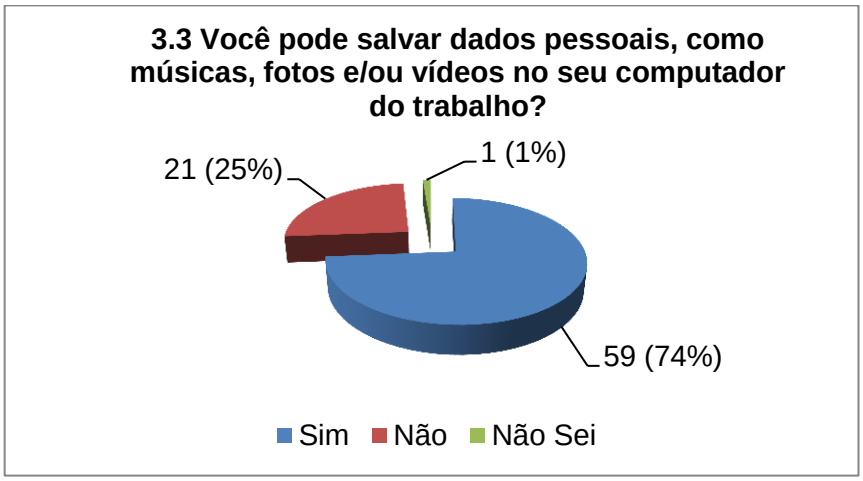


Avançando sobre os procedimentos de segurança relacionados já a política de segurança, os colaboradores são questionados se conhecem o padrão interno de procedimento em caso de furto ou roubo do dispositivo móvel. A pesquisa chama a atenção nesse ponto porque ocorre um empate alarmante. Os colaboradores utilizam de um dispositivo que a organização forneceu a eles, mas percebe-se que o procedimento de gozo do bem organizacional não é conhecido por muitos.

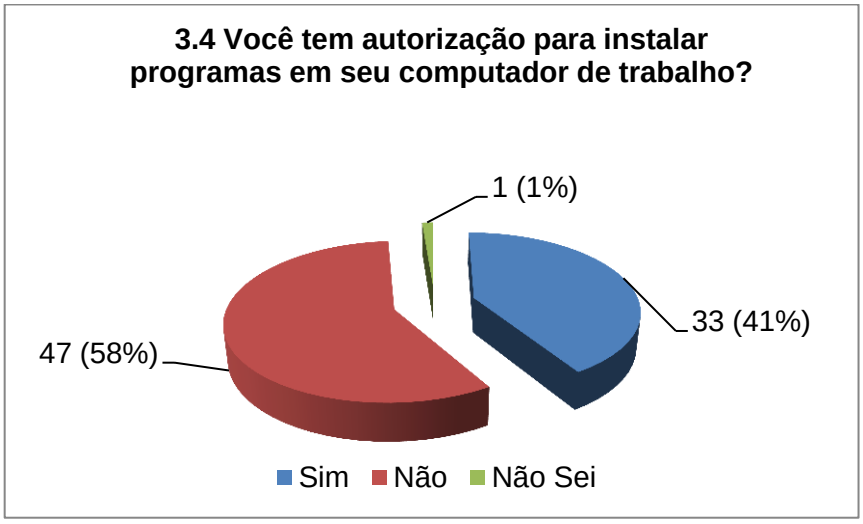


As perdas informacionais com inserção de dispositivos *universal serial bus* (USB) são muitas vezes incalculáveis, primeiro porque dispositivos externos são

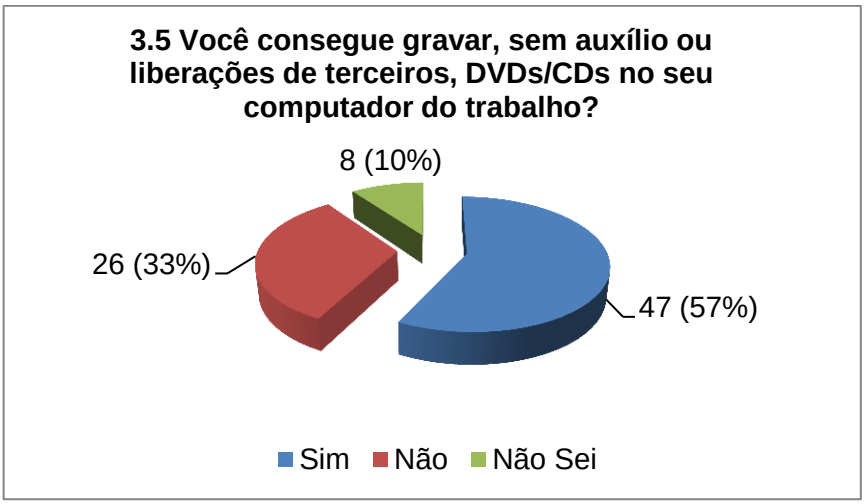
grandes portadores de vírus de terceiros que se instalam sem o conhecimento do colaborador e posteriormente porque o uso destes permite que sejam retiradas informações do dispositivo e inseridas em qualquer outro equipamento não autorizado. A maioria dos entrevistados possui esse tipo de permissão, o que revela um nível de segurança insatisfatório. Ressalta-se que ainda existem usuários que sequer conhecem se podem ou não executar esse tipo de tarefa, o que alarma a área de treinamento do mesmo nos procedimento básicos de computação.



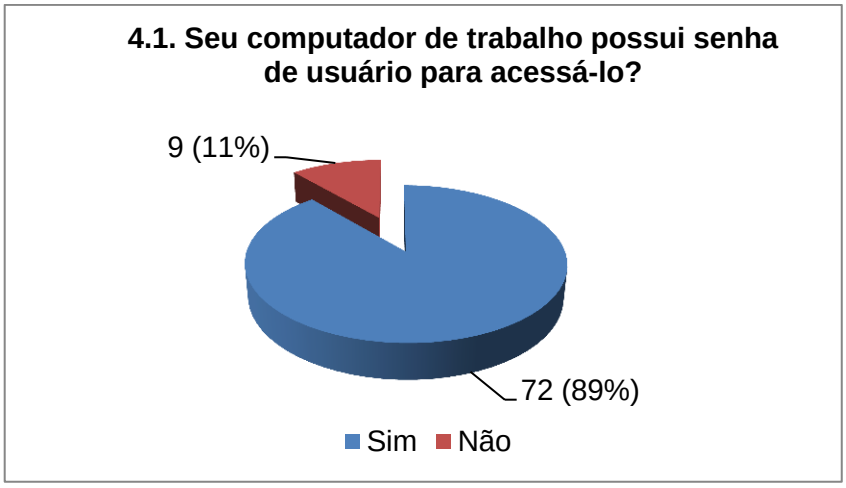
O salvamento de dados pessoais no computador revela alguns pontos de falha da política de segurança. Podem ser a autorização de fazer *downloads* de locais desconhecidos para a rede de dados local, se tornar a porta de acesso de um vírus por meio de dispositivo móvel inserido para tal atividade, envio de *e-mails* com assuntos classificados, entre outros. A pesquisa revelou que a grande maioria das organizações permite isso aos funcionários.



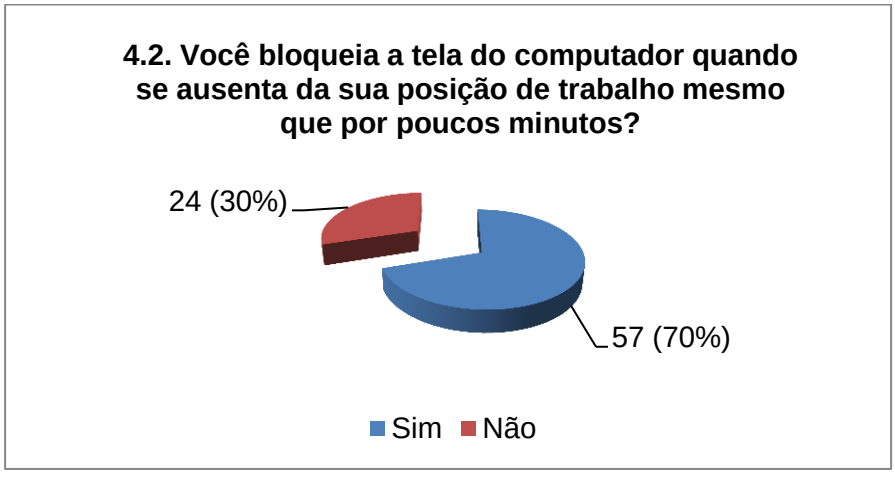
Essa questão se difere da outra porque ela está relacionada à permissão que é concedida aos usuários em suas máquinas locais e também em sua infraestrutura de rede local. A instalação de um programa está ligada ao acesso de um administrador local da estação de trabalho. O resultado é interessante pois revela claramente a preocupação dos administradores das redes de permitir que o usuário final possua menos liberdade de configuração de sua máquina local. Um exemplo de como essa atitude é positiva se dá ao fato de que alguns vírus só infectam a máquina caso o usuário tenha o acesso de administrador para se instalarem, caso não possua esse acesso o computador não é infectado.



Essa questão avalia dois pontos, primeiro o nível de relação que o colaborador tem com a tecnologia e segundo quanto à retirada de informações da organização. A pergunta revelou que as maiorias dos entrevistados sabem e possuem permissão para gravar mídias externas com informações locais. Uma média considerada alta é a dos funcionários que não possuem tal permissão, o que revela que 33% das organizações já compreenderam que é necessário o bloqueio desse tipo de atividade para que a informação não possa mover-se sem autorização prévia ou ainda sem o conhecimento da área de segurança.

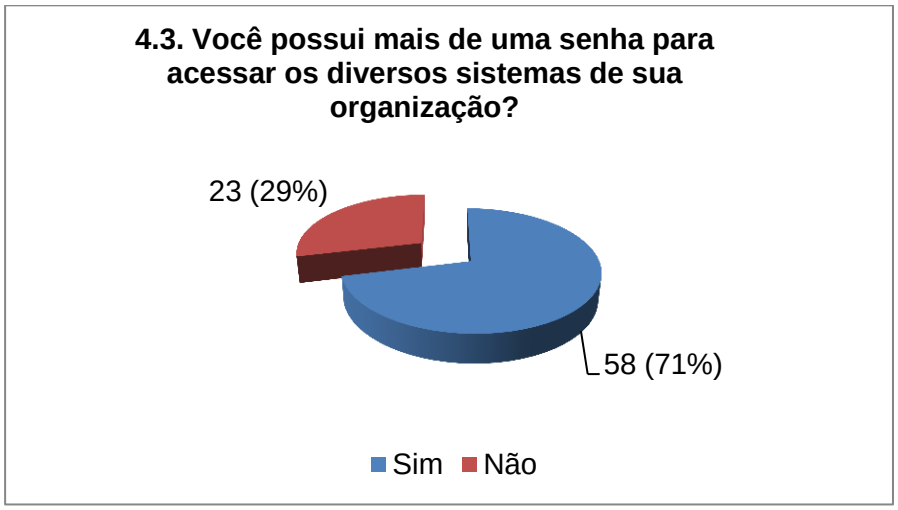


Um novo bloco de perguntas que visa extrapolar a questão mais física da segurança da informação iniciou-se com a pergunta acima. A partir desse momento passo a ser avaliadas questões de proteção informacional. A primeira questionou o acesso seguro aos dados de trabalho da organização e surpreendeu ao demonstrar que ainda 11% das organizações não exigem *login* dos seus colaboradores para identificar quem está manuseando aquelas informações, ou seja, não permite nenhuma auditoria ou controle da estação de trabalho.

