Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação
E-ISSN: 1518-2924
bibli@ced.ufsc.br
Universidade Federal de Santa Catarina
Brasil

Santos CARNEIRO, Luciana Emirena; Barcellos ALMEIDA, Maurício
Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações
Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, vol. 18, núm. 37, mayo-agosto, 2013, pp. 175-202
Universidade Federal de Santa Catarina
Florianopolis, Brasil

ARTIGO

Recebido em: 18/09/2012

Aceito em: 04/08/2013

Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, v. 18, n. 37, p. 175-202, mai./ago., 2013. ISSN 1518-2924. DOI: 10.5007/1518-2924.2013v18n37p175

Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações

Information and Knowledge Management in the Scope of the Information Security practices: The human factor within Organizations

Luciana Emirena Santos CARNEIRO[1]
Maurício Barcellos ALMEIDA[2]

RESUMO

A segurança dos ativos informacionais sempre foi uma necessidade corporativa. Esses ativos podem ser dimensionados em três esferas principais, a saber, as pessoas, os processos organizacionais e as tecnologias. A internet, a difusão da web, as redes, além da presença cada vez mais marcante das tecnologias na vida das pessoas e das organizações têm provocado profundas transformações nos processos intrínsecos às rotinas pessoais e organizacionais. Essas mudanças promovidas pelos avanços tecnológicos têm gerado maior competitividade e descentralização e, em contrapartida, necessidade de gestão, controle, segurança e a proteção das informações e do conhecimento. Este artigo apresenta os resultados de uma investigação sobre segurança da informação, enfatizando a interferência dos aspectos humanos nas práticas de gestão da informação e do conhecimento relacionadas à segurança informacional. Através de uma pesquisa quali-quantitativa são identificados perfis e ações comportamentais dos colaboradores de uma empresa da área de saúde e sua inter-relação com falhas de segurança da

v. 18, n. 37, 2013.
p. 175-202
ISSN 1518-2924

[1] Pontifícia Universidade Católica de Minas Gerais - lucianaemirena@gmail.com
[2] Universidade Federal de Minas Gerais - mba@eci.ufmg.br

informação. Conclui-se que o elemento “pessoas” é uma variável importante, até mesmo crítica, para a gestão de segurança informacional nas organizações.

PALAVRAS-CHAVE: Segurança da Informação. Gestão da Informação e do Conhecimento. Comportamento Informacional.

ABSTRACT

The security of informational assets has always been a corporate requirement. These assets can be scaled in three main spheres, namely, people, organizational processes and technologies. The internet, the web, the broadcast of networks, and the growing presence of technology both in people's lives and in organizational contexts have caused profound transformations in the intrinsic processes that constitute personal and organizational routines. On the one hand, these changes provided by the technological progress have fostered competitiveness and decentralization; on the other hand, they require better management, control, security and protection for information and knowledge. This article presents the results of an investigation within information security realm, focusing on the human aspects of knowledge and information management related to security practices. Using a quality-quantitative approach, we identify behavioral actions and profiles of employees of a company in the field of healthcare, which reveal some connections with information security failures. We conclude that the human element is a relevant variable, even a critical one, for the management of information security in organizations.

KEYWORDS: Information Security. Information and Knowledge Management. Informational Behavior.

1 INTRODUCÃO

As demandas empresariais vêm de encontro à necessidade de se encontrar soluções estratégicas para os negócios. No universo empresarial, a concepção acerca do que vem a ser segurança vem evoluindo, e não mais se restringe apenas à questão técnica. Nessa perspectiva, a segurança da informação surge como recurso relevante, visto que busca atrelar ao negócio da empresa variáveis que influenciam na proteção de ativos informacionais. Essas variáveis são agora vistas como elementos integradores do negócio principal, pois a salvaguarda da informação e do conhecimento é

fundamental para o sucesso, competitividade e sobrevivência no mercado globalizado.

Advoga-se aqui a necessidade de contemplar, de forma integradora, os elementos “pessoas”, “processos” e “tecnologias” como variáveis que coexistem nas empresas e que precisam ser tratadas com equilíbrio e igualdade de condições no âmbito da gestão de segurança da informação (SVEEN, TORRES E SARIEGI, 2009).

A mudança para este viés de análise implica em abandonar a dependência exclusiva dos aspectos tecnológicos e voltar a atenção para a subjetividade inerente aos seres humanos, suas relações e seu comportamento nas organizações, uma vez que tal comportamento em muito influencia a gestão de segurança da informação. Colwill (2010) pontua que o excesso de confiança na tecnologia, sem a consideração de outros fatores também relevantes, pode levar a resultados desastrosos na gerência de ameaça interna à segurança muito importante: o elemento humano. Este elemento traz riscos à segurança da informação, uma vez que pessoas podem obter acesso legítimo a informações, conhecem a organização e sabem a localização de ativos valiosos.

O presente artigo descreve os resultados de uma investigação cujo enfoque é a identificação da interferência de aspectos humanos nas práticas de gestão da informação e do conhecimento concernentes à segurança da informação. Esses aspectos são, de fato, inerentes à condição humana: o comportamento das pessoas, suas relações e condutas afetam o ambiente empresarial em um espectro de níveis diversos em que a segurança da informação é necessária. Para conduzir a investigação, aplicou-se uma metodologia quali-quantitativa com o objetivo de identificar perfis e mensurar como as ações comportamentais dos colaboradores de uma empresa da área da saúde são geradores de falhas na segurança da informação. As conclusões deixam claro o quão crítico é o elemento “pessoas” na gestão de segurança da informação das organizações.

O artigo está dividido da seguinte forma: a seção 1 apresenta a abordagem gerencial para tratar a segurança da informação e o elemento pessoas; a seção 2 apresenta considerações acerca do que significa construir um comportamento seguro; a seção 3 discute processos de gestão baseado na educação e no aprendizado concernentes à segurança informacional; a seção 4 apresenta a metodologia de pesquisa e, finalmente, a seção 5 analisa os dados obtidos e apresenta conclusões e considerações finais.

