PUCRS

FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
CURSO DE ADMINISTRAÇÃO DE EMPRESAS
LINHA DE FORMAÇÃO EM
GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

IDENTIFICAÇÃO DOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO E O IMPACTO NA SEGURANÇA DA INFORMAÇÃO CORPORATIVA

BRUNO REGINATO ARAUJO

Porto Alegre

2013

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
Av. Ipiranga, 6681 - Caixa Postal 1429
Fone: (51) 3320-3500 - Fax: (51) 3339-1564
www.pucrs.br
CEP 90619-900 Porto Alegre - RS
Brasil

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL
FACULDADE DE ADMINISTRAÇÃO, CONTABILIDADE E ECONOMIA
CURSO DE ADMINISTRAÇÃO DE EMPRESAS
LINHA DE FORMAÇÃO EM
GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

BRUNO REGINATO ARAUJO

IDENTIFICAÇÃO DOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO E O IMPACTO NA SEGURANÇA DA INFORMAÇÃO CORPORATIVA

Porto Alegre
2013

BRUNO REGINATO ARAUJO

IDENTIFICAÇÃO DOS USUÁRIOS DE TECNOLOGIA DA INFORMAÇÃO E O IMPACTO NA SEGURANÇA DA INFORMAÇÃO CORPORATIVA

Artigo apresentado como requisito parcial à obtenção do grau de Bacharel em Administração de Empresas, linha de formação Gestão de Tecnologia da Informação na Faculdade de Administração, Contabilidade e Economia da Pontifícia Universidade Católica do Rio Grande do Sul.

Professor Orientador: Prof Alessandro Nunes de Souza

Porto Alegre

2013

1 INTRODUÇÃO

É notável a importância da tecnologia de informação para as organizações nos tempos atuais, onde cada vez mais a informação tem valor agregado para a empresa. Para acompanhar o avanço dos negócios, a tecnologia da informação tem como competências, agilizar, garantir e assegurar o processamento de dados da organização.

Dada a relevância da tecnologia de informação para os negócios, a segurança da informação deve assegurar a disponibilidade, confidencialidade, integridade e análise dos riscos para estimar eventuais danos aos sistemas da organização.

Conforme Gartner Group (2007), os investimentos em Segurança da Informação devem superar os gastos em relação à Tecnologia da Informação Corporativa. Gartner Group (2007) afirma que as empresas que alcançarem maior índice de maturidade em segurança tecnológica reduzirão os gastos anuais com TI.

Em um mercado globalizado e competitivo, onde a rivalidade está cada vez mais acirrada, a organização que não acompanhar o ritmo da tecnologia da informação corre o risco de ver seu negócio ameaçado. Não basta ter apenas planos, investimentos e equipamentos: é necessário desenvolver e executar um plano de ações de TI para evitar riscos em relação à segurança da informação corporativa.

A situação problemática do artigo irá analisar o comportamento, atitudes e os possíveis fatores causais que possam gerar problemas nas informações corporativas, decorrentes de falhas na utilização por parte dos usuários de tecnologia da informação. Além disso, verificar o seu impacto organizacional na segurança da informação, sendo utilizado como referência o modelo de Torkzadeh e Doll (1999), que trata da "Cadeia de Valores". Esse modelo é baseado na construção de sistemas de sucesso de crenças, atitudes, comportamento, impactos sociais e econômicos da TI.

Segundo Beal (2005), os riscos e ameaças contra a segurança da informação podem ter 4 (quatro) origens básicas: ambiental, técnica, lógica ou humana. De todas as ameaças, o comportamento humano é o mais difícil de gerenciar. As organizações investem milhões em recursos tecnológicos e de sistemas eficientes para diminuição dos riscos a seus ativos, mas um colaborador mal intencionado ou mal treinado pode tornar estas medidas ineficientes.

A empresa Modulo (2006) realizou a 10ª Pesquisa Nacional de Segurança da Informação e trouxe indicadores, melhores práticas e tendências do mercado brasileiro na área de segurança da informação. Esta pesquisa levantou dados importantes para melhora da

evolução das organizações nacionais, identificou que a expectativa das empresas (77%) é de no futuro aumentar o combate a problemas relacionados com segurança da informação, já que as falhas mais comuns são causadas por funcionários (24%) e hackers (20%). Conforme Modulo (2006), os gestores (55%) consideram a falta de conscientização dos executivos e usuários a principal dificuldade para a implementação da segurança da informação. A pesquisa relata que problemas com vírus (15%), spam (10%) e fraudes (8%) são os maiores causadores de problemas financeiros nas organizações.

Albrechtsen (2007) realizou um estudo que identificou que o aumento do ritmo e da carga de trabalho e tarefas pode comprometer a forma como os colaboradores utilizam e dão importância ao uso seguro da TI.

O foco do artigo é na Faculdade de Administração, Contabilidade e Economia (FACE) da PUCRS, que iniciou suas atividades em 1931, com a denominação de Faculdade de Ciências Políticas e Econômicas (FCPE). Em 1978 passou a adotar oficialmente o nome Faculdade de Administração, Contabilidade e Economia (FACE).