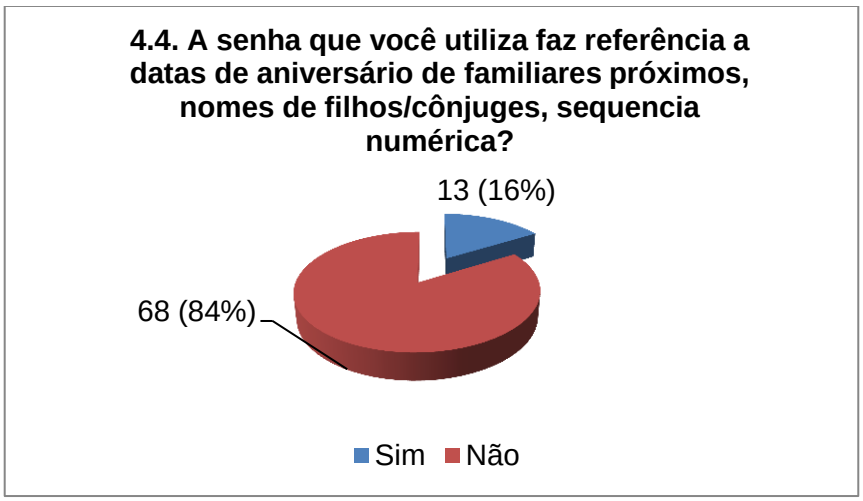


Existe um termo em TI conhecido pelos administradores de rede de dados que é o “carona”. Quando o colaborador se retira da mesa por alguns minutos, por exemplo, para um café, o ambiente informacional de trabalho dele fica inseguro e exposto caso ele não bloqueie a máquina. É nesse momento que o “carona” acessa a máquina desse colaborador e facilmente consegue acesso as informações. O

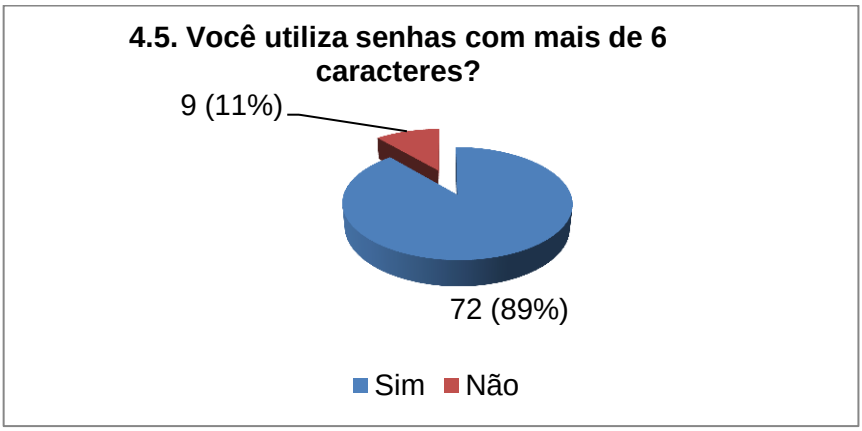
questionamento revelou que 70% dos colaboradores possuem o entendimento de que caso não possam estar presentes a máquina dele deverá ser protegida.



Aqui buscou-se avaliar a complexidade da política adotada pelas organizações. Se os sistemas delas possuem algum tipo de comunicação que bloqueie a mesma senha para mais de um, ou ainda a presença de algum *software* que gerencie as senhas. Constatou-se que a maioria dos entrevistados não faz uso de mais de uma senha. Esse tipo de atitude faz com que a segurança seja menos forte do que a adequada. Isso permite que, a partir do momento que uma senha seja conhecida, os demais programas passam a ser acessados. Isso é um risco que pode ser facilmente evitado com ações preventivas e políticas de segurança adequadas.



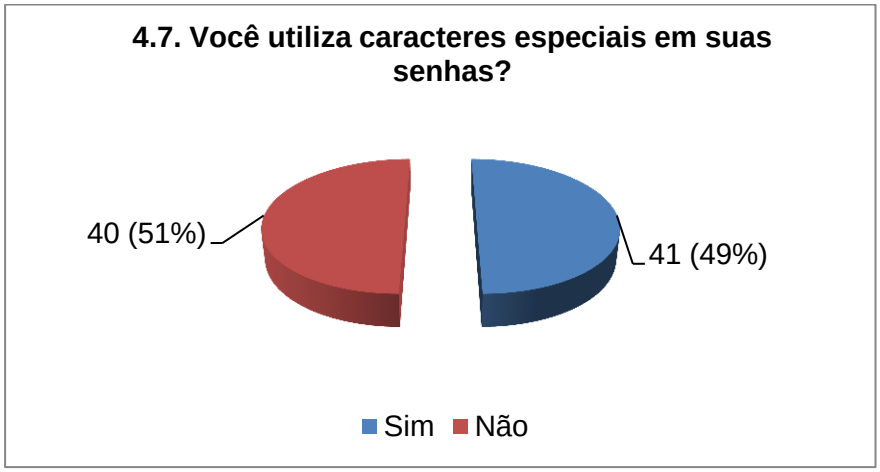
Nesse ponto o questionário passa a avaliar a senha dos colaboradores, visando a identificar se os padrões verificados por tantos anos ainda permanece. Como já visto os colaboradores tendem a utilizar senhas de fácil assimilação, o que torna o processo mais inseguro pois a quebra da senha se torna mais simples. Nessa questão identificou-se que 16% dos colaboradores possuem senhas próximas e já conhecidamente obvias para os seus acessos corporativos.



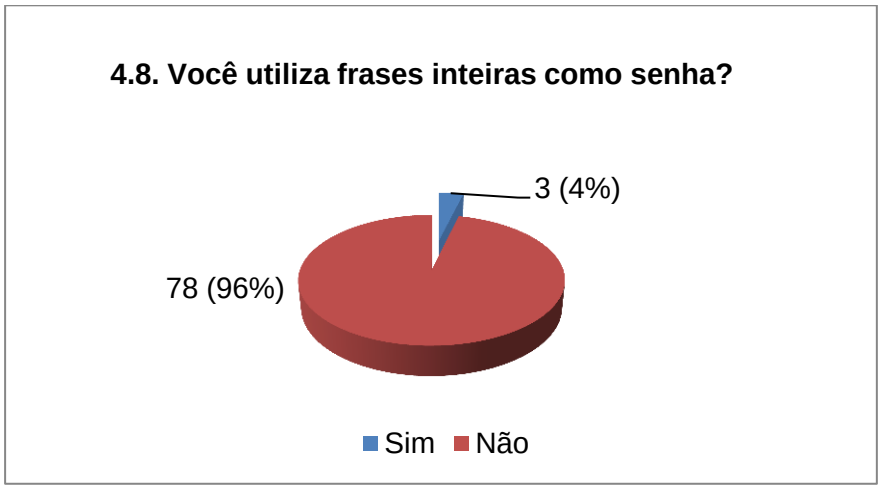
Senhas curtas não são recomendadas, pois as mesmas são mais simples de serem quebradas. Verificou-se que apenas 11% dos funcionários possuem esse tipo de senha fraca. Acredita-se que esse baixo porcentual reflete a fixação de padrões de senhas já implementados em muitas organizações que fornecem uma máscara padrão de senhas que deve ser atendida.

Para as senhas serem consideradas fortes e praticamente impossível de serem quebradas ou conhecidas, elas devem possuir letras maiúsculas e minúsculas e ainda caracteres especiais em sua composição. Buscou-se com essa

questão identificar se os colaboradores já estão considerando senhas fortes no seu dia a dia. Constatou-se que 56% deles já fazem uso do uso de letras maiúsculas nas suas senhas o que figura como um número razoável.

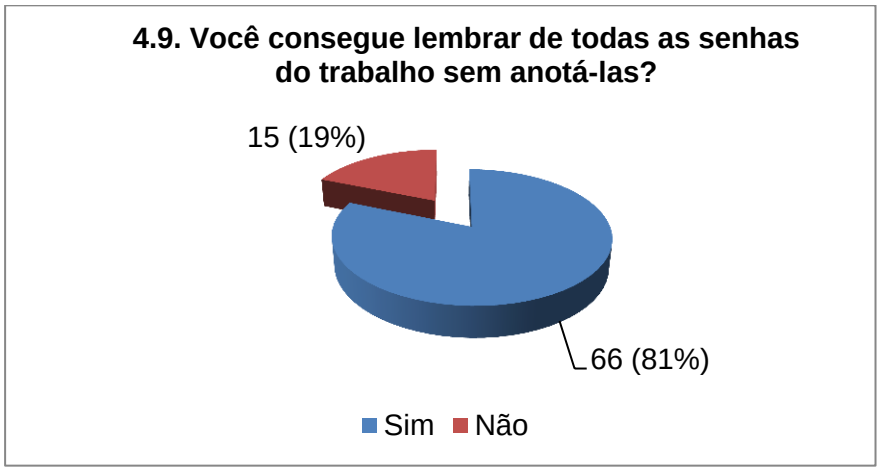


O uso do caractere especial aumenta a dificuldade de quebra da senha exponencialmente e 49% dos usuários já fazem uso deles na composição de suas senhas. Esse resultado foi positivamente surpreendente devido ao fato de se acreditar que o conhecimento de dificuldade que é agregado devido à inserção do caractere especial fosse ainda pouco conhecido dos colaboradores.

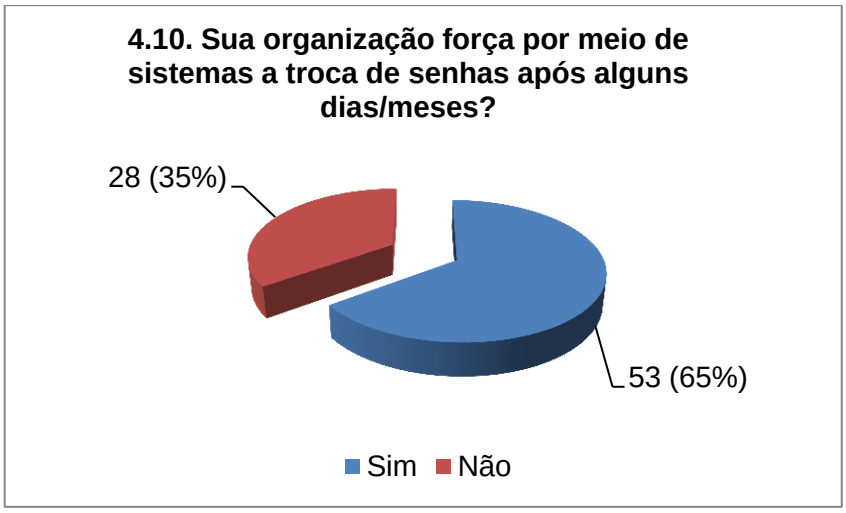


Frases inteiras como senha faz com que elas possam ser quebradas de maneira simplificada. O resultado de que 4% dos entrevistados ainda faça uso desse tipo de grafia para senhas o que surpreendente de maneira negativa por se tratar de uma recomendação básica e primordial em termos de força de senhas e criptografia. Por exemplo, se uma pessoa torce pelo clube atlético mineiro, e esse dado é de

conhecimento publico, uma das opções de senha obvia formato de frase seria: campeãolibertadores2013.

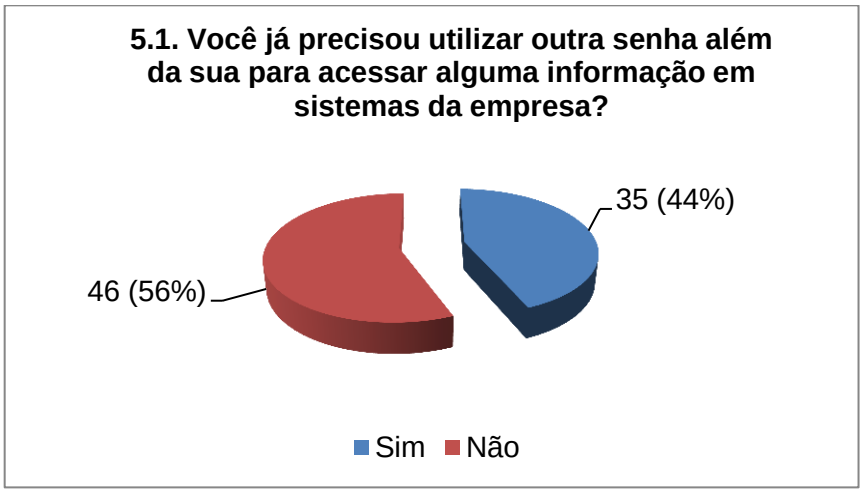


Um ponto pesquisado relacionado a senhas e ao comportamento do usuário relatou que 19% dos colaboradores das organizações pesquisadas necessitam anotar as senhas, pois não conseguem se lembrar de todas. Isso configura-se como um risco informacional já que a anotação pode ser encontrada por alguém mal intencionado que fará o uso negativo e inseguro com aquela informação.