2 SEGURANÇA DA INFORMAÇÃO E PESSOAS: UMA ABORDAGEM DE GESTÃO CENTRADA NO USUÁRIO

As empresas se organizam em mercados globais para manter a competitividade e seu padrão de trabalho.

A tecnologia é o catalisador que abastece de eficiência e eficácia as empresas. Entretanto, por mais sofisticada que seja uma solução tecnológica ela será apenas mais um elemento do processo de manter a competitividade da organização. Pessoas e processos são elementos críticos e somente uma gestão estratégica que leve em conta todos os componentes da organização – planejamento, ação efetiva e tratamento estratégico da informação – pode alcançar os níveis de competitividade que a empresa necessita.

Dessa forma, ao refletir sobre como os recursos humanos interferem na segurança da informação de uma organização, observa-se facilmente que o elemento "pessoas" é vulnerável. Esta vulnerabilidade se manifesta através de duas inter-dimensões, sendo que ambas interferem na segurança da informação e tornam o fator humano o elo mais fraco: em primeiro lugar, os colaboradores devem, idealmente, ter conhecimento suficiente sobre a segurança da informação para a efetiva implementação e manutenção dos controles de segurança, o que nem sempre ocorre; em segundo lugar, os colaboradores devem ter a atitude correta em relação à segurança da informação, mas as vezes eles não foram informados sobre como fazer isso (NIEKERK e SOLMS, 2008).

Esta primeira abordagem traz a reflexão a respeito da necessidade de transparência, gestão e comunicação eficaz no que diz respeito às diretrizes de

segurança da informação adotadas por uma empresa. Todos os elementos da organização devem estar envolvidos de forma sinérgica para que saibam lidar com as questões de segurança, desenvolvendo completude de ações e verdadeira conscientização no que concerne à necessidade de se salvaguardar os ativos organizacionais.

Kraemer, Carayon e Clem (2009) contribuem com essa perspectiva observando que os usuários não são necessariamente contrários a segurança, mas muitas vezes são incapazes de determinar as implicações de suas ações na segurança.

Este panorama remete à reflexão sobre como a falta de conhecimento gera condutas inapropriadas diante das ações de segurança da informação esperadas, uma vez que o agir corretamente se desenvolve exclusivamente a partir da prerrogativa do saber como agir. Por isso é importante que as organizações dediquem atenção à manutenção e compartilhamento de informações confiáveis para fins de gestão da informação e do conhecimento corporativo, bem como para um melhor entendimento das necessidades de seus usuários.

Os usuários da informação devem ser percebidos como aqueles que, não são apenas impulsionados a buscar informações para fins cognitivos, mas sim como entes que vivem e trabalham em ambientes sociais (como as empresas) e que, no contexto destes, criam suas próprias motivações para buscar informações e satisfazer suas necessidades (WILSON, 2006b). Este usuário da informação é definido, para esse estudo, como aquele que é fortemente dependente da informação e a utiliza com fins específicos, como por exemplo, com finalidade profissional (MEADOW,1992).

Esse processo de busca de informações segundo Marchionini (1998) é direcionado pela necessidade informacional do indivíduo. A extrema variedade de necessidades informacionais dos indivíduos torna complexa e difícil a tarefa de enumerá-las (ALLEN, 1996).

Choo (2006), complementando as reflexões de Marchionini (1998) e de Allen (1996), destaca que no âmbito do processo de busca e uso da informação o valor da mesma reside no relacionamento que o usuário constrói com determinada informação. Assim, vários elementos afetam os padrões de busca

informacional e o comportamento informacional como um todo, como por exemplo, a variedade de fontes de informação, os tipos diferentes de usuários, as necessidades e preferências dos usuários, dentre outros.

Nessa perspectiva, a escolha de fontes de informação por determinado usuário é orientada de acordo com suas preferências, necessidades, acessibilidade, ambiente, etc. Choo (2006) destaca, ampliando sua análise, que a escolha de uma fonte de informação é determinada pelo binômio custo (acessibilidade física e o custo psicológico) *versus* resultado (qualidade técnica e confiabilidade). Sugere ainda que as fontes de informação são classificadas nas seguintes categorias: internas e pessoais, internas e impessoais, externas e pessoais, e, externas e impessoais.

Pereira (2006) contribui para essa análise indicando que fontes estruturadas são sinônimas de fontes impessoais, fontes estas que são, na maioria das vezes, de caráter documental ou formal. Por outro lado, as fontes não estruturadas, que são sinônimas de fontes pessoais, se caracterizam por proporcionar a troca de informação entre pessoas.

Choo (2006) finalmente ressalta que as necessidades e os usos da informação devem ser analisados dentro da situação profissional, organizacional e social nas quais os usuários estão inseridos, haja vista que elas variam de acordo com a profissão ou o grupo social do usuário, suas origens demográficas e os requisitos específicos da tarefa que este usuário está executando.

Observa-se que nesse processo de necessidade e busca informacional, o recurso disponibilizado através das informações eletrônicas, estruturados em vários caminhos, vem se tornando um ambiente dominante. O engajamento entre a relação daquele que busca a informação com a rede mundial, com as bibliotecas digitais e com outras estruturas de informação se tornam a cada dia mais forte (WILSON, 2006c).

Com a presença cada vez mais marcante dos recursos tecnológicos no dia-a-dia, principalmente a internet, torna-se relevante destacar a análise de Pereira (2006), a qual inclui além das quatro categorias de fontes de informação mencionadas por Choo (2006), mais outras duas: as fontes eletrônicas e não eletrônicas.