A estrutura da FACE tem em torno de 170 colaboradores entre professores e técnicos administrativos. Seu prédio fica localizado na Av. Ipiranga, 6681, prédio 50, no bairro Partenon, em Porto Alegre, Rio Grande do Sul.

A FACE apresenta cinco áreas de conhecimento: Administração, Contabilidade, Economia, Hotelaria e Turismo, oferecendo nove cursos em suas linhas de formação. Tem em torno de quatro mil alunos nos turnos da manhã e noite (PUCRS, 2012a).

A FACE é uma unidade da PUCRS (Pontifícia Universidade Católica do Rio Grande do Sul), que é uma das mais tradicionais instituições de Ensino Superior do Brasil, tendo como missão, "fundamentada em princípios da ética e do cristianismo e na tradição educativa marista, tem por missão produzir e difundir conhecimento e difundir conhecimento e promover a formação humana e profissional, orientada por critérios de qualidade e relevância, na busca de uma sociedade justa e fraterna" (PUCRS, 2012b).

A PUCRS conta com a Gerência de Tecnologia da Informação e Telecomunicação (GTIT), que é responsável pela área de tecnologia, concentrando todos os colaboradores e equipamentos que realizam atividades ligadas à tecnologia da informação, entre estas funções está a segurança da informação. A GTIT conta com mais de 100 colaboradores nos setores de *helpdesk*, suporte (telecom e informática), desenvolvimento de sistemas (acadêmicos e administrativos), coordenação de infra-estrutura e sistemas operacionais.

O objetivo geral do trabalho é identificar e analisar o perfil dos usuários de tecnologia da informação e os seus impactos na segurança da informação corporativa. Já os objetivos específicos são identificar o perfil dos usuários; e obter informações referentes a atitudes, comportamentos, impactos no trabalho individual e impactos organizacionais.

Este trabalho trata-se de uma pesquisa de tecnologia da informação, que tem por finalidade detectar possíveis falhas humanas que possam interferir diretamente na segurança da informação da empresa. Para tanto, está dividido em 3 (três) capítulos.

No segundo capítulo é desenvolvida a revisão da literatura, onde são abordados os principais conceitos do assunto a ser pesquisado, relatando as interpretações de diversos autores sobre o tema.

A seguir, no terceiro capítulo, é relatado o instrumento de pesquisa que norteia o rumo deste trabalho, fundamentando o método de pesquisa a ser utilizado e como foi realizada a coleta e análise dos dados na realização do estudo.

2 IMPACTOS DA TECNOLOGIA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Atualmente, integrar os recursos de Tecnologia da Informação (TI) ao negócio empresarial tem se tornado um problema cada vez maior nas organizações, devido aos conflitos culturais existentes nas gestões. Atualmente a tecnologia da informação é vista como um fardo que gera desperdício de investimentos; a realidade é que a organização é um todo, onde todas forças devem levar a um único objetivo.

Nestes conflitos culturais é que podem ocorrer falhas e perdas das informações corporativas, podendo comprometer seriamente a gestão da organização. A segurança da informação baseia-se em garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações e dos dados da empresa.

Tendo em vista que o tema proposto possui uma vasta disponibilidade de literatura, se torna possível obter diversas opiniões e experiências conceituais sobre o mesmo. Para se chegar a uma análise definitiva do assunto, existem diversos conceitos e questões a serem abordadas, iniciando pela descrição da cultura organizacional, relatando o impacto da tecnologia da informação na organização, a importância da segurança da informação nas empresas, e abordando o modelo de “cadeia de valores” de Torkazadeh e Doll (1999), até chegar ao conceito do tema proposto.

2.1 Cultura organizacional, cultura de tecnologia da informação e os impactos organizacionais.

Toda empresa, independentemente de seu ramo de atuação, seja privado ou de caráter público, possui culturas, filosofias e políticas, podendo ser definidas formal ou informalmente aos seus colaboradores.

Chiavenato (2010) cita que, no ponto de vista mais amplo, cada nação tem uma cultura própria que influencia os comportamentos das pessoas e das organizações. Compreende os valores compartilhados, hábitos, usos e costumes, códigos de conduta, tradições e objetivos que são aprendidos das gerações mais velhas.

Rezende e Abreu (2011) afirmam que a filosofia é caracterizada pela intenção de ampliação da compreensão de conhecimentos, doutrinas e sabedorias. E que as políticas empresariais podem ser definidas como regras e normas das gestões das organizações. Todos esses conceitos, unidos ou isolados, devem ser observados e respeitados, já que influenciam significativamente no planejamento estratégico, nos sistemas de informação e no modelo de gestão da empresa.

Jones (2010) descreve a cultura organizacional como o conjunto de valores compartilhados e normas que controlam as interações dos membros da organização entre si com fornecedores, consumidores e de pessoas de fora dela. A cultura é modelada pelas pessoas que fazem parte da organização, que modela e controla o comportamento dentro dela. Isto influencia a maneira de como os colaboradores respondem a uma situação e como interpretam o ambiente ao redor da organização.

Segundo Probst, Raub e Romhardt (2002), cada empresa tem sua própria cultura organizacional, moldada por sua história e suas circunstâncias. A cultura organizacional serve para definir regras básicas de comportamento social e de ações coletivas.