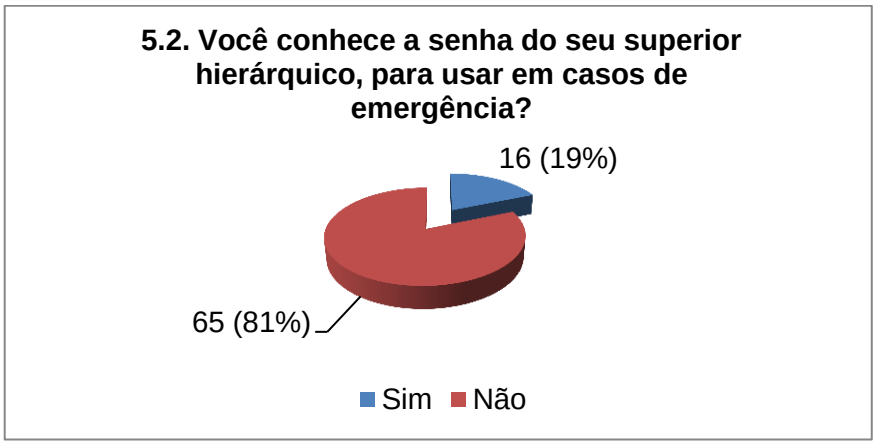


Este item pontuado em outra questão, e é interessante verificar que 65% das organizações possuem políticas de mudanças de senhas, o que força o usuário a realizar mudanças periódicas. Verificou-se aqui portanto que, essas mesmas organizações não possuem a continuação da política fazendo com que essas

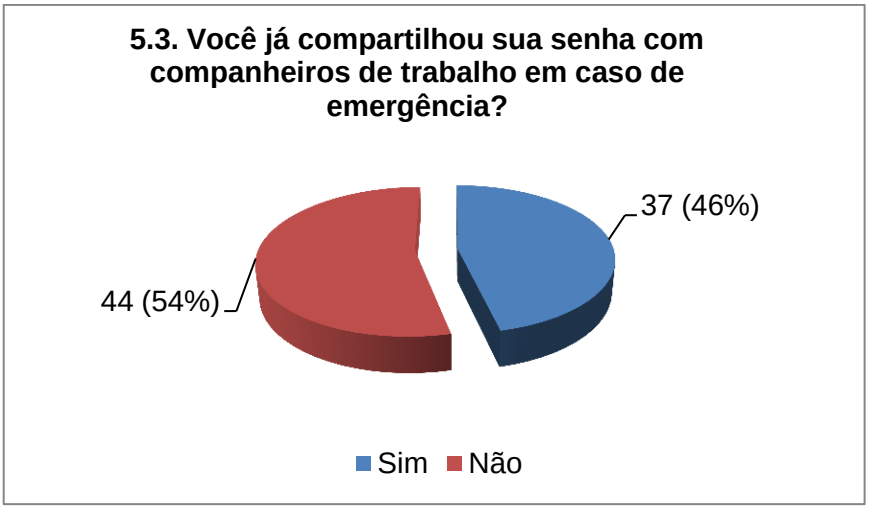
senhas sejam distintas, uma para cada tipo de sistema e ainda que não sejam senhas fracas.



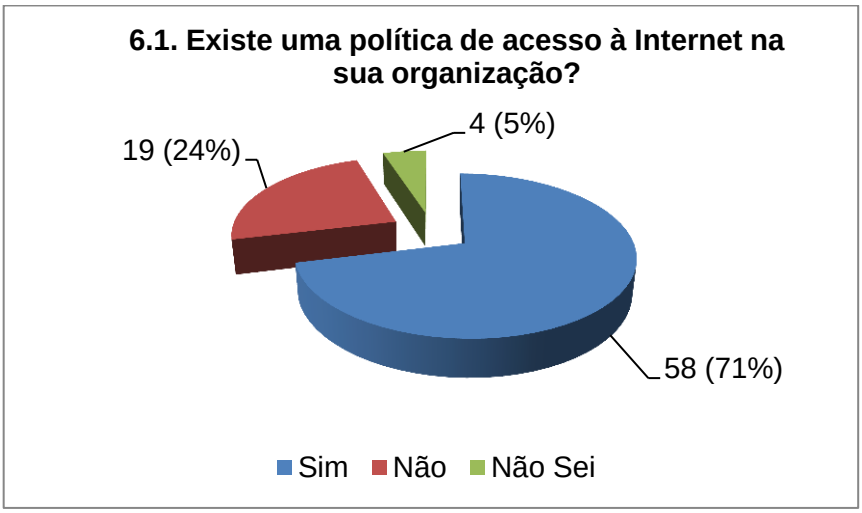
Aprofunda-se mais na questão comportamental quando se questiona em relação à comunicação entre os usuários no quesito compartilhamento de senhas. A senha é secreta, individual e intransferível por definição. No dia a dia das organizações é sabido que existem momentos em que são necessárias outras senhas com níveis de autorizações distintos, por exemplo, para aprovação de algum processo interno realizado feito via sistema, Ex.: os sistemas de SAP e Microsoft CRM necessitam de fluxo de aprovação hierarquizado. Esse tipo de questão faz com que 44% dos entrevistados responda que sim, já necessitaram da senha de outra pessoa nas atividades organizacionais.



A questão acima pontua-se sobre o conhecimento dessa senha de terceiros. Verificou-se que 19% dos colaboradores possuem conhecimento da senha de seu superior hierárquico. Perde-se a característica de confidencialidade e de identificação pessoal do colaborar que não pode garantir mais que é ele mesmo porque a senha não é mais exclusiva.

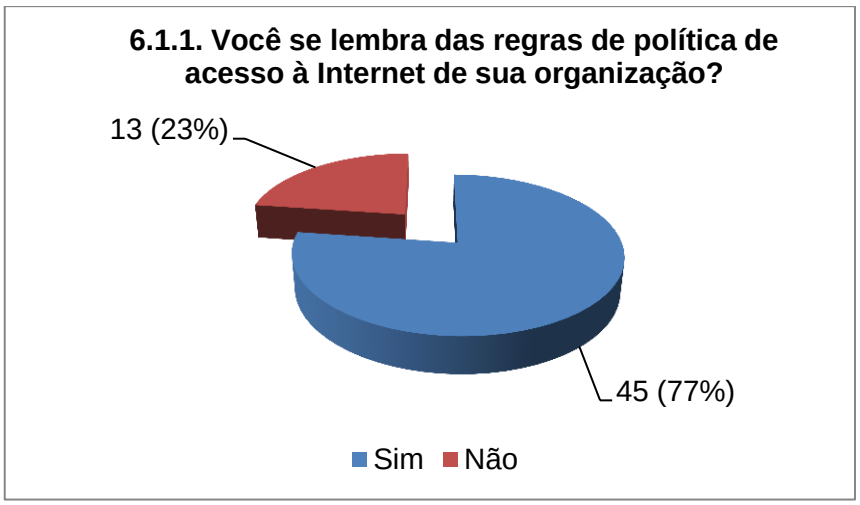


A questão anterior, obteve-se um resultado curioso. Verificou-se que apenas 19% responderam conhecer a senha do superior, já nesta questão, 46% informaram que compartilharam a senha com outro colaborador. Ocorre uma questão mais comportamental/pessoal do que de processos neste caso. Verifica-se que a relação de cumplicidade entre os colaboradores é superior a entre superiores. O compartilhamento de senhas entre os funcionários, mesmo que em uma emergência, não deve ocorrer e o percentual verificado de ocorrência está muito alto. Os colaboradores necessitam ser mais conscientizados dos impactos que podem ocorrer derivados desse tipo de comportamento.

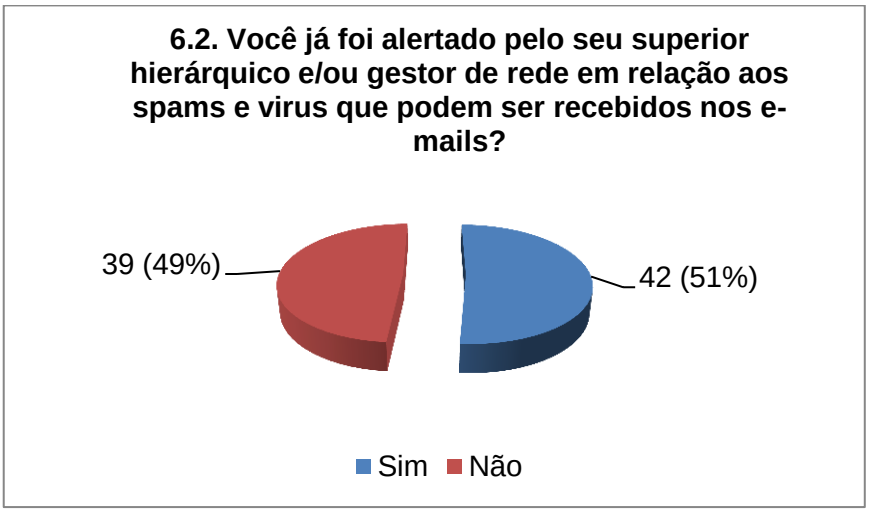


O novo tópico abordado pela pesquisa está relacionado à organização do que ao colaborador em si. Questionou-se sobre a existência de uma política de acesso à Internet nas organizações e verificou-se que 71% delas, segundo os seus funcionários, possuem a política. O desconhecimento referente à político ficou em

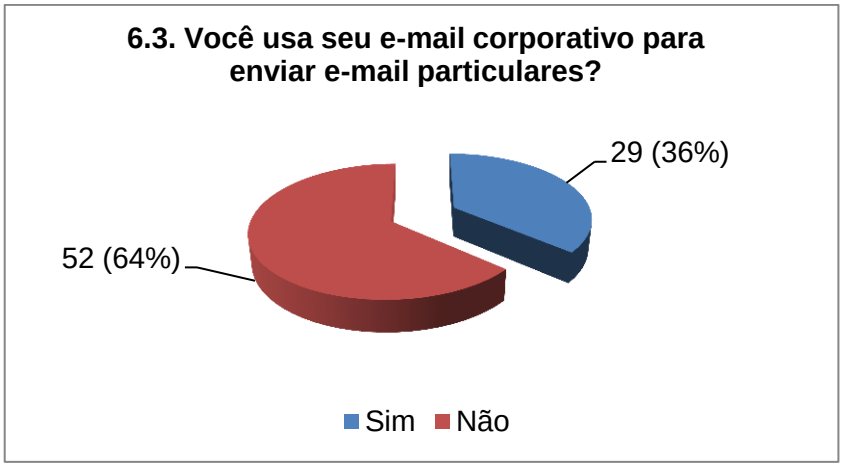
5% que é considerado nessa pesquisa como aceitável. A questão abaixo, 6.1.1, tem sua amostra reduzida de respondentes para 58, visto que ela é o complemento da análise dos respondentes de sim a questão principal, 6.1.