Pereira (2006) afirma que as fontes eletrônicas são as informações obtidas através da internet, CD-ROM´s, bases de dados on-line, etc.; e, as fontes não eletrônicas são as informações em papel. Mesmo considerando a amplitude de possibilidades de busca de conteúdo pela internet, conclui que apesar das fontes eletrônicas serem as mais utilizadas, as fontes pessoais ainda são consideradas as mais relevantes e confiáveis.

Nota-se que visão de Pereira (2006) ratifica a de Barbosa (2002), a qual promove um estudo com o intuito de identificar as fontes informacionais para empresas. Nesse âmbito, apresenta estudo do qual participaram 91 profissionais brasileiros. A conclusão é que apesar dos vários aspectos evidenciados com o uso crescente da tecnologia, as pessoas continuam a ser as fontes mais utilizadas e aquelas vistas como as mais relevantes.

Por isso mesmo, o entendimento sobre necessidades informacionais de usuários perpassa pelo comportamento de busca da informação e resulta no reconhecimento de alguma necessidade percebida pelo usuário. Este comportamento pode ser determinado de várias formas, seja através de demandas do usuário sobre os sistemas formais (os sistemas de informação), pleitos sobre sistemas que podem desempenhar funções de informação agregada a uma função primária ou não primária e, finalmente, pela busca de informação através de outra pessoa, pela troca informacional (WILSON, 2006b).

Além da busca informacional, é o comportamento que evidencia as necessidades de informação a única base na qual se pode estabelecer julgamentos acerca da natureza da necessidade informacional e sua respectiva satisfação. Unindo essas perspectivas pode-se concluir que as necessidades informacionais são construtos explanatórios que ajudam a entender o comportamento informacional (ALLEN, 1996).

Esse pensamento nos faz perceber que para se construir um comportamento de segurança da informação em uma organização, será preciso interagir com elementos pertinentes à Ciência da Informação, e que esses elementos alimentam uma trajetória que se inicia com a necessidade de informação, passa pela busca informacional e termina com o comportamento informacional.

De fato, o comportamento de necessidade, busca e uso informacional é um processo de construção de significado. Essa construção de significado se dá quando o usuário cria significado a partir das informações encontradas, passando de um estado de incerteza e indefinição para a clareza e a confiança (CHOO, 2006).

3 A CONSTRUÇÃO DE UM COMPORTAMENTO SEGURO

Ao refletir sobre como as pessoas poderiam adotar um comportamento seguro, observa-se que é necessário ter esclarecimentos sobre o que vem a ser um comportamento seguro e sua relação com a segurança da informação e seus elementos como: minimização de riscos, proteção dos ativos informacionais, e, posicionamento para se preservar de ataques.

Andalécio e Souza (2008) contribuem com essa reflexão quando afirmam, a partir da leitura da obra de *Jean Piaget*, que o conhecimento tem como meta ou propósito específico ajudar a pessoa a adaptar-se ao ambiente.

Esse panorama demonstra que no ambiente corporativo, empregados intencionalmente ou por negligência, e muitas vezes devido à falta de conhecimento, são a maior ameaça à segurança da informação.

A conscientização das pessoas sobre a importância de um nível adequado de cooperação do usuário e do compromisso com a construção de conhecimento é preponderante, haja vista que sem tais contribuições, as técnicas de segurança são passíveis de má utilização ou má interpretação pelos usuários tornando-se assim ineficazes. Por esse motivo é que a segurança da informação depende tanto do conhecimento quanto da cooperação humana. A expectativa é que a falta de conhecimento pode, na maior parte dos casos, ser tratada através da educação; a falta de cooperação pode ser abordada através da promoção de uma sub-cultura de segurança da informação na organização (NIEKERK; SOLMS, 2008).

É compreensível que essas abordagens levem a reflexão sobre como os fatores relacionados à produção do conhecimento e à cooperação por parte das pessoas são elementos críticos à variável humana na gestão de segurança da

informação. Analogamente, elementos como compartilhamento de conhecimento, aprendizagem organizacional e gestão do capital intelectual trazem tônus à abordagem proposta e propiciam amplitude de visão e desenvolvimento de ações organizacionais abrangentes para gerir os recursos humanos.

Não obstante percebe-se o quanto as pessoas precisam ser encaradas como possíveis promotoras de risco no ambiente corporativo, pois através dessa percepção, mais rapidamente, as brechas de segurança geradas por essas pessoas podem ser entendidas e as devidas ações implementadas.

Nessa perspectiva, Marchionini (1998) ressalta que as ações reativas requerem a percepção de *inputs* de informações e o resgate de informações da memória, ou seja, percebe-se a situação através dos sentidos e automaticamente determinam-se reações de acordo com os modelos mentais existentes. Já as ações previamente pensadas (proativas) são conduzidas por planos, empregam *outputs*, a coleta da informação ativa e requerem síntese.

Complementando essa visão, Andalécio e Souza (2008) sugerem que a aquisição de conhecimento influencia os sistemas de educação e que a cognição modifica o comportamento do indivíduo através de aquisição de novas associações, informações, *insights*, aptidões, hábitos, etc. Assim, o processo de mudança de comportamento, na visão de Andalécio e Souza (2008), ocorre segundo o condicionamento respondente, o condicionamento operante e a observação. Verifica-se também a mudança de comportamento através da observação dos atos de outro indivíduo através de: aprendizagem por observação, aprendizagem vicariante, aprendizagem social, modelação ou imitação (ANDALÉCIO; SOUZA, 2008).

Outro ponto importante mencionado por Andalécio e Souza (2008) é que através do processamento da informação o indivíduo, aqui considerado o usuário da informação, avalia se o recurso empregado por ele na solução de um ou mais problemas foi suficiente e obteve sucesso ou não. Em caso de sucesso, ocorre o processo de reorganização do conhecimento e mudança de comportamento.