Chiavenato (2010) relata que, da mesma maneira que cada país tem a sua própria cultura, as empresas também tem suas culturas organizacionais ou corporativas próprias e específicas. Afirma que, “para se conhecer uma organização, o primeiro passo é conhecer sua cultura. Fazer parte de uma organização é assimilar a sua cultura”. Observa também que a cultura organizacional pode sofrer impactos originados pela tecnologia da informação. O autor afirma que a internet está mudando não apenas a maneira de interação entre clientes, fornecedores e companhias, como também a maneira pela qual as organizações estão trabalhando internamente. Após poucos anos da introdução da tecnologia da informação, ela

passou a afetar profundamente a base de competição de muitos mercados e que, para minimizar este impacto na cultura organizacional, as empresas devem analisar a tecnologia de informação quanto ao seu negócio.

Medeiros e Sauvé (2003) definem a Tecnologia da Informação como sendo a junção das funcionalidades das áreas da informática e telecomunicações. Através da aplicação de conceitos, conhecimentos e equipamentos das áreas de informática (software, hardware e internet) e de telecomunicações, a TI torna-se ferramenta de essencial utilidade para toda e qualquer área da empresa, unindo o potencial da informática e o poder de interconexão das telecomunicações, podendo transformar e integrar todas as áreas e setores das organizações. O uso da TI permite uma infinidade de opções de aplicações que podem auxiliar, aprimorar e facilitar desde a automatização de tarefas até a tomada de decisões gerenciais. É preciso que as empresas conheçam melhor os recursos e a realidade das tecnologias novas e emergentes, avaliando possíveis impactos organizacionais na sua maneira de trabalhar. É preciso relacionar a adoção de tecnologias às reais necessidades e perspectivas de crescimento dos negócios da empresa.

Walton (1998) cita uma característica da Tecnologia da Informação avançada que é sua dupla potencialidade, a habilidade de uma tecnologia em produzir um conjunto de efeitos organizacionais ou seus opostos. A TI pode padronizar atividades ou ampliar o poder de decisão dos usuários, pode reforçar o controle hierárquico ou facilitar a auto-gestão e a aprendizagem dos usuários. O autor resume que os administradores podem utilizar Tecnologia da Informação para reforçar uma estratégia que se apóie sobre a concordância dos colaboradores, ou pode utilizá-la para criação de um contexto organizacional que promova o comprometimento dos empregados. A dupla potencialidade da TI significa uma cuidadosa dose de precauções na sua implantação, devendo tornar claro seus efeitos pretendidos para que a gerência e usuários não interpretem de maneira diferente os processos dos sistemas, apresentando um dos maiores desafios para que o processo seja plenamente eficaz.

Laurindo (2008) afirma que, para avaliar os impactos da tecnologia da informação nas operações, é necessário precisão nos resultados advindos da tecnologia da informação em relação a objetivos, metas e requisitos destas organizações.

2.2 Segurança da Informação

Para Foina (2011), as informações de uma empresa têm valor não só para ela como para a concorrência (espionagem empresarial) e para outras empresas, devido a cadastros de clientes, lista de produtos e informações confidenciais. A preocupação com a segurança da informação deve ser constante na organização, principalmente na área de TI. Pelo setor de Tecnologia da Informação transita um grande número de informações sensíveis e estratégicas de interesse interno (empresa) e externo (concorrência). A divulgação dessas informações pode acarretar prejuízos e penalidades graves.

Conforme Foina (2011), a Segurança da Informação pode ser dividida em duas partes. A **Segurança Física** tem como objetivo preservar o patrimônio da empresa, seus arquivos contra roubos e sabotagens. A segurança física fica restrita ao CPD (Centro de Processamento de Dados) e aos pontos de acesso remotos e à rede de dados. Alguns dos problemas relacionados à segurança física são roubo de insumos (memórias, discos, etc), acesso de pessoas não autorizadas às informações da empresa ainda dentro do setor de TI, roubo de dados armazenados em arquivos magnéticos ou ópticos com conteúdos confidenciais e sabotagem nos equipamentos e arquivos de dados. Para minimizar tais problemas, é recomendado o rígido controle de acesso às áreas sigilosas da empresa, como dispositivos de identificação biométrica nos ambientes mais críticos.

A **Segurança Lógica** compreende a integridade dos arquivos de dados e dos programas da empresa. Qualquer sabotagem ou dano nos arquivos de dados pode ocasionar sérios problemas para a organização. A segurança lógica estabelece mecanismos de acesso aos arquivos, sistemas e páginas *Web* da empresa, limitando os recursos para cada usuário. Problemas relacionados à segurança lógica são ataques de *hackers* através da Web, pirataria (cópia ilegal) de programas de computadores, pirataria de *software* e contaminação de vírus e perda de dados importantes causadas por estes ataques.

Conforme Beal (2005), a segurança da informação pode ser entendida como o processo de proteger informações das ameaças a sua integridade, disponibilidade e confidencialidade:

a) Confidencialidade: garantir o acesso às informações a usuários restritos e legítimos;
b) Integridade: garantir a consistência da informação durante seu ciclo de vida, em especial prevenção contra alteração ou perda de dados da informação. Outro objetivo é garantir a autenticidade da informação;

c) Disponibilidade: garantir que a informação e os ativos associados estejam disponíveis quando necessário aos usuários que tenham acesso às informações.