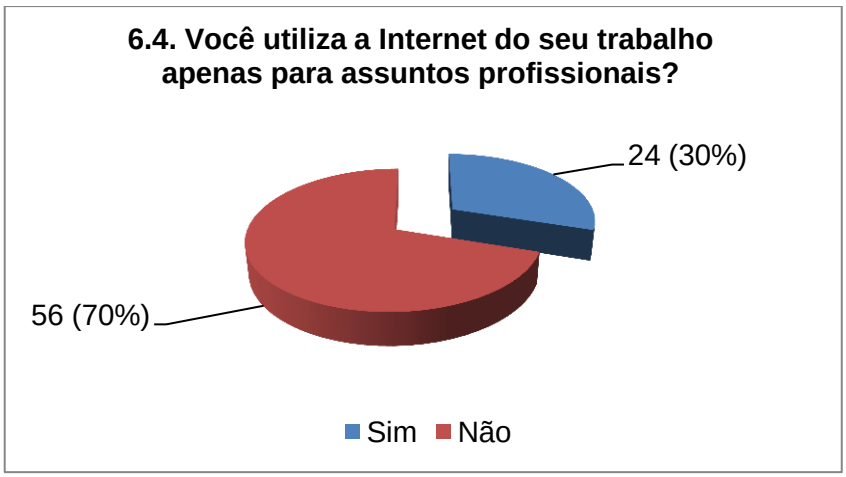
Em relação a política de acesso à Internet, constatou-se que 77% dos colaboradores se lembravam do conteúdo dela.



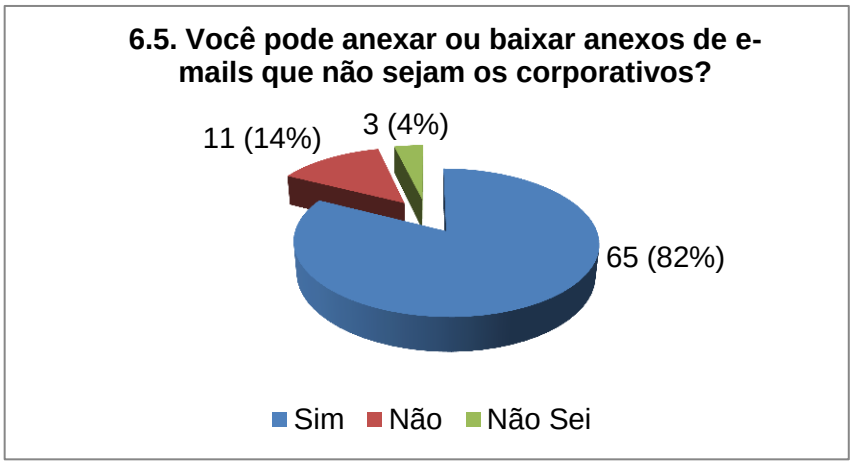
Nessa questão avaliou-se o nível de comunicação e maturidade encontrado dentro das organizações pesquisadas no que tange a capacidade delas de criar políticas e as manter. O questionado é tido como básico e fundamental, trata da questão de recebimento de *e-mails* maliciosos. Verificou-se que 51% dos colaboradores foram orientados em relação a esse tipo de dano.



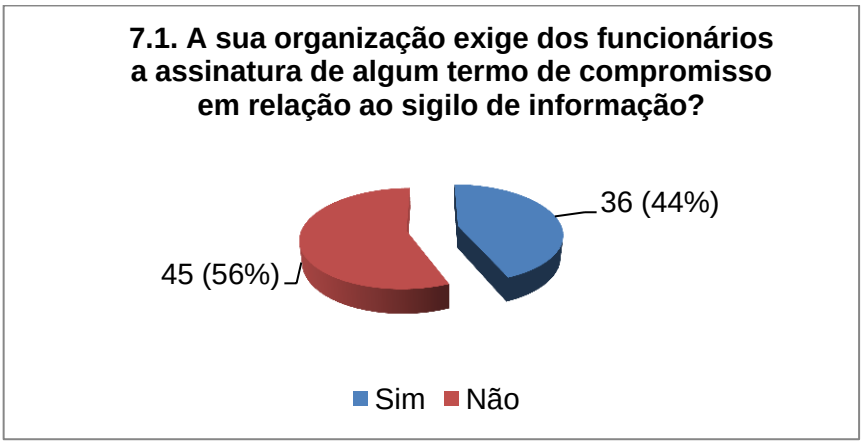
Em relação ao uso dos recursos da organização pelo colaborador no tange ao entendimento do comportamento adequado e seguro foi questionado se o *e-mails* corporativo era utilizado para fins particulares. Dos colaboradores pesquisados, 36% responderam que sim. Esse dado é preocupante, pois o *e-mail* da organização deve ser utilizado para fins profissionais apenas. Um dos problemas que poderiam ser causados em relação a isso seria o envio de *e-mail* para destinatário incorreto, o que faria com que a informação recebesse um desvio de comportamento adequado e fosse enviada para ambiente sem controle com resultados negativos. A existência de políticas de Internet anteriormente pesquisadas torna esse dado curioso já que o colaborador poderia fazer uso de seu *e-mail* particular de acordo com o definido na política. Esse item se torna cultural e deve ser verificado para que esse percentual seja reduzido por meio de treinamentos ao usuário final.



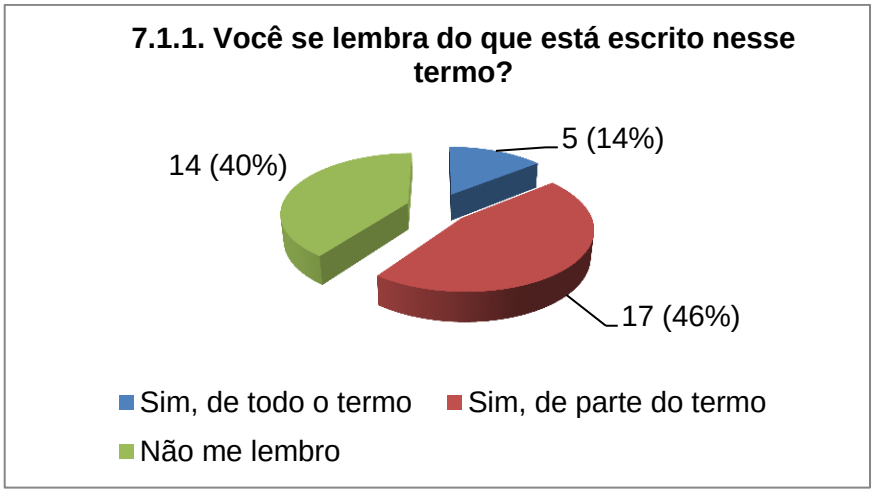
Essa questão está de acordo com o esperado já que em relação ao uso da Internet os colaboradores pesquisados estão bem orientados.



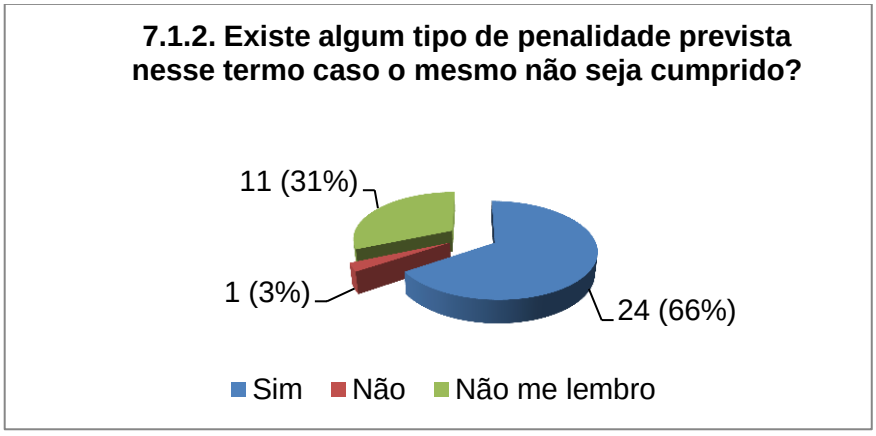
Os entrevistados que figuram dentro dos 82% afirmam que podem retirar ou inserir informações de fontes não controladas, como e-mail particular, para dentro da organização sem auxílio ou bloqueio inicial. Faz-se aqui um ponto de atenção, porque caso a organização não possua equipamento de rede específico para identificar esse tipo de ação, a organização está bastante exposta, o que significa que o processo e a política de segurança da informação devem ser revistos.



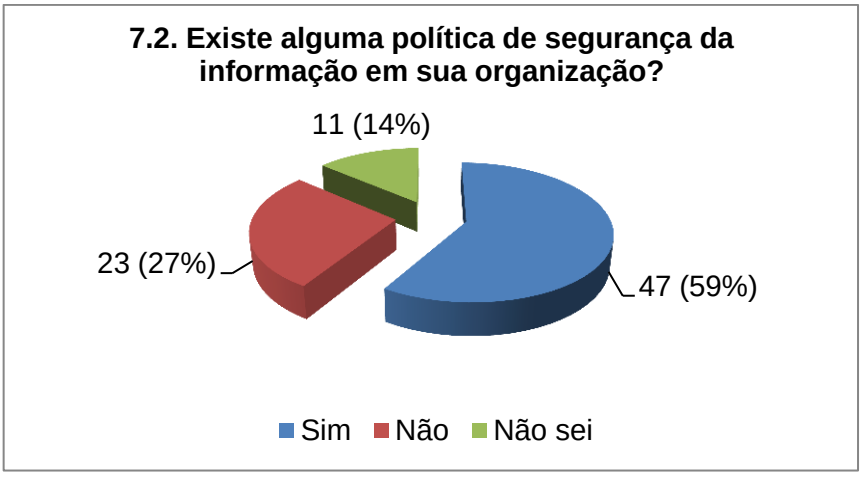
Em termos de proteção intelectual da organização, muitas possuem um termo de sigilo informacional. A pesquisa revelou que apenas 44% das organizações realizam tal procedimento. Essa ação não tem base legal no Brasil ainda, portanto essa prática necessita ser revista de acordo com a lei brasileira. Essa pesquisa não pretende se aprofundar nas questões legais, mas como elas figuram como características da informação e conseqüentemente de suas segurança vale ser pontuada. As questões que se seguem, 7.1.1 e 7.1.2 são desdobramentos da questão principal, 7.1 e os respondentes destas são os que disseram assinar um termo de compromisso.



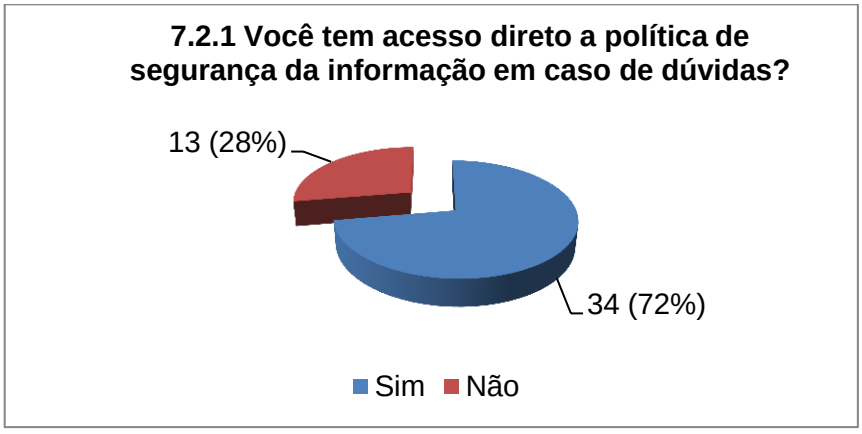
Em relação ao termo de responsabilidade, dos que o assinaram, 40% não se lembram do seu conteúdo e outros 46% lembram de apenas parte dele. Como dito anteriormente, a legislação brasileira não é clara, então o que se verifica é que não se encontra um padrão no mercado. As normas de segurança também não explicitam nenhuma informação detalhada ou mesmo modelo dessas cartas, portanto esse é um ponto que necessita de maior amadurecimento em toda cadeia do processo.