Percebe-se, com base no que foi discutido na seção anterior, que nas ações preventivas há um comportamento de busca informacional em fontes diversas para sanar determinada necessidade e que, quando se planeja com detalhes formas

para alcançar um objetivo, um conjunto de ações é proposta e modifica o comportamento informacional dos colaboradores.

Adverte-se, porém, que no caso de medidas corretivas, a base para as ações são os modelos mentais existentes. Essa visão ratifica mais uma vez a importância de se promover o desenvolvimento do conhecimento, da cooperação e da aprendizagem organizacional entre os colaboradores visando a disseminação de informações sobre segurança da informação. Essa disseminação de informações possibilita que a instrução seja considerada antes da necessidade de uma atitude corretiva.

Ressalva-se, inclusive, que os modelos de avaliação de riscos podem ajudar na tarefa de promover a produção do conhecimento, uma vez que eles podem ser vistos como mecanismos de aprendizado auxiliares no processo de aprendizagem organizacional. Fazendo uma correlação entre avaliação de riscos e aprendizagem organizacional, vale ressaltar que se a percepção de segurança através da avaliação de risco aumenta, a empresa aprende mais e, consequentemente a taxa de aprendizagem e o corpo de conhecimento em segurança da informação aumentam, reforçando a capacidade da empresa de detectar falhas de segurança e dos funcionários de agirem de forma mais consciente (SVEEN; TORRES; SARIEGI, 2009).

Em suma, pode-se dizer que o comportamento seguro é algo construído e deve estar dentre os objetivos das organizações. O processo de aquisição de conhecimento e de construção de significado é imprescindível para que as pessoas tenham um comportamento seguro, haja vista que, conforme já citado, o agir se desenvolve exclusivamente a partir da prerrogativa do saber como agir. É possível intervir de forma que determinada pessoa tenha um comportamento seguro a partir do momento que essa pessoa entenda o que quer dizer ter um comportamento seguro e consiga agir proativamente frente aos estímulos advindos do ambiente.

4 SEGURANÇA DA INFORMAÇÃO E GESTÃO DE PESSOAS: UM PROCESSO DE GESTÃO BASEADO NA EDUCAÇÃO E NO APRENDIZADO

Reunindo todos os aspectos discutidos até aqui, percebe-se que ao identificar as pessoas como causadoras de ameaças à segurança da informação e, diante da impossibilidade de se erradicar tal ameaça, a alternativa viável é avaliar e gerenciar continuamente os recursos humanos da empresa.

Colwill (2010) enumera alguns fatores característicos da ameaça humana interna no contexto corporativo: motivação, oportunidade e capacidade. A motivação virá dos recursos humanos internos à empresa e será conduzida pessoalmente por eles. Já a oportunidade e a capacidade serão proporcionadas aos novos colaboradores pela própria organização, seja através de acesso a informações para execução de suas atividades ou através de acesso não autorizado por parte de pessoas que agem dentro da organização. É importante que todos esses fatores sejam incluídos nas avaliações de ameaças internas.

É importante destacar que as organizações precisam equilibrar a acessibilidade à informação para que seus colaboradores executem seu trabalho com a aplicação de níveis adequados de controle e auditoria. Desta forma entende-se que todos os esforços para consolidar aspectos como lealdade, confiança e sensibilização das pessoas para as questões de segurança devem ser postos em prática. Todavia, um esforço adicional por parte da organização faze-se necessário de forma a tornar essas questões intangíveis mais acessíveis e compreensíveis na visão dos colaboradores (COLWILL, 2010).

Quando se sugere que gestão de segurança da informação é participante ativa do negócio da empresa, quer-se dizer que o olhar das corporações deve ser ampliado no sentido de ver que a informação como um ativo de valor, o qual gera competitividade no mercado globalizado. Esse ativo informacional é processado no ambiente organizacional e ganha valor agregado. As pessoas processam a informação, seja através dos sistemas de informação ou outros recursos, e por isso elas detém parte do conhecimento que constitui o ativo total.

Almeida (2007) ressalta que uma organização não possui apenas dados em formato digital, haja vista que existem informações sobre determinada empresa armazenadas fora de seus domínios (governo, fornecedores etc.). Assim, para proteger o ativo informacional que está disperso nos sistemas, fontes, pessoas e processos organizacionais, as empresas devem se atentar para o fato de que suas estratégias de atuação contemplem a necessidade prioritária de proteção dos ativos informacionais corporativos. Como consequência, os objetivos e o planejamento estratégico contemplarão ações nos níveis operacional, tático e estratégico da estrutura organizacional.

Muito se tem discutido sobre a correlação entre funcionários descontentes e ataques internos que resultam em ameaças à segurança. Essa questão merece cuidado especial uma vez que pode apenas estereotipar pessoas induzindo a erros de avaliação quanto aos elementos envolvidos, como por exemplo, dirigentes sindicais e funcionários com queixas verdadeiras. A NIAC (2008) *apud* Colwill (2010) não considera a existência de correlação direta entre os trabalhadores descontentes e as ameaças internas e, que a maioria dos funcionários descontentes nunca sequer imaginou uma ação que prejudicasse a empresa. Uma verdadeira análise de motivação para traição exige levantamento psicológico complexo e varia de indivíduo para indivíduo. Shaw et al. (1999) *apud* Colwill (2010) identificam seis características pessoais que tem implicações diretas para riscos de um potencial invasor malicioso:

- Falsa sensação de falta de reconhecimento e direito, resultando em desejo de vingança;
- Raiva e frustrações sociais, alienação, resistência à autoridade;
- Dependência do computador e solidão agressiva, desejo de explorar redes, quebrar códigos de segurança e desafiar os profissionais de segurança;
- Ética e flexibilidade sem inibições morais que impedem o comportamento malicioso;
- Redução de lealdade, quando o elemento se identifica mais com a sua profissão ou especialidade de computador do que com o seu empregador;
- Falta de empatia e descaso ou incapacidade de apreciar o impacto do comportamento dos outros.