Beal (2005) afirma que a segurança de tecnologia da informação deve ser uma responsabilidade compartilhada por todos os integrantes da organização para eficácia das medidas de proteção. E que existe uma grande tendência nas empresas de atribuir à tecnologia da informação as atividades e responsabilidades de segurança, pelo fato de que grande parte dos problemas de segurança sejam relacionados aos equipamentos de tecnologia da informação. Devem ser considerados outros fatores fora do contexto, que incluem aspectos físicos, humanos e de gestão de processos.

ABNT NBR ISO/IEC 27001 (2005) define um conjunto de boas práticas para a gestão da segurança da informação, que foi elaborada para estabelecer um modelo de implementação, operação, monitoração e revisão para certificação de sistemas de segurança da informação. Foi publicada em outubro de 2005 pela *International Organization for Standardization (ISO)* e pela *International Electrotechnical Commision (IEC).* Esta norma cobre todos os tipos de organizações, sejam privadas, públicas ou organizações sem fins lucrativos. Ela especifica requisitos para a implementação de controles de segurança customizados para as organizações.

De acordo com o padrão ABNT NBR ISO/IEC 27001 (2005), a segurança da informação tem como premissas básicas a preservação da confidencialidade, integridade e disponibilidade da informação. Outra função da segurança da informação é garantir a autenticidade, responsabilidade e confiabilidade das informações. A norma define pontos essenciais da segurança da informação:

a) Evento de segurança da informação: é a ocorrência identificada de um sistema, serviço ou rede que demonstre possíveis violações das políticas de segurança da informação ou falha de controles, ou de situações desconhecidas, que possa ter impacto na segurança da informação;
b) Incidente de segurança da informação: é um simples (ou série de) evento(s) indesejado(s) ou inesperado(s), que tenha grande chance de impactar a operação da organização e ameaçar as informações;
c) Sistema de gestão da segurança da informação: baseada em uma aproximação de risco empresarial, que deve estabelecer, implementar, operar, monitorar, revisar, manter, aperfeiçoar a segurança da informação.

2.3 Modelo de Doll e Torkzadeh

Torkzadeh e Doll (1999) descrevem o modelo de "cadeia de valores" na construção de um sistema de sucesso de crenças, atitudes, comportamentos, impactos sociais e econômicos da tecnologia da informação. O impacto deve ser conceito central que incorpora os efeitos. É difícil imaginar como a tecnologia da informação pode ser avaliada sem mensurar o impacto que pode ter no trabalho do indivíduo. Este impacto ocupa a posição central da "Cadeia de Valores" para a construção do sistema, porque é uma conseqüência direta do uso, e um fator importante para determinar o seu impacto na organização, conforme demonstrado na figura 1.

Fatores Causais	Crenças	Atitudes	Comportamento	Impacto sobre o trabalho Individual	Impacto na Organização

Figura 1- Sistema de Cadeia de valor.
Fonte: Torkzadeh e Doll (1999)

Torkzadeh e Doll (1999) justificam a pesquisa pela Teoria Comportamental da Administração, afirmando que o impacto da TI sobre o indivíduo é refletido diretamente no uso geral da tecnologia da informação, sendo um fator importante no impacto da tecnologia da informação nos aspectos organizacionais.

Para Torkzadeh e Doll (1999), concepção de impacto da tecnologia da informação, cuja visão é voltada para o controle gerencial, é um paradigma que limita e ignora aspectos importantes e fundamentais para o sucesso das organizações contemporâneas. As empresas estão realizando diversos investimentos na Tecnologia da Informação e na constatação de que o usuário final é peça-chave para o sucesso ou fracasso da tecnologia da informação na organização. Deste modo, a elaboração de dados, que possam embasar a avaliação do impacto na organização, passa diretamente pela opinião do usuário final, que assume um papel fundamental no estudo.

3 MÉTODO

Segundo Romero e Nascimento (2008), a definição de método científico é o conjunto de procedimentos, técnicas ou operações, com uma lógica de pensamento e cognição, capazes de construir e embasar o processo de conhecimento científico, respondendo a uma problemática e, assim alcançar os objetivos da pesquisa.

Para Cooper e Schindler (2004), uma boa pesquisa é gerada por meio de dados confiáveis, sendo derivada de práticas conduzidas profissionalmente e que podem ser usadas com segurança na tomada de decisão gerencial. Os autores ainda definem a pesquisa em administração como uma investigação sistemática que fornece informações para orientar as decisões empresariais.

Tendo em vista a situação problemática e os objetivos definidos neste trabalho, fica definida uma abordagem de caráter quantitativo neste estudo. Segundo Romero e Nascimento (2008), esta natureza apresenta as seguintes definições:

a) Enfoque quantitativo;
b) Procura generalizar os resultados;
c) Envolve grandes amostras;
d) Os dados são objetivos;
e) O pesquisador é independente do que está sendo pesquisado;
f) Permite generalizações.

Quanto aos objetivos, será utilizada uma pesquisa descritiva que, para Gil (2007), têm como característica primordial a descrição das características de determinada população ou fenômeno ou estabelecimento entre variáveis. Conforme Romero e Nascimento (2008), a pesquisa descritiva têm como objetivo principal descrever as características de grandes amostras ou estabelecer relações e correlações entre variáveis.