Muitos desses termos possuem ameaças aos colaboradores com penas que deverão ser pagas em caso de não cumprimento do sigilo informacional. Como eles não possuem base legal válida acabam se perdendo e resultando nas respostas da questão anterior.

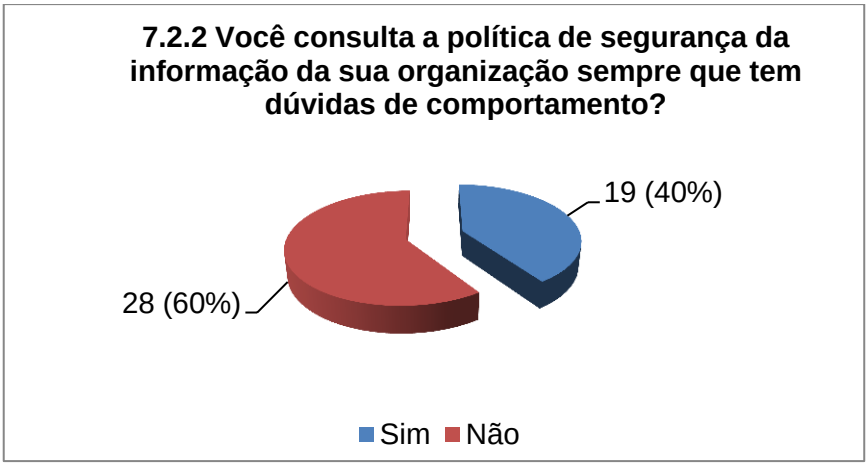


Políticas de segurança da informação ainda são pouco claras e pouco difundidas na maioria das organizações como estudado anteriormente. De qualquer maneira,elas existem, surpreendentemente, em 59% das organizações dos entrevistados. Uma confirmação de que o afirmado é verdadeiro o desconhecimento da política por 14% dos colaboradores. As questões que se seguem, 7.2.1 e 7.1.2 são complementares a questão principal, 7.2 e o total de respondentes são os que disseram sim para essa pergunta.

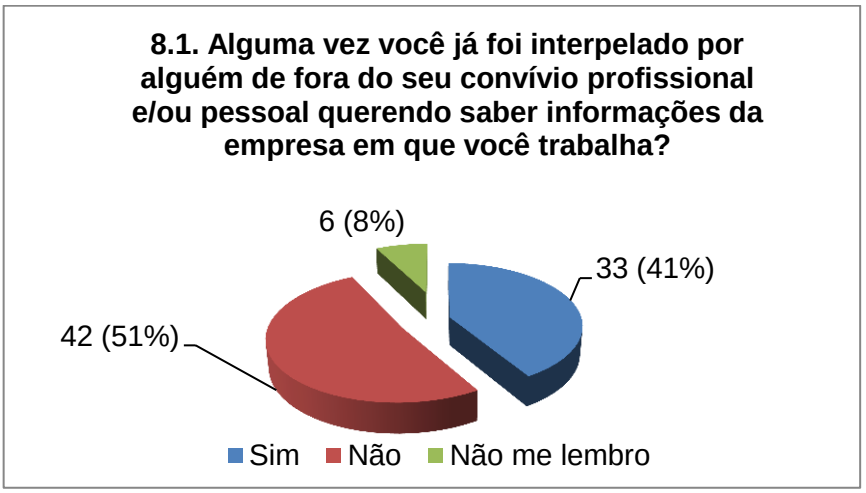


Geralmente quando a política de segurança da informação existe na organização, ela fica disponível em algum espaço de acesso dos colaboradores, como uma intranet, ou impressa no departamento pessoal, ou de segurança da informação entre outros. Dos que possuem a política dentro da organização relataram que a grande maioria, 72%, possui acesso a política para retirada de dúvidas,enquanto 28% não possuem. A política de segurança da informação deveria estar disponibilizada sempre que o funcionário possuísse alguma dúvida em relação

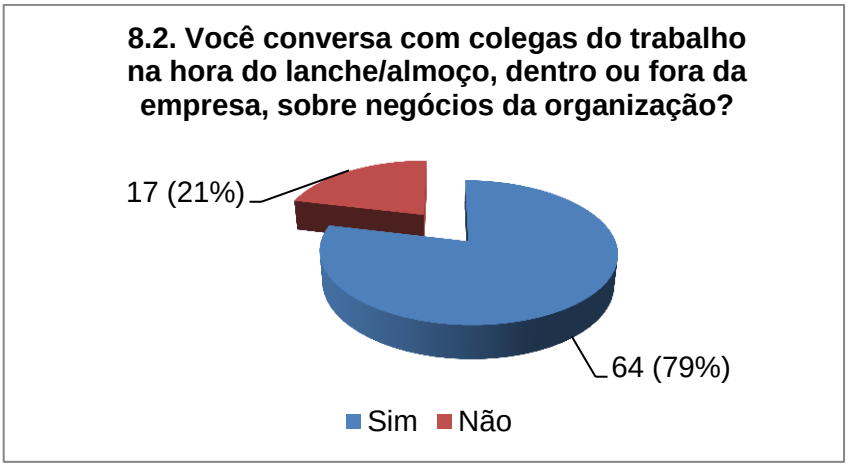
a qual postura tomar. O índice de indisponibilidade é alto, há necessidade de reduzi-lo.



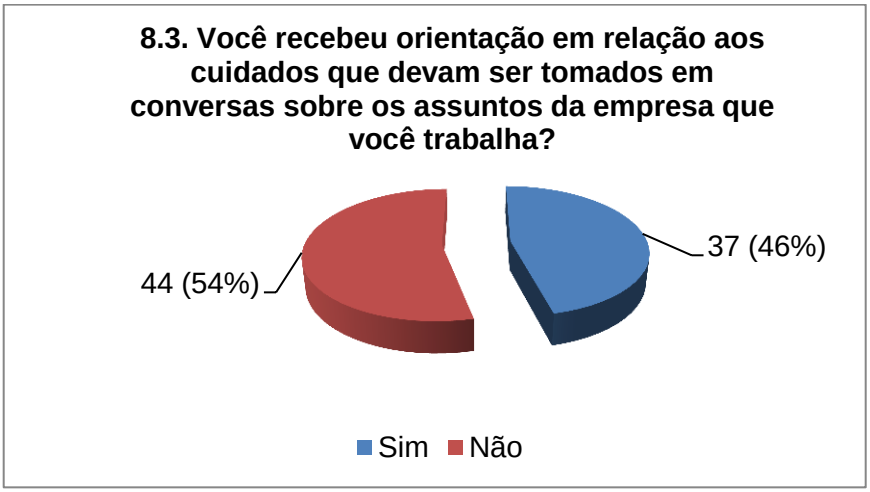
Dos colaboradores que possuem acesso à política, 40% a acessam em caso de dúvidas. O que explicita a necessidade de treinamento e incentivo ao acesso da política.



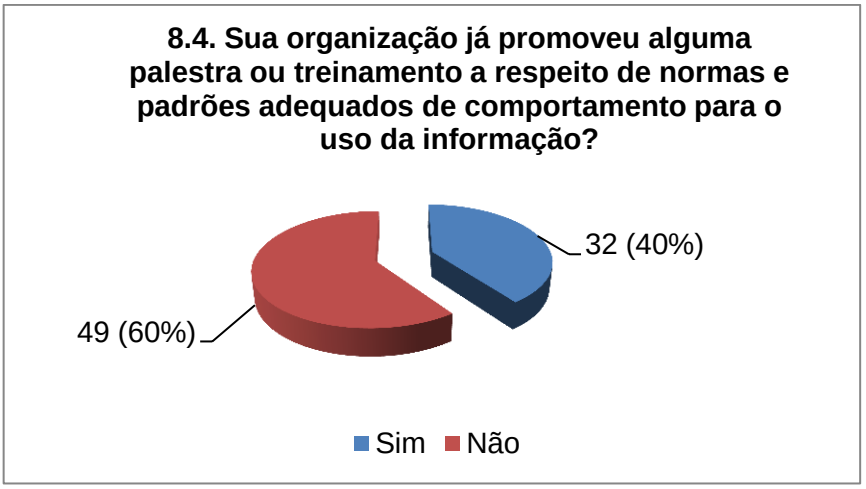
O questionário nesse ponto passa a investigar a questão de inteligência competitiva e de comportamento pessoal informacional inseguro. Nesta questão, 41% dos entrevistados relatam que já foram interpelados por alguém de fora da organização, que buscava informações da dessa. Esse número é bem alto, o que figura como ponto de atenção para que os funcionários recebam treinamentos adequados com esclarecimentos em relação a inteligência competitiva e ao valor e proteção da informação.



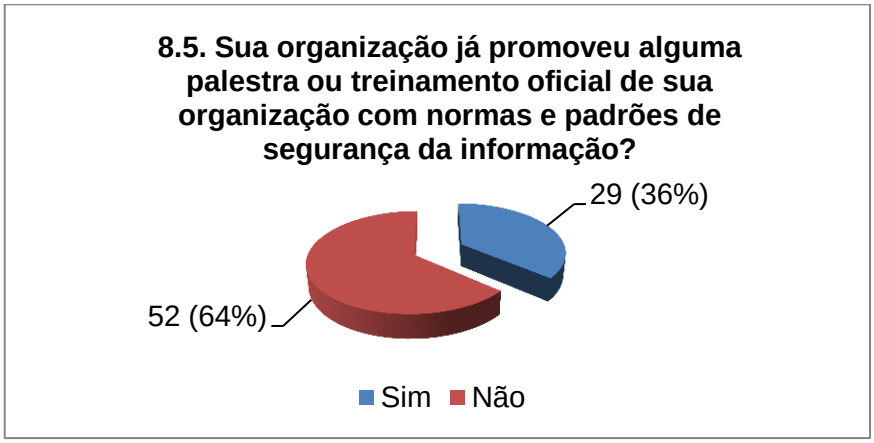
Para esse tipo de conversa, mesmo as mais informais, os colaboradores deveriam ser informados sobre o risco de falar, por exemplo, sobre nome de clientes e projetos, demissões, movimento de mercado entre outros assuntos pertinentes à organização. Muitas vezes a inteligência competitiva pode ter contrato com pessoas que ficam nesses locais, próximos a organização objeto de estudo, para apenas ouvir o que os colaboradores compartilham. Como a maioria dos entrevistados, 79%, disseram que conversam sobre trabalho dentro e fora das organizações com colegas esse é um ponto de atenção para orientação a um comportamento seguro.



O ponto de atenção da questão anterior se revela verdadeiro com a questão acima, informando que apenas 46% dos colaboradores receberam orientações sobre o cuidado que se deve tomar em conversas relativas ao trabalho.

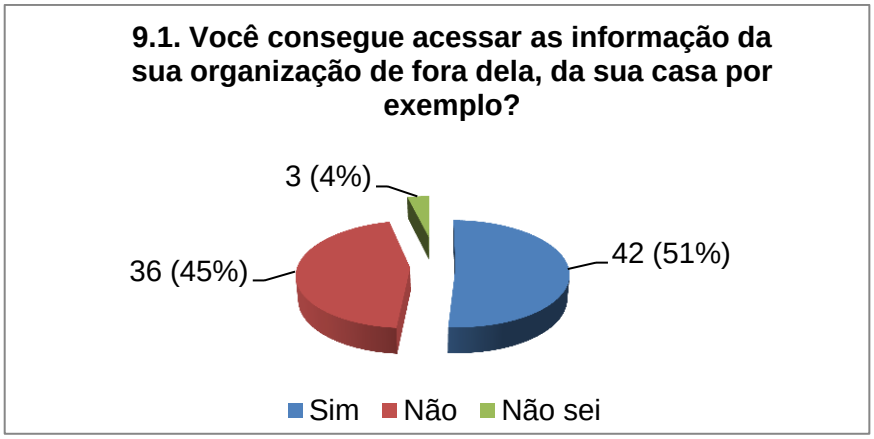


Mais especificamente sobre temas de informação e treinamento de segurança e comportamento informacional seguro, essa questão aborda a promoção de treinamentos voltados aos padrões e normas de comportamento para o uso da informação. Dos entrevistados, 40% afirmam que já receberam treinamentos nessa área promovidos pelas organizações ao qual trabalham. Entende-se que esse dado possa ter recebido um retorno de 40% de afirmações devido a certificação ISO 27000 que muitas empresas buscaram em meados dos anos 2000 em função de padronizações que o próprio mercado exigiu. Faz-se necessária uma investigação mais profunda sobre o tipo de treinamento e/ou palestras que foram oferecidos aos colaboradores para uma visão mais ampla da questão de divulgação da informação.