Colwill (2010), ainda em sua interpretação de NIAC (2008), conclui que as pessoas que cometem ações mal-intencionadas a partir de privilégios que possuem têm uma experiência de causalidade ou mecanismo que afeta a motivação e conduz a traição. Essas experiências podem ser classificadas em três fontes principais: o descontentamento crescente; a contratação por entidades exteriores hostis ou grupos; e a infiltração de ator malicioso em uma posição de confiança.

Quando se cruzam esses elementos com o imperativo de desenvolver cooperação e conhecimento compartilhado nas empresas, levando ainda em conta variáveis intrínsecas à personalidade humana – oportunidade, motivação, capacidade e descontentamento – observa-se que mais do que nunca as organizações precisam de estratégias para lidar com os recursos humanos (BEAUTEMENT; SASSE, 2009).

As pessoas podem desenvolver sentimentos a partir de experiências e agir de forma a prejudicar a organização. Por isso é muito importante que as organizações ajam proativamente no desenvolvimento e incentivo de ações cooperativas entre os colaboradores e também entre a organização e seus colaboradores. Não obstante, existe a necessidade de se promover ações que venham a contribuir com a expansão e o compartilhamento de conhecimento nas empresas, de forma a criar consciência nas pessoas e aproximá-las da organização.

Cabe destacar a perspectiva dos colaboradores confiáveis que também se respaldam na reciprocidade: eles confiam e esperam, em contrapartida, também receber confiança, e por isso as organizações devem estar atentas para proporcionar esse equilíbrio. Agindo dessa maneira todos são beneficiados, uma vez que da parte dos colaboradores haverá o compromisso com a proteção das informações sensíveis da organização; e da parte da organização haverá esforços para fornecer algum tipo de proteção (WORKMANN, 2007).

A sinergia entre organização e colaboradores é primordial na manutenção de uma cultura organizacional que tem foco na segurança de ativos informacionais. Paralelamente, o desenvolvimento de ações cooperativas,

disseminação de conhecimento e aprendizagem organizacional são facilitadas pela sinergia entre as partes.

A conexão adequada entre empregadores e empregados é tão importante que, de forma geral, nota-se que as organizações não podem proteger a integridade, confidencialidade e disponibilidade das informações alocadas em ambiente de sistemas em rede, sem garantir que cada pessoa envolvida compreenda seus papéis e responsabilidades, bem como seja treinada para realizá-los (ALMEIDA, 2007).

Assim, um usuário deve estar ciente dos controles operacionais específicos, uma vez que a eficiência do processo depende de seu comportamento. Para garantir esse nível de conhecimento exigido, será necessária uma formação ostensiva, conscientização e programas educativos (NIEKERK; SOLMS, 2008).

A partir da percepção de que a segurança da informação não é apenas um problema de tecnologia, observa-se que, por parte das organizações, há uma concordância sobre a necessidade de mudança de comportamento dos funcionários visando alcançar níveis mais elevados de proteção em conformidade com suas políticas de segurança. Entretanto o caminho adotado para realizar esse objetivo é muitas vezes equivocado, pois na maior parte das vezes as empresas adotam somente uma postura de ameaça frente aos trabalhadores impondo sanções caso as políticas não sejam seguidas (BEAUTEMENT; SASSE, 2009).

A perspectiva abordada até o momento leva a crer que a eficiência na gestão dos recursos humanos, sob a ótica das necessidades de segurança informacional corporativa, está vinculada à relação que a organização estabelece com seu colaborador. Nesse sentido, todos os esforços para conscientizar esse colaborador, desenvolver a cultura de compartilhamento de conhecimento, colaboração e aprendizagem organizacional não funcionarão se a empresa adotar uma postura de ameaça frente aos funcionários e se guiar pela promoção da coação dos colaboradores.

Vale ressaltar que uma postura de medo, coação e ameaça é bem diferente da adoção de métodos de gestão como no caso das sanções e recompensas. Por isso, uma mudança de crenças e valores se dá a partir de resultados de processos

de aprendizagem com base no comportamento de sucesso. Assim, comentários, recompensas e sanções, são mecanismos de gestão que devem ser usados de forma correta a fim de garantir que os funcionários entendam o que seria um comportamento considerado bem-sucedido (NIEKERK; SOLMS, 2008).

Em sintonia com a necessidade de mudança do comportamento dos colaboradores, a educação aparece como uma opção e se caracteriza, frequentemente, como a única maneira de convencer funcionários e gerentes sobre a necessidade de fazer as coisas de forma diferente. Para uma mudança paradigmática na organização é vital ensinar os funcionários o que fazer, como fazer e porque isso deve ser feito de certa forma ou porque essa ou aquela conduta deve ser adotada (NIEKERK; SOLMS, 2008).

Everett (2008) contribui sugerindo que a formação dos funcionários e a sua educação são fatores preponderantes para se obter ou aumentar conscientização acerca do valor dos dados manipulados dentro da organização e, respectivamente, do papel de cada indivíduo na organização para salvaguardar este ativo. Por isso a conscientização deve ser um componente intrínseco da cultura organizacional e deve ser medido antes e depois de qualquer mudança promovida. As ferramentas utilizadas para tal medição são enquetes cujos resultados possam comprovar a compreensão acerca da mudança proposta e, mais diretamente, através dos pedidos de renovação de senha e diminuição de incidentes de acesso indevido ou não autorizado à empresa.

A ISO 1799 traz diretrizes relativas a educação de colaboradores, especificando que esta deve incluir requisitos de segurança, responsabilidades legais e controles corporativos, bem como treinamento no uso correto das instalações de processamento de informação antes que o acesso a informações ou serviços seja concedido.