A estratégia de pesquisa adotada é a survey que, para Gil (2007), se caracteriza pela interrogação do comportamento das pessoas que se deseja conhecer. Para Gil (2007), as vantagens da survey são: conhecimento direto da realidade, economia, rapidez e quantificação dos dados obtidos, pois o resultado do estudo possibilita análises estatísticas, tornando possível até mesmo conhecer a margem de erro do resultado obtido. Neste mesmo segmento, Cooper e Schindler (2004) dissertam que a survey visa buscar no entrevistado suas idéias em

relação aos aspectos importantes do assunto tratado e descobrir a importância dentro do campo de conhecimento da pessoa.

Ao fim desta seção, fica definido que esta pesquisa caracteriza-se por uma abordagem quantitativa, de objetivo de pesquisa descritiva e a estratégia para o seu desenvolvimento é a survey.

As fases da pesquisa seguem, conforme mostrado na figura 2:

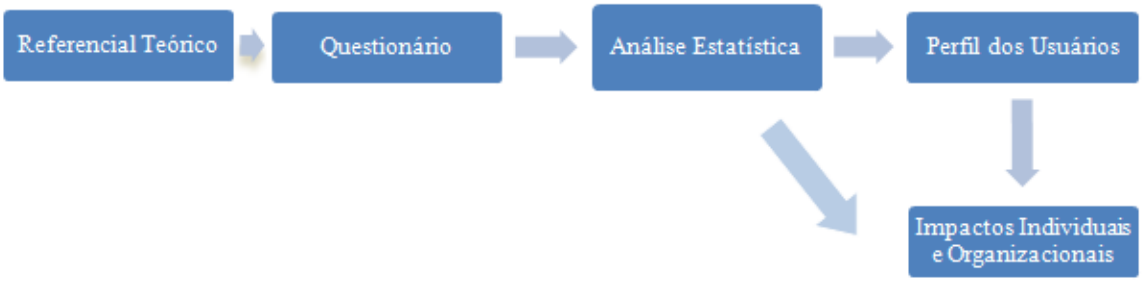

Figura 2 – Desenho de Pesquisa.

Fonte: O pesquisador (2012)

A pesquisa foi executada com 30 (trinta) colaboradores da organização, divididos em dois grupos: G1 (14 assistentes administrativos/Colaboradores) e G2 (16 professores/ coordenadores). A escolha das pessoas foi por amostragem aleatória simples como, por exemplo, matrícula funcional ou *login* de acesso a rede de dados da empresa.

Segundo Gil (2007), a amostragem aleatória simples consiste em atribuir a cada elemento da população um número único para depois selecionar alguns desses participantes de forma casual.

Neste trabalho, o instrumento de pesquisa foi elaborado pelo pesquisador, realizando perguntas sobre a utilização dos componentes de tecnologia da informação na organização, a fim de estudar os seguintes itens, perfil, comportamento, atitude e utilização de infra-estrutura de rede.

O referido instrumento é composto por 3 (três) partes, e encontra-se no apêndice A:

a) Apresentação sucinta do conteúdo da pesquisa e explicação de sua finalidade;
b) Instruções para o preenchimento da pesquisa;
c) Conjunto de 10 (dez) perguntas englobando os assuntos como perfil, comportamento, atitude e utilização de ferramentas fornecidas pela TI.

A análise de dados foi por estatística descritiva, que visa comprovar tendências de comportamento dos usuários.

4 ANÁLISE DOS DADOS

A amostra verificada possui 30 respondentes, divididos em dois grupos, coordenadores 16, e auxiliares administrativos 14, de uma população de 39 pessoas. A seguir é apresentados os resultados obtidos no questionário de escala com auxilio da tabulação dos dados, constituídos de freqüência e percentual de respostas.

Após aplicação da pesquisa de identificação dos usuários de tecnologia da informação, foi realizada a análise dos dados, conforme tabulação no apêndice B.

4.1 Perfil dos usuários

O perfil geral dos respondentes é composto por pessoas dos sexos feminino e masculino, com faixa etária entre 20 e 50 anos, que trabalham na empresa.

Conforme verificado na tabulação dos resultados, ficou evidente a diferença de compartilhamento do computador com outro colega de serviço entre os grupos. No grupo de coordenadores 93,75% tem baixa freqüência de divisão, enquanto no grupo de auxiliares administrativos o compartilhamento do equipamento em média é de 42,86% dos respondentes.

Analisando os dados de grau de importância das informações corporativas que os respondentes têm acesso, ficou evidente a igualdade de nível médio entre os grupos de coordenadores 56,25% e auxiliares administrativos 50%.

Observando os resultados da tabulação, ficou demonstrada a baixa freqüência de acesso dos grupos as redes sociais no ambiente de trabalho. Onde a amostra do grupo de coordenadores ficou em 87,5%, e dos auxiliares administrativos em 78,57 de freqüência de acessos.

Os resultados examinados no que diz respeito ao risco relativo de bloqueio da base de trabalho foram bem diferentes, 56,25% respondentes do grupo coordenadores considera de baixo risco o bloqueio da base. Já 50% dos pesquisados do grupo de auxiliares administrativos considera alta o risco relativo de bloqueio da base de trabalho.