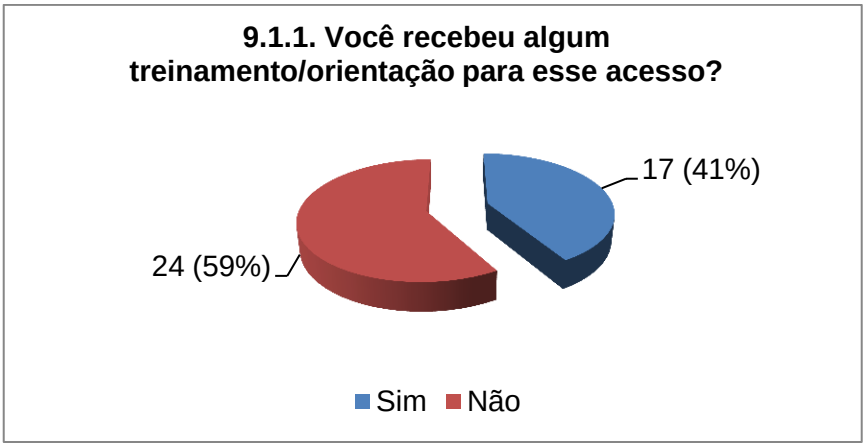


Essa questão, diferentemente da anterior que foca o comportamento do usuário, visa retorno referente aos padrões e normas de segurança da informação amplamente abordado nesse estudo. A mesma análise da questão anterior vale como reflexão nesta. Ressaltando que, esta por se tratar das normas e padrões necessita necessariamente vir de uma diretriz da organização de forma clara e definida. Já do ponto de vista comportamental, pode ter sido considerados

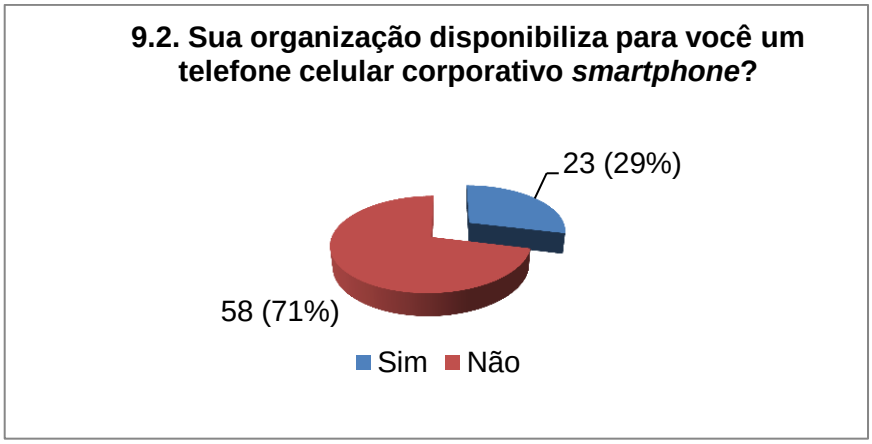
treinamentos de outras áreas da organização visando o comportamento e não necessariamente a área de segurança da informação.



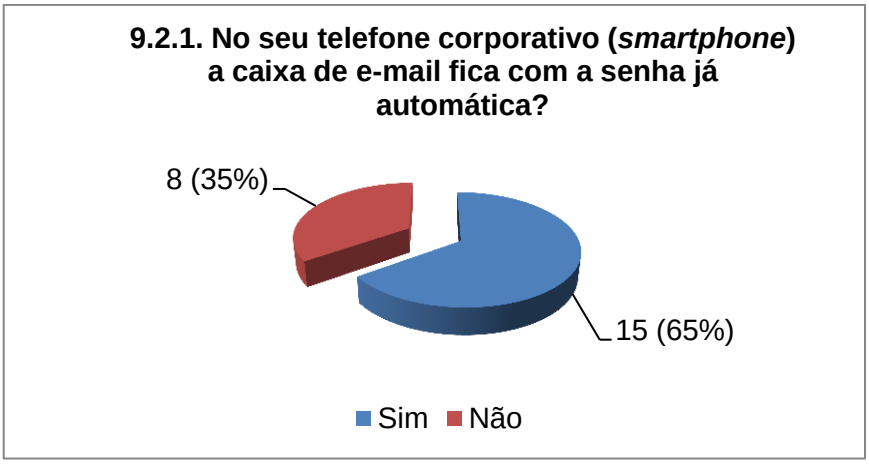
A mobilidade está a cada dia mais em expansão na sociedade. Dentro das organizações, as urgências e negócios surgem a todo o momento. Com o acesso a organização não precisando mais ser apenas no local sede da empresa, passa-se a controlar um ambiente muito maior e garantir segurança para um ambiente móvel dessa dimensão é um grande desafio da área de segurança da informação atualmente. Essa questão visa identificar qual porcentagem dos entrevistados consegue acesso aos dados da organização de maneira remota. O resultado foi que 51% deles podem acessar os dados remotamente. Cruzando com o dado dos que acessam via *notebook*, temos um total de 27 entrevistados contra 42 nessa questão, os outros 14 acessam os dados via outros dispositivos móveis, como *tablets* por exemplo, ou mesmo o *desktop* da residência, mas o meio é a Internet. Essa administração e controle pode ser extremamente complexa para gerenciar. Mais uma vez o treinamento do usuário faz toda a diferença. A questão abaixo, 9.1.1 complementa a questão 9.1 e portanto tem sua amostra reduzida visto que ela compreende apenas os colaboradores que responderam possuir acesso às informações do trabalho fora dele conforme viu-se.



O complemento da questão anterior é que apenas 41% desses colaboradores que tem acesso aos dados da organização fora do ambiente de trabalho receberam treinamento para tal.

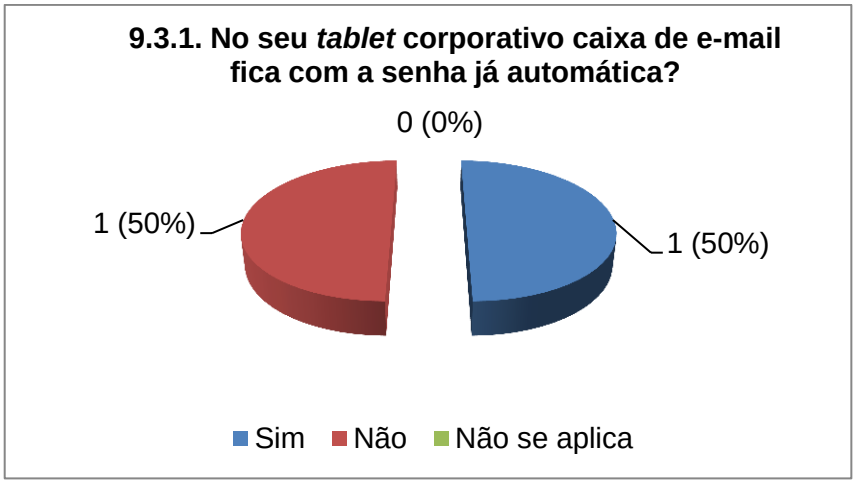


Continuando a investigação sobre mobilidade e treinamentos, questionou-se se os colaboradores entrevistados recebiam da organização um *smartphone* para o trabalho, 29% deles disseram que sim. As organizações estão buscando deixar cada vez mais os seus colaboradores estratégicos mais conectados, promovendo acesso a *e-mails* e sistemas internos móvel, mas o treinamento deles ainda está falho. A quantidade de perda informacional não pode ser calculada, mas o risco pode ser reduzido. A questão 9.2.1 possui sua amostra reduzido devido ao fato da mesma compreender como um complemento da questão 9.2 referente ao *smartphone* corporativo.

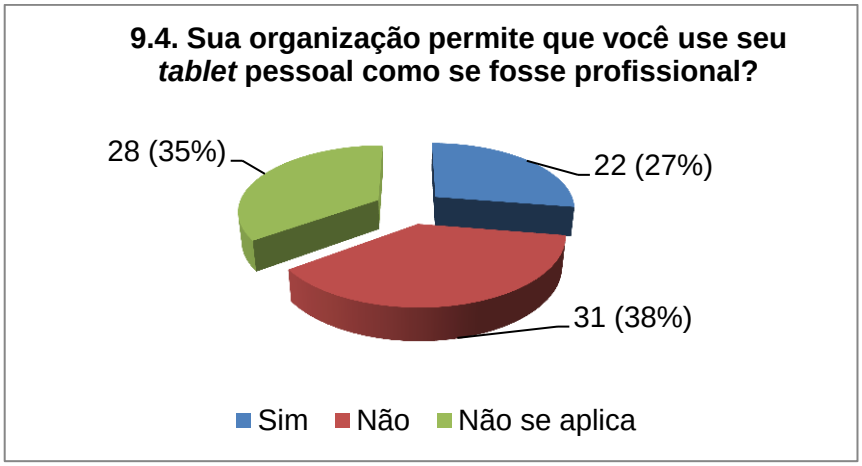


Verifica-se que da questão anterior 65% dos entrevistados afirmam que deixam a senha automaticamente salva em seus *smartphones*. Esse tipo de atitude é insegura. Já verificamos que em caso de perda de dispositivo o colaborador em sua maioria não sabe o que fazer. Perder um telefone que possui a caixa de *e-mail* com acesso permitido ao possuidor do aparelho é uma falha de segurança da informação.

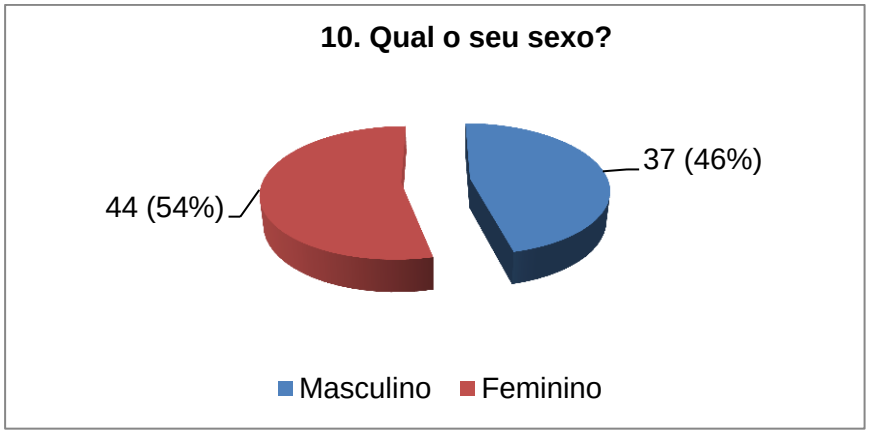
Nessa questão identificou-se que os *tablets* ainda não estão sendo muito utilizados como dispositivo corporativo móvel pelas organizações que ainda preferem o *smartphone*. A questão abaixo possui a amostra reduzida por refere-se apenas aos respondentes de sim dessa questão.