Entretanto, a dificuldade de construir controles informais fortes, levou a uma espécie de compensação que se deu através da construção de controles formais muito fortes (políticas, normas, diretrizes etc.). Esse fato pode ser constatado pelo grande número normas de segurança de informação como, por exemplo, as normas ISO 1799 e COBIT. No entanto, não há como garantir a plenitude dos controles formais sem o desenvolvimento paralelo de controles

informais. As características particulares da cultura de cada empresa impõe adequações ao conjunto de normas de segurança no ato de sua implementação. Por este motivo há uma diferença entre o que está escrito nas normas e que é realmente praticado nas empresas (SVEEN; TORRES; SARIEGI, 2009).

O objetivo de fomentar comportamentos de segurança da informação faz com pessoas sejam favoráveis à proteção dos ativos de informação de acordo com as políticas da organização no que concerne à segurança da informação e com base no código de ética. O êxito dos comportamentos de segurança geraria maiores índices de comunicação de incidentes de segurança, a adesão a uma política de mesa limpa ou eliminação de documentos confidenciais (DA VEIGA; ELOFF, 2009).

Huang, Rau e Salvendy (2010), relendo o trabalho de Yenisey et al. (2005) o qual investiga como se dá percepção da segurança da informação, sugerem que tal percepção é o mecanismo através do qual uma pessoa avalia as ameaças à segurança da informação, o qual, por sua vez, determina sua resposta comportamental.

Em contrapartida identifica-se que alta carga de trabalho pode criar um conflito de interesses entre a funcionalidade e segurança da informação. Além disso, a alta carga de trabalho estão associadas ao erro humano durante uso dos sistemas (KRAEMER; CARAYON; CLEM, 2009).

Proteger as informações da organização é responsabilidade de todos os funcionários. Educação, formação e sensibilização são as mais eficientes medidas não técnicas disponíveis na perspectiva que relaciona o elemento humano e a segurança da informação. Requisitos de segurança devem ser integrados ao comportamento das pessoas como uma atividade normal, através de políticas claras e de educação. Muitos problemas de vazamento de informação confidencial provêm da ignorância e não da má-intenção. Além disso, falhas acidentais podem gerar grandes impactos.

Observa-se que em muitas empresas, a questão da segurança e da educação são quesitos obrigatórios, auditados sob a perspectiva legal. Um foco na mudança necessária é medir o comportamento da força de trabalho como parte do plano de desenvolvimento organizacional. A formação básica e as instruções

podem ser adotadas, mas a ênfase deve ser direcionada para a integração e a sensibilização sobre a segurança, bem como para a compreensão da cultura organizacional. Os colaboradores devem alterar seu comportamento a fim de proteger os bens e informações. Para conseguir este objetivo, além de aumentar a sensibilização dos funcionários, é preciso incorporar as necessidades de segurança aos valores culturais da organização. Para obter real eficácia em segurança, deve-se ir além de apenas seguir políticas de segurança, mas trabalhar num processo de construção de empatia, compreensão, apropriação e desenvolvimento de conhecimento acerca de situações que podem causar riscos à segurança, comportamentos e reações (COLWILL, 2010).

Assim, a forma pela qual a informação é processada pelo indivíduo, no grupo e consequentemente na cultura da empresa é fator de importante avaliação para solidificação de valores e paralelamente de criação de impressões marcantes nos colaboradores.

A cultura de segurança informacional, ou seja, percepções, atitudes e pressupostos que são aceitos e encorajados em uma organização, bem como o modo pelo qual as coisas são feitas em uma organização para proteger os ativos de informação, se desenvolvem como resultado da interação dos colaboradores com controles de segurança, tais como senhas, cartões de acesso ou software antivírus. Uma cultura de segurança informação, de fato, é a maneira pela qual as coisas são feitas na organização para proteger os ativos de informação (DA VEIGA; ELOFF, 2009). Kraemer, Carayon e Clem (2009) ressaltam que a perspectiva da cultura de segurança é multidimensional, incluindo governança da segurança, controle, coordenação, processos de segurança, apoio à gestão, participação e formação dos funcionários e conscientização dos colaboradores sobre segurança.

Abrindo o leque das dimensões de segurança informacional, observa-se que a questão educacional do colaborador no que concerne à segurança da informação deve ser referenciada não apenas no âmbito empresarial, mas também no que se refere ao comportamento dessa pessoa fora da organização (DA VEIGA; ELOFF, 2009).

Por isso a formação dos cidadãos é primordial para que se tenham atitudes conscientes frente a incidentes de segurança, independentemente do ambiente corporativo ou social. Conforme Workmann (2007), quando ocorre internamente o ato de percepção, as ações e reações podem ser alteradas e nesse caso o instrumento promotor da mudança é a comunicação persuasiva. Por isso mesmo, o fator persuasão é determinante do comportamento das pessoas frente a situações de ameaça. Com relação a desdobramentos da persuasão, três são os fatores emergentes: confiança, medo e compromisso.

Narita e Kitamura (2010) confrontam a questão da persuasão com a ação do que chamam de "agentes conversacionais". Nas conversas convencionais não existe um objetivo específico entre os participantes. Já nas conversas persuasivas, os agentes persuasivos ou conversacionais têm o claro objetivo de persuadir um usuário a mudar suas atitudes.

Vários ataques se concretizam quando invasores em potencial utilizam a aceitação de determinada mensagem junto ao usuário através elementos tais como credibilidade, simpatia ou um atrativo qualquer no remetente da mensagem, ou seja, utilizam uma rota periférica de persuasão. Existem algumas características que são vinculadas à rota periférica de persuasão e podem ser descritas como reciprocidade (compromisso normativo), consistência (compromisso de continuidade), prova social (comprometimento efetivo), simpatia (ganho de confiança), autoridade (geração de medo) e escassez (percepção da falta de certos itens) (WORKMANN, 2007).