4.2 Atitudes, comportamentos e o impacto no trabalho individual

Integrar a tecnologia da informação ao negócio empresarial é um problema freqüente nas organizações, devido aos diferentes níveis culturais no que diz respeito ao comportamento e atitudes de seus usuários. Nestes diferentes níveis de culturas individuais é que ocorrem falhas e perdas de informações corporativas. Torkazadeh e Doll (1999) baseiam sua teoria de "cadeia de valores" com relação à crença, atitudes e comportamentos, e que isto reflete diretamente no trabalho individual.

Beal (2005) relata que, de todas as ameaças sobre tecnologia da informação, o comportamento e atitudes humanas são as mais difíceis de gerenciar, pois os usuários podem estar mal treinados ou mal intencionados.

Nas questões sobre comportamento, ficou constatado o baixo nível de freqüência em relação à utilização de redes sociais no ambiente de trabalho, sendo este um ponto positivo para a organização, já que quanto menor utilização destes elementos, menor será a perda de tempo de seu colaborador em ações extra profissionais. Em contraponto a este ponto positivo, ficou evidenciado risco com relação ao bloqueio da base de trabalho, já que 50% do grupo de auxiliares administrativos consideram de alto risco esta questão. Neste ponto, o comportamento do usuário deve ser altamente trabalhado pela organização, para a conscientização e atenção do indivíduo para possíveis falhas individuais e possíveis perdas de informações.

Os dados sobre atitudes dos grupos de usuários obteve um consenso médio no que diz respeito ao nível de segurança das suas senhas nos sistemas de TI. Este dado pode ser considerado preocupante para a organização, pois senhas de nível médio não são totalmente seguras para invasões internas ou externas destes sistemas.

A utilização de dispositivos móveis pode ser considerado outro fator preocupante para a organização, pois mais de 50% dos entrevistados dos dois grupos consideram sua utilização média ou alta no ambiente de serviço. Isto requer um alto nível de controle da área de TI sobre todas as informações corporativas dos sistemas da empresa, a fim de diminuir ou minimizar possíveis fraudes ou roubos.

4.3 Impactos individual e organizacional

A partir da aplicação da pesquisa de identificação dos usuários de tecnologia da informação na organização, utilizando como base o modelo de "cadeia de valores" de Torkazadeh e Doll (1999), analisando crenças, atitudes e, principalmente, o comportamento

dos usuários de TI, observa-se que o grau de relação do impacto individual é proporcionalmente ligado ao impacto organizacional.

Chiavenato (2010) relata que cada empresa tem suas culturas organizacionais ou corporativas próprias e específicas. Observa também que a cultura organizacional pode sofrer impactos originados pela tecnologia da informação. Albrechtsen (2007) identificou que o aumento do ritmo da carga de trabalho, tarefas e informações está comprometendo a forma com que os usuários utilizam e dão importância ao uso seguro da tecnologia da informação.

Os impactos individuais oriundos dos usuários da tecnologia da informação, podem ser sentidos na organização de diversas maneiras, sejam elas na área de gestão de pessoas, informática ou principalmente financeiras, decorrentes de perdas de informações corporativas importantes ou sigilosas. Jones (2010) descreve a cultura organizacional como um conjunto de valores compartilhados e normas que controlam as interações dos membros da organização entre si. O autor define que cultura organizacional é modelada pelas pessoas que fazem parte da organização, que controla o comportamento e atitudes dentro dela.

Conforme Modulo (2006), os gestores consideram a falta de conscientização dos executivos e usuários como a principal dificuldade para a implementação da segurança da informação nas organizações. Afirma também que problemas com vírus, spam e fraudes são os maiores causadores de problemas financeiros nas organizações atualmente.

Para minimizar estes riscos, se faz necessário que as organizações tenham um plano claro e específico de políticas de segurança, e de utilização dos mais diversos sistemas que integram a área de tecnologia da informação na empresa. Atualmente, a baixa maturidade de gestão de pessoas de TI é apontada como a causadora de diversas perdas para as organizações, sejam por cópias ilegais de dados ou ataques piratas.

5 CONSIDERAÇÕES FINAIS

Analisando o modelo de “cadeia de valores” de Torkazadeh e Doll (1999), que o impacto individual pode gerar diversas perdas para a organização, chega-se à conclusão que a empresa deve criar e implantar uma cultura organizacional de tecnologia de informação.

A pesquisa de identificação dos usuários de tecnologia da informação pode ser um passo muito importante no que diz respeito à qualidade dos serviços prestados pela área de TI nas organizações, tanto na gestão de pessoas (conhecimento do perfil do usuário) quanto no que diz respeito à segurança da informação corporativa (minimizar impactos organizacionais).

A pesquisa encontrou limitações para ter uma melhor percepção sobre o assunto, como o baixo número de pessoas pesquisadas, já que foram enviados 39 questionários enviados por *e-mail* aos entrevistados e apenas 30 respondentes concluíram as perguntas. Outra limitação foi o nível das perguntas realizadas no que diz respeito aos sistemas de tecnologias utilizados na jornada de trabalho, já que a Gerência de Tecnologia da Informação e Telecomunicação (PUCRS) não permite que estes dados sejam utilizados em pesquisas acadêmicas. Para pesquisas futuras e para ter uma análise de perfil dos usuários, é sugerido que este questionário seja elaborado pelo pesquisador, juntamente com a área de tecnologia de informação, utilizando dados de ocorrências de falhas, perdas e riscos das informações corporativas da empresa.