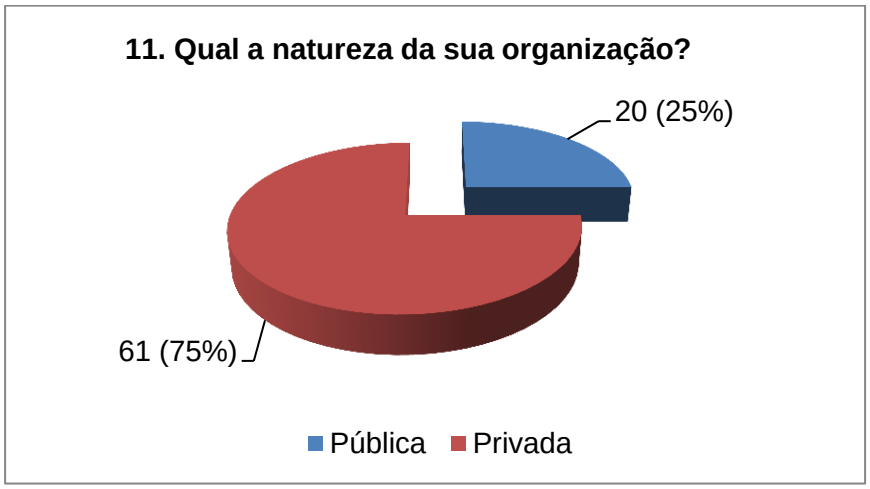
Mesmo conceito aplicado sobre a questão de senha no *smartphone*.



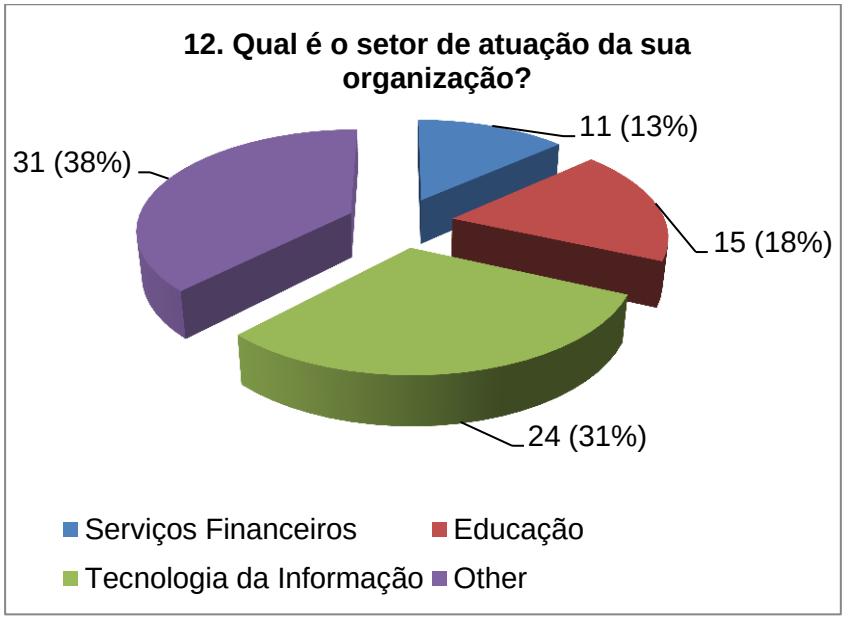
Com o advento do termo *bring your own device* (BYOD) as organizações mais fortemente desde 2010, vem incentivando os seus colaboradores das áreas mais estratégicas a possuírem seu próprio dispositivo móvel integrado aos sistemas da organização. Verificou-se com esse questionamento que ainda que esse movimento de BYOD ainda é pouco aceitado no mercado brasileiro já que a maioria das organizações não permite.



A maioria de entrevistados foi do sexo feminino, 54%.



Dos entrevistados 75% trabalham no mercado privado.



Os setores foco do estudo que eram serviços financeiros, educação e tecnologia da informação representaram um total de 62% dos entrevistados. As outras áreas que somaram 38% foram: indústria, biotecnologia, transporte, jurídica, engenharia e cultura.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa objetivou traçar o perfil dos usuários e das organizações na qual eles trabalham, abordando questões sobre o conhecimento de segurança da informação, comportamentos informacionais pessoais, processos de segurança da informação, política de segurança da informação e entendimento do valor da informação nas organizações.

Verificou-se que as organizações possuem um nível aquém do entendimento desejado do valor da informação frente a números baixos de entrevistados que relataram terem recebido algum tipo de treinamento em segurança da informação. As preocupações das organizações quanto a questões de segurança física também apresentaram nível insatisfatório. Questões como o acesso ao local de trabalho, que são nocivas ao negócio, não possuem a atenção devida. Ainda, sobre a questão da segurança física ressalta-se que existem políticas presentes em relação ao descarte de materiais físicos, como *e-mails* impressos, memorando e demais documentações corriqueiras.

Nas questões de segurança lógica encontra-se ainda alguma confusão em fundamentos de segurança da informação, visto que as organizações permitem que a grande maioria dos usuários possa retirar ou inserir informações dentro da organização sem bloqueio ou autorização prévia. Essa questão é preocupante pois vem de encontro à chave do estudo apresentado, que são as pessoas. Sem políticas de acessos como esta, a segurança da informação acaba fixando-se sobre apenas um dos três pilares, a pessoa. Portanto, a organização fica dependente da boa índole do colaborador em não fazer uso das informações que podem ser por ele retiradas. Mesmo com a existência de um termo de confidencialidade em muitas das organizações pesquisadas este não impede, ou mesmo tem valor legal, caso o usuário não receba bloqueios tecnológicos para a retirada de informação sem autorização. Esse tipo de situação figura como um risco alto.

No que tange às políticas implementadas pelas organizações, verificou-se que até existem políticas, mas os usuários pouco lembram-se delas, portanto recomenda-se que sejam realizados mais treinamentos a fim se promover melhor orientação dos usuários, de forma a contribuir para uma diminuição do risco informacional e maior sucesso da política aplicada.

Os resultados do estudo evidenciam que as senhas adotadas pelos entrevistados são mais condizentes com bons padrões de segurança do que se poderia esperar. De fato, muitos deles, 50%, fazem uso de senhas fortes. O ponto de atenção mais uma vez recai sobre o fato de que os colaboradores tendem a escrever as senhas em locais diversos para não se esquecer delas. Por mais que as organizações se esforcem, em criar políticas de mudança de senhas, como foi verificado na pesquisa, os usuários continuam anotando-as e ainda compartilhando-as com terceiros em caso de emergência. Novamente verifica-se a necessidade de treinamento para os colaboradores em segurança da informação, com o foco voltado para o entendimento dos fundamentos da segurança informacional que diz que a senha é pessoal e intransferível.

A pesquisa revelou ainda a questão dos engenheiros sociais, pessoas da área de inteligência competitiva, que interpelam os colaboradores em locais comuns é realidade no Brasil. Mesmo com esse assunto de inteligência competitiva gerando ainda muita discussão entre espionagem e atos legais podemos afirmar que as organizações entenderam o valor da informação e estão começando a executar ações para fora delas mesmas, buscando novas oportunidades e investindo acreditando no treinamento inadequado dos colaboradores das organizações objeto de análise.

Após a análise das informações e estudo da bibliografia disponível recomenda-se que o foco da segurança da informação dentro das organizações seja dado pelo par de resoluções proposto, pessoas e processos.

As pessoas devem ser treinadas com períodos pré-definidos de espaçamento entre eles para que haja fixação e manutenção das políticas. O foco dentro das pessoas deve ser dado às questões comportamentais. Uma sugestão interessante seria a apresentação de jograis com exemplos de situações em que o comportamento informacional foi adequado e também inadequado. Dessa maneira a má fixação verificada em um problema, poderia ser reduzida. Treinamentos técnicos também são um ponto de falha verificado na pesquisa nos casos em que a tecnologia está disponível, mas o usuário não foi treinado para utilizá-la de maneira segura.

A necessidade de políticas aderentes ficou explicitada. As políticas existentes e em operação demonstraram-se falhas, visto que a maioria dos colaboradores ou a desconhecem ou não se lembram delas. Elas necessitam ser

aderentes ao negócio do cliente e dentro do padrão das normas internacionais de segurança. É necessária a clara presença de um instrumento de segurança da informação que possua recomendações, regras, responsabilidade e ações que devem ser executadas rumo a segurança da informação.

O estudo conclui que tanto colaboradores quanto organizações estão crescendo no entendimento da segurança da informação, mas ressalta que ainda existe um longo caminho a ser seguido e o segredo deles está nas pessoas e no comportamento delas.

Acredita-se que o resultado apresentado neste trabalho poderá ser utilizado como insumo para que sejam aprofundadas as questões em cada um dos 12 temas propostos relacionados aos tipos e níveis de segurança pesquisados buscando assim o detalhamento do cenário atual de segurança da informação.

REFERÊNCIAS

ABNT - Associação Brasileira de Normas Técnicas. Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão da segurança da informação. Disponível em: <http://pt.scribd.com/doc/2449992/Abnt-Nbr-Isoiec-17799-Tecnologia-da-Informacao-tecnicas-de-Seguranca-Codigo-de-Pratica-para-a-Gestao-da-Seguranca-da-Informacao>. Acesso em: 18 fevereiro 2012.

BARCLAY, Rebecca O.; MURRAY, Philip C. *What is knowledge management*. Em: *Knowledge* Praxis. Disponível em <http://www.providersedge.com/docs/km_articles/what_is_knowledge_management.pdf>. Acesso em 20ago. 2013.

BARROSO,Antônio Carlos de Oliveira; GOMES, Elisabeth Braz Pereira. Tentando entender a gestão do conhecimento. RAP - Revista de Administração Pública, Rio de Janeiro, v. 33, n. 2, mar./abr. 1999. Disponível em: <http://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/7656/6201>. Acesso em 25 abr. 2012.

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

BATEMAN & SNEAL. Administração *management:* construindo vantagem competitiva. São Paulo: Editora Atlas. 1998.

BELLETTINI, C.; BERTINO, E.; FERRARI, E*. Role based access control models. Information Security Technical Report*, v. 6, n. 2, p. 21–29, June 2001.

CARVALHO, Rodrigo Baroni de; FERREIRA, Marta Araújo Tavares.Acelerando a Espiral do Conhecimento com a Tecnologia da Informação. Disponível em <http://comlurbnet.rio.rj.gov.br/extranet/sysbibli/arquivos/dig224.pdf>. Acesso em 20 fev. 2012.

COOK, Michelle; COOK Curtis. Competitive Intelligence: create an intelligent organization and compete to win. London: Kogan Page, 2000.

Davenport, Thomas H; Prusak, Laurence: Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual. 16° Ed. Rio de Janeiro: Campus, 2008.

DRUCKER, P. The age of social transformation.The Atlantic Monthly Company, 1994.

FAYOL, H. Administração industrial e geral. São Paulo: Atlas, 1994. 138 p.

FIUZA, Gustavo de Abreu. A percepção dos analistas de TI do Banco do Brasil quanto à importância da transformação do conhecimento tácito em conhecimento explícito. 2011. p.34. Monografia (Graduação em Administração à distância) - Faculdade de Economia, Administração e Contabilidade, Universidade de Brasília, Brasília.

FONTES, Edson. Segurança da Informação: o usuário faz a diferença. 1° Ed. São Paulo. Saraiva, 2006.

FLEURY, Afonso; FLEURY, Maria Tereza Leme (Org.); OLIVEIRA JR., Moacir de Miranda (Org.). Gestão estratégica do conhecimento: Integrando Aprendizagem, Conhecimento e Competências. 1. Ed. São Paulo: Atlas, 2001. p. 352.

FREITAS. Henrique M. R.; KLADIS, Constantin Metaxa. Da Informação à política informacional das organizações: um quadro conceitual. São Paulo: RAP, v.29, n. 03, Jun./Set. 1995.

HANDY, Charles. *Gods of Management: The Changing Work of Organizations*. . 4° Ed. Inglaterra: Oxford University Press. 1995.