Além da busca de sinais de comportamento adverso em potenciais invasores, a preocupação com ataques reais precisa sempre ser mantida. Isto envolve uma combinação de medidas processuais, de gestão de pessoas e desempenho em todos aqueles sob mandato de um gestor, incluindo os colaboradores terceirizados. Essa postura leva a uma relação mais estreita entre os requisitos de segurança e do negócio como um todo. Acredita-se em uma abordagem ativa em detrimento da reativa em ambos os elementos, gerentes e colaboradores. O foco não se resume em apenas recolher diferentes dados sobre o comportamento anômalo, mas também em coligir e analisar dados que podem determinar os padrões e os cursos de medidas corretivas (COLWILL, 2010).

Admite-se que a ameaça à informação privilegiada e à segurança da informação não pode ser totalmente eliminada, mas pode ser controlada, avaliada e gerenciada. Através da compreensão dos fatores humanos vinculados à segurança informacional, é possível obter uma melhor compreensão dos riscos reais que as organizações enfrentam no atual ambiente comercial global. A gestão da informação e do conhecimento deve ser eficaz nesse sentido. O uso informacional deve ser controlado, de forma que, qualquer comportamento anormal seja investigado e ações de contenção sejam postas em prática rapidamente.

5 METODOLOGIA DE PESQUISA E ANÁLISE DOS DADOS

Buscando entender a interferência do elemento humano na segurança da informação, realizou-se pesquisa em uma organização privada brasileira da área de saúde, no estado de Minas Gerais em Belo Horizonte (o nome não será divulgado a pedido da instituição). A população-alvo desta pesquisa foi constituída pelos funcionários do setor de tecnologia da informação da instituição.

O presente estudo seguiu as diretrizes da pesquisa *survey*, de forma que foram observadas várias características dos elementos de uma determinada população ou amostra, utilizando-se questionários ou entrevistas como instrumentos de pesquisa. A observação foi feita naturalmente e sem interferência do pesquisador. Foi escolhido o método quantitativo com a intenção de garantir a precisão dos resultados, evitar distorções de análise e interpretação, possibilitando uma margem de segurança quanto às inferências. A abordagem dessa pesquisa também se caracterizou pela exploração. Em termos mais técnicos, uma análise exploratória de dados consiste na busca de um padrão ou modelo que possa nos orientar em análises posteriores (BABBIE, 1999; RICHARDSON, 2007).

Para que se consiga entender a interferência do elemento humano na segurança da informação foi proposta uma amostragem por conveniência na qual foram questionados 35 funcionários da empresa já mencionada. Adotou-se um questionário estruturado, disponibilizado na Internet

(http://www.kwiksurveys.com) por tempo determinado. As respostas ao questionário foram armazenadas no próprio site, onde somente o pesquisador tinha acesso, sem identificação do respondente.

Os funcionários da empresa estudada foram convidados por seu gestor a participar da pesquisa. O *link* para responder ao questionário foi disponibilizado via e-mail e, pelo fato do elemento pesquisado ter sido selecionado por estar disponível no local onde a pesquisa estava sendo realizada, caracterizou-se como uma amostra não probabilística por conveniência. O universo a ser pesquisado era formado por 100 funcionários do setor de tecnologia da informação. Desses 100 funcionários convidados a participar da pesquisa, 35 responderam ao questionário, totalizando 35% de respostas completas.

O instrumento quantitativo de coleta de dados, o questionário, foi estruturado em duas partes. A primeira tinha por objetivo obter o perfil do entrevistado com relação a dados pessoais básicos, como sexo e escolaridade. A segunda parte, composta por 49 declarações, seguiu uma estrutura matricial associada uma escala de *Likert* (Likert, 1932).

A escala de *Likert* é uma escala de mensuração itemizada, também denominada de "escala multi-itens". Exige que os entrevistadores indiquem um grau de concordância ou discordância com relação a cada afirmação de uma série. A escala Likert possui as características de descrição, ordem e distância (Malhotra, 2012). É importante salientar que, neste trabalho, optou-se por manipular quatro itens, sem ponto neutro, conforme segue: (1) discordo totalmente, (2) discordo parcialmente, (3) concordo parcialmente, e, por fim, (4) concordo totalmente. A escala utilizada, segundo categorização de Malhotra (2012), é *balanceada* pois apresenta número igual de categorias favoráveis e desfavoráveis; e *forçada*, pois os entrevistados foram forçados a emitir uma opinião, não havendo a posição neutra, ou seja, para cada afirmativa o respondente tinha necessariamente que discordar ou concordar.

Nesse contexto, considerou que a análise poderia ser feita item por item ou calculando um escore total (somatório) para cada entrevistado, somando-se os itens. Para o somatório, as categorias atribuídas pelos respondentes a afirmações negativas, deveriam ser escalonadas em ordem inversa a da escala. Para uma

afirmação negativa, uma concordância traduziria uma resposta desfavorável. Ao cruzar dados, objetivava-se obter informações sobre os perfis e ações comportamentais dos colaboradores da empresa em questão, bem como a sua inter-relação com falhas de segurança da informação através de percentuais de dados quantificados.

Apresenta-se a seguir uma tabela composta de parte do questionário e da quantificação dos dados obtidos em cada pergunta respondida. Ressalta-se que nesse artigo é avaliado o elemento “pessoas” sob a perspectiva de seu entendimento acerca de questões de segurança informacional.