A pesquisa realizada no artigo foi um *survey*, que é caracterizada pelo estudo do comportamento de um grupo de pessoas que se deseja conhecer, realizando um estudo direto da realidade dos indivíduos, gerando análises estatísticas, tornando possível um melhor entendimento sobre o assunto pesquisado. Chiavenato (2010) cita que a cultura individual compreende valores, hábitos, costumes e tradições, gerando código de conduta que refletem na organização. Os dados da pesquisa reforçam esta observação do autor em relação à cultura de tecnologia da informação.

Esse estudo, realizado em âmbito acadêmico, pode ser um aprendizado importante na formação do conhecimento dos novos gestores de tecnologia da informação, podendo abrir um novo conceito de gestão, integrando conhecimentos técnicos, financeiros e de gestão de pessoas. Hoje em dia, um bom gestor de TI não pode apenas focar seu conhecimento na parte de *hardware* e *software*: deve ter um olhar mais abrangente com enfoque nas pessoas, conhecendo seu comportamento e suas atitudes, diminuindo os gastos da empresa com segurança da informação.

A pesquisa, sendo realizada nas organizações, poderá gerar diversos ganhos e benefícios para o gerenciamento de seus usuários, ativos e dos sistemas de tecnologia da informação. Conhecendo o perfil dos usuários, a gestão poderá prever falhas, minimizando assim os gastos advindos de impactos individuais e garantir a integridade das informações corporativas. É muito difícil mensurar o valor de uma informação corporativa, por isso a gestão de tecnologia da informação não pode cometer o erro de investir grande parte de seus orçamentos em segurança da informação. Conforme Gartner Group (2007), os investimentos de segurança da informação devem alcançar 50% do orçamento das áreas de tecnologia da informação, e afirma que as empresas que atingirem o maior grau de maturidade em

segurança de TI reduzirão os gastos anuais, podendo realocar este orçamento em outras áreas de TI, como treinamentos, cursos para usuários e ativos da empresa. Outro ponto que reforça esse tipo de pesquisa é o baixo nível de maturidade da gestão de pessoas na área de tecnologia de informação.

Para que essas melhorias sejam alcançadas, a empresa deverá realizar uma política de segurança eficaz de utilização dos sistemas e equipamentos de tecnologia da informação, para minimizar ou diminuir impactos nas informações corporativas da organização, e garantir assim a confidencialidade, integridade e disponibilidade das informações necessárias para os usuários de TI.

Estas ações devem ser integradas, sendo disponibilizados cursos, palestras e seminários para os usuários de TI, a fim de para criar um *feedback* de informações que conscientize o amadurecimento nas crenças, atitudes e comportamento dos usuários, criando uma cultura de tecnologia de informação na organização.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001. **Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.** Rio de Janeiro, 2005

ALBRECHTSEN, E. **A qualitative study of users` view on information security.** Computers & Security, v.26, n.4, p.276-289, 2007.

BEAL, A. **Segurança da Informação: Princípios e Melhores Práticas para a proteção dos ativos de informação nas organizações".** São Paulo: Atlas, 2005.

CHIAVENATO, I. **Comportamento Organizacional: A dinâmica do sucesso das organizações"** 3 reimpr**.** Rio de Janeiro: Elsevier, 2010.

COOPER, D.R.; SCHINDLER, P.S. **Métodos de Pesquisa em Administração**. 7. ed. Porto Alegre: Bookman, 2004.

FOINA, P.R. **Tecnologia de Informação: planejamento e Gestão**. 2 ed. – 4 reimpr. São Paulo: Atlas, 2011.

GARTNER GROUP. **XII Conferência Anual**. São Paulo, 2007.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 5. ed. São Paulo: Atlas, 2007.

JONES, G.R. **Teoria das Organizações**. São Paulo: Ed Pearson Education do Brasil, 2010.

LAURINDO, Fernando José Barbin. Tecnologia da Informação, Estratégia e Organização. In: LAURINDO, Fernando José Barbin. ROTONDARO, Roberto Gilioli. (Orgs) **Gestão Integrada de Processos e da Tecnologia da Informação**. 1 ed. São Paulo: Atlas, 2008, p.68-97.

MEDEIROS, E.M.S.; SAUVÉ, J.P. **Avaliação do Impacto de tecnologia da informação emergentes nas empresas.** Rio de Janeiro: Qualitymark Editora Ltda, 2003.

MODULO. **10ª Pesquisa Nacional de Segurança da Informação**. 2006. Disponível em <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf > Acesso em: 27 setembro de 2012.

PROBST, G.; RAUB S.; ROMHARDT K.. **Gestão do Conhecimento: Os elementos construtivos do sucesso**. São Paulo: Bookman, 2002.

PUCRS. Conheça a FACE a escola de negócios da PUCRS. Disponível em <http://www3.pucrs.br/portal/page/portal/faceuni/faceuniCapa/faceuniconheca> Acesso em: 22 agosto de 2012.