JONES, Andrew; MARTIN, Thomas. Making Information Security Acceptable to the User. School of Computer and Information Science, Security Research Centre, Edith Cowan University, Perth, Western Australia. Disponível em: < http://ro.ecu.edu.au/icr/6/ >. Acesso em: 19 fev. 2012.

LAUREANO, Marcos Aurelio Pchek. Gestão de Segurança da Informação - 2005. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 15 fev. 2012.

LIMA, M. C. A Engenharia da Produção Acadêmica. São Paulo: Unidas, 1997.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel.Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação - 2005. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752005000200002&lng=en&nrm=iso>. Acesso em: 4fev. 2012.

MORESI, Eduardo Amadeu Dutra. Inteligência organizacional: um referencial integrado. Ciência da Informação, Brasília, v. 30, n. 2, maio/ago. 2001. Disponível em: <http://revista.ibict.br/ciinf/index.php/ciinf/article/view/192/169>. Acesso em: 12 abr. 2012.

MORESI, Eduardo Amadeu Dutra. Monitoramento ambiental. In: TARAPANOFF, Kira (Org.). Inteligência organizacional e competitiva. Brasília: Editora Universidade de Brasília, 2001.

NETTO, Abner da Silva; SILVEIRA, Marco Antônio Pinheiro da. Gestão da segurança da informação: Fatores que influenciam sua adoção em pequenas e médias empresas. Revista de Gestão da Tecnologia e Sistemas de Informação, São Caetano do Sul, v. 4, n.3, out/nov. 2007. Disponível em: <http://www.scielo.br/pdf/jistm/v4n3/07.pdf>. Acessoem 25 Abr. 2012.

NONAKA, I. & TAKEUCHI, H. Criação do conhecimento na empresa. Rio de Janeiro: Campus, 1997.

PURSER, Steve. A Practical Guide to Managing Information Security. Boston: Artech House, 2004. p. 280.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva - Rio de Janeiro: Campus, 2003.

STAREC et. al. Gestão estratégica da Informação e Inteligência Competitiva. São Paulo: Saraiva. 2006.

STONER, James A. F.; FREEMAN, R. Edward. Administração. 5º ed. Rio de Janeiro: Prentice Hall do Brasil, 1992. 533 p.

TAYLOR, Frederick Winslow. Princípios de Administração Científica. 7° Ed. São Paulo: Atlas, 1970.

VERGARA, Sylvia Constant. Projetos e relatórios de pesquisa em administração. 3. Ed. São Paulo: Atlas, 2000.

WADLOW, Thomas. Segurança de Redes - Projeto e Gerenciamento de Redes Seguras. Editora Campus. Rio de Janeiro,
2000.

WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security. Course Technology: Boston, MA, EUA. 2011.

WHITMAN, Michael E.; MATTORD, Herbert J. Principles of Information Security.4.Ed. Boston: Cengage Learning, 2011. p.656.

ZAPATER, Marcio; SUZUKI, Rodrigo. Segurança da Informação: Um diferencial determinante na competitividade das corporações. Disponível em <http://www.promon.com.br/portugues/noticias/download/Seguranca_4Web.pdf>.Acesso em 05 abr. 2012.

Apêndice 1

Comportamento Seguro

Questionário para composição de monografia a ser apresentada em Nov/2012 como conclusão do curso de especialização em Gestão Estratégica da Informação na Universidade Federal de Minas Gerais.
O objetivo desse questionário é avaliar o comportamento informacional do usuário no ambiente profissional. Para tal, faz-se necessária a análise de questões que tangem algumas atividades do dia a dia do profissional em sua organização.
A pesquisa tem como fim compor material para apresentação da monografia conforme supracitado. Ressalto a não identificação de qualquer participante assim como a não divulgação dos nomes das organizações envolvidas.

O questionário possui 12 grupos de perguntas e o tempo médio gasto para resposta do mesmo é de 8 minutos. Conto com a participação de vocês para enriquecer a base de dados de minha pesquisa. Desde já agradeço a todos.
*Obrigatório

1.1. Você utiliza algum meio de identificação para acessar o prédio da sua organização? *
Por exemplo: cartão de ponto, biometria, catraca, crachás, etc.

- Sim
- Não

1.2. Você é obrigado a ficar com seu crachá visível durante o expediente? *

- Sim
- Não
- Não se aplica

1.3. Quando você precisa entrar na organização fora do seu horário de trabalho, você consegue o acesso através dos meios de identificação usados diariamente? *
Ex.: fora do horário de expediente (após as 18h) ou nos finais de semana.

- Sim
- Não
- Não se aplica

2.1. Sua organização possui protocolos de cópias de documentos e/ou impressões? *
Ex.: quando você vai copiar um contrato você deve preencher algum protocolo?

- Sim
- Não
- Não sei

2.2. Sua organização tem uma política quanto ao descarte de documentos físicos? *

- Sim
- Não
- Não Sei

2.3. Sua organização classifica as informações que circulam internamente via comunicados impressos e/ou e-mails, como por exemplo: confidencial, restrita, pública, etc? *

- Sim
- Não
- Não sei

2.4 Quando você manda imprimir algum documento do trabalho em uma impressora da rede, que não fique sobre sua mesa, você vai imediatamente buscar na impressora? *

- Sim
- Não

3.1 No seu local de trabalho o computador que você utiliza é um notebook? *

- Sim
- Não

3.1.1 Você pode levar o notebook do trabalho para sua casa?

- Sim
- Não

3.1.2 Os notebooks são guardados em local específico e reservado de um dia para o outro?

- Sim
- Não

3.1.3 Os notebooks possuem uma trava para que os mesmos não sejam retirados da mesa na ausência do usuário?

- Sim
- Não

3.1.4 Os notebooks permanecem sobre as mesas no final do dia sem trava física?

- Sim
- Não

3.1.5. Se o seu notebook for roubado você sabe qual é o procedimento a cumprir?

- Sim
- Não

3.2. Você pode inserir dispositivos USB de armazenamento, como um pen drive ou HD externo, no seu computador para colocar ou retirar informações dele? *

- Sim
- Não
- Não Sei

3.3 Você pode salvar dados pessoais, como músicas, fotos e/ou vídeos no seu computador do trabalho? *

- Sim
- Não
- Não Sei

3.4 Você tem autorização para instalar programas em seu computador de trabalho? *

- Sim
- Não
- Não Sei

3.5 Você consegue gravar, sem auxílio ou liberações de terceiros, DVDs/CDs no seu computador do trabalho? *

- Sim
- Não
- Não Sei
- Não
- Não se aplica

4.1. Seu computador de trabalho possui senha de usuário para acessá-lo? *

- Sim
- Não

4.2. Você bloqueia a tela do computador quando se ausenta da sua posição de trabalho mesmo que por poucos minutos? *

- Sim
- Não

4.3. Você possui mais de uma senha para acessar os diversos sistemas de sua organização? *

- Sim
- Não

4.4. A senha que você utiliza faz referência a datas de aniversário de familiares próximos, nomes de filhos/cônjuges, sequencia numérica? * *

Ex.: Senhas do tipo: 123456/147741/987654 ou ainda seu time de futebol.

- Sim
- Não

4.5. Você utiliza senhas com mais de 6 caracteres? *

- Sim
- Não

4.6. Você utiliza letras maiúsculas em suas senhas? *

- Sim
- Não

4.7. Você utiliza caracteres especiais em suas senhas? *

Ex: @, #, &.

- Sim
- Não

4.8. Você utiliza frases inteiras como senha? *

- Sim
- Não

4.9. Você consegue lembrar de todas as senhas do trabalho sem anotá-las? *

- Sim
- Não

4.10. Sua organização força por meio de sistemas a troca de senhas após alguns dias/meses? *

Ex.: a senha de acesso a rede que pede para ser trocada quando você se loga.

- Sim
- Não

5.1. Você já precisou utilizar outra senha além da sua para acessar alguma informação em sistemas da empresa? *

Ex.: a senha de um gestor além da sua para alguma aprovação interna.

- Sim
- Não

5.2. Você conhece a senha do seu superior hierárquico, para usar em casos de emergência? *

- Sim
- Não

5.3. Você já compartilhou sua senha com companheiros de trabalho em caso de emergência? *

- Sim
- Não

6.1. Existe uma política de acesso à Internet na sua organização? *

- Sim
- Não
- Não Sei

6.1.1. Você se lembra das regras de política de acesso à Internet de sua organização? *

- Sim
- Não

6.2. Você já foi alertado pelo seu superior hierárquico e/ou gestor de rede em relação aos spams e virus que podem ser recebidos nos e-mails? *

- Sim
- Não

6.3. Você usa seu e-mail corporativo para enviar e-mail particulares? *

- Sim
- Não

6.4. Você utiliza a Internet do seu trabalho apenas para assuntos profissionais? *

Exemplos de acessos não profissionais: acesso ao e-mail pessoal, Google, etc.

- Sim
- Não

6.5. Você pode anexar ou baixar anexos de e-mails que não sejam os corporativos? *

- Sim
- Não
- Não Sei

7.1. A sua organização exige dos funcionários a assinatura de algum termo de compromisso em relação ao sigilo de informação? *

- Sim
- Não

7.1.1. Você se lembra do que está escrito nesse termo? *

- Sim, de todo o termo
- Sim, de parte do termo
- Não me lembro

7.1.2. Existe algum tipo de penalidade prevista nesse termo caso o mesmo não seja cumprido? *

- Sim
- Não
- Não me lembro

7.2. Existe alguma política de segurança da informação em sua organização? *

- Sim
- Não
- Não sei

8.1. Alguma vez você já foi interpelado por alguém de fora do seu convívio profissional e/ou pessoal querendo saber informações da empresa em que você trabalha? *

- Sim
- Não
- Não me lembro

8.2. Você conversa com colegas do trabalho na hora do lanche/almoço, dentro ou fora da empresa, sobre negócios da organização? *

- Sim
- Não

8.3. Você recebeu orientação em relação aos cuidados que devam ser tomados em conversas sobre os assuntos da empresa que você trabalha? *

- Sim
- Não

8.4. Sua organização já promoveu alguma palestra ou treinamento a respeito de normas e padrões adequados de comportamento para o uso da informação? *

- Sim
- Não

8.5. Sua organização já promoveu alguma palestra ou treinamento oficial de sua organização com normas e padrões de segurança da informação? *

- Sim
- Não

9.1. Você consegue acessar as informação da sua organização de fora dela, da sua casa por exemplo? *

- Sim
- Não
- Não sei

9.1.1. Você recebeu algum treinamento/orientação para esse acesso? *

Ex.: redes privadas virtuais por meio de aplicativos que são instalados no notebook (VPN), requisitos mínimos de segurança, etc.

- Sim
- Não

9.2. Sua organização disponibiliza para você um telefone celular corporativo smartphone? *

- (•) Sim
- ( ) Não

9.2.1. No seu telefone corporativo (smartphone) a caixa de e-mail fica com a senha já automática? *

- ( ) Sim
- ( ) Não

9.3. Sua organização disponibiliza para você um tablet corporativo? *

- ( ) Sim
- ( ) Não

9.3.1. No seu tablet corporativo caixa de e-mail fica com a senha já automática? *

- ( ) Sim
- ( ) Não
- ( ) Não se aplica

9.4. Sua organização permite que você use seu tablet pessoal como se fosse profissional? *

Por exemplo: você consegue usar o tablet pessoal para acessar a rede de sua organização e/ou email corporativo normalmente?

- ( ) Sim
- ( ) Não
- ( ) Não se aplica

10. Qual o seu sexo? *

- ( ) Masculino
- ( ) Feminino

11. Qual a natureza da sua organização? *

- ( ) Pública
- ( ) Privada

12. Qual é o setor de atuação da sua organização? *

- ( ) Serviços Financeiros
- ( ) Educação
- ( ) Tecnologia da Informação
- ( ) Outro: [ ]