PUCRS. A Universidade. Disponível em <http://www3.pucrs.br/portal/page/portal/pucrs/Capa/AUniversidade> Acesso 22 agosto de 2012.

REZENDE, D.A.; ABREU A.F. **Tecnologia da Informação Aplicada a Sistemas de Informações Empresariais.** São Paulo: Atlas, 2011.

ROMERO, Sonia Mara Thater; NASCIMENTO, Belmiro J.C. Método de Pesquisa. In: FOSSATTI, Nelson C.; LUCIANO, Edimara Messomo. (Orgs) **Prática Profissonal em Administração:** Ciência, Método e Técnicas. 1 ed. Porto Alegre: Sulina, 2008, p.51-64.

TORKAZADEH, G.; DOLL, W. J. **The Development of a Tool for Measuring the Perceived Impact of Information Technology on Work.** Omega, 1999, v. 27, n.3, p.327-339.

WALTON, R.E. **Tecnologia da Informação: O uso de TI pelas empresas que obtêm vantagem competitiva** São Paulo: Atlas, 1998.

APÊNDICE A – INSTRUMENTO DE PESQUISA

a) **Objetivo** - Este instrumento de pesquisa tem como principal objetivo avaliar e estudar o comportamento dos funcionários em relação à segurança da informação coorporativa e identificar possíveis relações com danos relacionados aos sistemas utilizados na organização.

b) **Instrução de preenchimento da pesquisa** - Abaixo será realizada 10 (dez) perguntas com relação à utilização da Tecnologia da Informação, que irá avaliar o perfil, comportamento e atitudes na utilização das tecnologias disponíveis na empresa. Obrigado pela colaboração, suas informações serão muito úteis para o aperfeiçoamento da segurança da informação coorporativa.

c) Questionário

QUESTIONÁRIO COM ESCALA					
Sócio-Demográfico	**1**	Sexo do colaborador (a) ?	**Masculino**		**Feminino**
	2	Faixa etária colaborador (a)?	**20 a 30**	**31 a 40**	**40 a 50**
Impacto Individual / Organizacional	**3**	Com que frequência o computador utilizado por você, na empresa, é dividido com outros colegas da organização?	**Baixa**	**Média**	**Alta**
	4	Qual o grau de importância das informações coorporativas que você tem acesso?	**Baixa**	**Média**	**Alta**
Comportamento	**5**	Com que frequência você acessa redes sociais (Facebook, Twitter,outros) no ambiente de trabalho?	**Baixa**	**Média**	**Alta**
	6	Qual é o risco relativo ao bloqueio do computador, sempre que você necessita sair da base de trabalho?	**Baixa**	**Média**	**Alta**
Crença	**7**	Qual é o seu grau de utilização das ferramentas de acesso aos sistemas de Tecnologia da informação da organização?	**Baixa**	**Média**	**Alta**
	8	Qual é o seu nível de conhecimento na área de informática?	**Baixa**	**Média**	**Alta**
Atitude	**9**	Qual é o nível de segurança das senhas utilizadas nos sistemas de tecnologia da informação?	**Baixa**	**Média**	**Alta**
	10	Com que frequência você utiliza dispositivos móveis (pen drive,celular,outros) de uso pessoal no ambiente de serviço?	**Baixa**	**Média**	**Alta**

APÊNDICE B – TABULAÇÃO DOS RESULTADOS DA PESQUISA

Questões		Coordenador				Auxiliar Administrativo			
		Baixa	Média	Alta	Total	Baixa	Média	Alta	Total
3. Com que frequência o computador utilizado por você, na empresa, é dividido com outros colegas da organização?	f	15	1	0	16	5	6	3	14
	%	93,75	6,25	0	100	35,71	42,86	21,43	100
4. Qual o grau de importância das informações coorporativas que você tem acesso?	f	1	9	6	16	2	7	5	14
	%	6,25	56,25	37,5	100	14,29	50	35,71	100
5. Com que frequência você acessa redes sociais (Facebook, Twitter, outros) no ambiente de trabalho?	f	14	2	0	16	11	3	0	14
	%	87,5	12,5	0	100	78,57	21,43	0	100
6. Qual é o risco relativo ao bloqueio do computador, sempre que você necessita sair da base de trabalho?	f	9	5	2	16	6	5	3	14
	%	56,25	31,25	12,5	100	21,43	28,57	50	100
7. Qual é o seu grau de utilização das ferramentas de acesso aos sistemas de Tecnologia da informação da organização?	f	6	4	6	16	3	4	7	14
	%	37,5	25	37,5	100	21,43	28,57	50	100
8. Qual é o seu nível de conhecimento na área de informática?	f	3	9	4	16	0	12	2	14
	%	18,75	56,25	25	100	0	85,71	14,29	100
9. Qual é o nível de segurança das senhas utilizadas nos sistemas de tecnologia da informação?	f	2	13	1	16	4	10	0	14
	%	12,5	81,25	6,25	100	28,57	71,43	0	100
10. Com que frequência você utiliza dispositivos móveis (pen drive,celular,outros) de uso pessoal no ambiente de serviço?	f	5	5	6	16	7	4	3	14
	%	31,25	31,25	37,5	100	50	28,57	21,43	100