TABELA 1

DADOS ARENA PESSOAS

Questão número:	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
3	Você entende o que é segurança da informação	28	7	0	0
5	Você, dentro de suas atribuições e funções no dia-a-dia, se sente parte responsável pela segurança da informação praticada na instituição?	29	6	0	0
6	A partir das diretrizes que a instituição fornece sobre como agir seguramente, eu consigo entender como atuar e agir de modo a garantir a confidencialidade, disponibilidade e a integralidade dos dados com os quais trabalho.	9	21	3	2
7	Na minha percepção, a instituição investe mais em tecnologia para assegurar a segurança da informação corporativa e menos em treinamentos para as pessoas sobre segurança da informação e em políticas de segurança da informação.	14	14	5	2
9	Eu poderia dizer que as ações de segurança da informação em minha instituição geram conhecimento e promovem o aprendizado entre os colaboradores?	2	15	8	9
10	Frequentemente ocorrem interações sociais entre os colaboradores para discutir temas sobre segurança da informação.	0	3	7	25
15	Você fica ciente de todas as atualizações de avaliação de riscos de seu departamento, setor ou área?	5	10	9	11
17	Você sabe quem são as pessoas responsáveis pela segurança da informação na sua instituição?	18	11	1	5
22	Conheço os procedimentos e políticas de segurança da informação adotadas pela instituição na qual trabalho.	4	15	10	6
24	Costumo conversar com colegas sobre incidentes de segurança da informação ocorridos comigo ou que tenham ocorrido com eles ou com alguém que conheçamos.	6	12	8	9
25	Tenho oportunidade de sugerir ações de segurança da informação na instituição na qual trabalho.	10	10	4	11
30	Através das regras de segurança da informação disponibilizadas por minha organização, eu consigo entender qual deve ser o seu comportamento e como a empresa espera que eu aja com relação à segurança da informação.	5	12	12	6
35	Posso dizer que há envolvimento e apoio das gerências, diretorias e presidência no que concerne às ações se segurança da informação.	5	21	3	4
41	Posto em redes sociais fatos ou ocorrências que aconteceram na organização ou no meu setor para alertar amigos.	2	1	1	30
43	Sinto vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é segurança da informação de minha instituição.	1	2	3	28
44	Você poderia dizer que em primeiro lugar você dedica atenção à sua profissão e à especialidade do computador no qual trabalha para depois absorver os valores, missão e visão da empresa para a qual trabalha.	2	10	15	8

TABELA 1 - Continuação

DADOS ARENA PESSOAS

Questão número:	Perguntas do Questionário	Concordo Totalmente	Concordo Parcialmente	Discordo Parcialmente	Discordo Totalmente
45	Existem sanções e recompensas para corrigir ou bonificar o bom comportamento frente às ações de segurança da informação propostas pela instituição.	2	6	3	24
46	Sou treinado para ter um comportamento seguro.	4	8	6	17
47	Sei com clareza qual é o meu papel na segurança informacional da empresa.	9	10	12	4
48	Existem, na instituição na qual trabalho, programas de educação para formar pessoas com relação à segurança da informação.	2	6	11	16
49	As ameaças de segurança da informação que sofro determinam meu comportamento frente às situações que vivencio.	9	15	6	5
50	Avaliando a situação atual, sinto que o ambiente da empresa é seguro no que concerne às informações que nele são processadas.	7	15	7	5
51	A alta carga de trabalho vinculada à minha atividade prejudica minha percepção e ação com relação à segurança da informação.	5	15	9	6

O cenário obtido destacou que cerca de 80% dos respondentes entendiam o significado da segurança da informação e se sentiam parte responsável pela segurança informacional praticada na instituição. Mais de 70 % dos funcionários conheciam quem eram os responsáveis pela segurança da informação de sua empresa e afirmavam envolvimento do *staff* corporativo nas ações de segurança informacional. Entretanto, apesar dos respondentes entenderem o que significa segurança da informação, 60% do total de entrevistados informaram que compreendiam apenas parcialmente as diretrizes da empresa para, a partir delas, agir de forma a garantir a confidencialidade, integridade e disponibilidade dos dados a que tem acesso. Outros 50% de colaboradores afirmavam conhecer as políticas e procedimentos da organização no que concerne à segurança da informação.

Destarte, apesar dos colaboradores entenderem as regras, os procedimentos, as diretrizes e as políticas de sua organização, mais de 51% dos respondentes discordaram sobre o fato de que essas informações documentais eram suficientes para determinar um comportamento seguro por parte do usuário.

Paralelamente, os respondentes salientaram que as ameaças sofridas por eles determinavam seu comportamento nas situações vivenciadas em seu dia-a-dia, e, que o grande volume de atividades executados em sua rotina de trabalho prejudicavam sua percepção e ação no que concerne à segurança da informação.

A vertente da perspectiva tecnologicamente orientada continuava em voga na organização pesquisada. Observou-se que 80% dos respondentes concordavam que a empresa investia mais em tecnologia em detrimento de treinamentos e políticas. Essa abordagem tecnológica veio a ser ratificada quando mais 50% dos colaboradores pesquisados relataram que as ações de segurança da informação desenvolvidas na empresa não eram geradoras de conhecimento e não promoviam o aprendizado organizacional. A questão da aprendizagem organizacional realmente era um aspecto a se desenvolver nessa organização, haja vista que mais de 70% dos funcionários relataram que não ocorriam interações sociais onde seriam discutidos temas de segurança da informação.

Apesar dessas constatações, a maior parte dos respondentes afirmou que a empresa desenvolvia programas educacionais visando formar pessoas com relação à segurança da informação. Concomitantemente, mais de 50% desses respondentes afirmaram haver abertura por parte da empresa para a sugestão de ações de segurança informacional. Todavia, essa aprendizagem era um tanto prejudicada, uma vez que, na falta de um programa formal de gestão da informação e do conhecimento, as sugestões não eram incorporadas às ações de segurança da informação como deveriam ser.

Doravante, por mais que os respondentes relatassem a falta de interações sociais, mais de 50% dos entrevistados afirmaram conversar com outros colegas sobre incidentes de segurança ocorridos consigo ou com algum conhecido. Essa interação entre colegas é uma ação que promove troca de conhecimento, entretanto, pareceu ser isolada e não incentivada pela empresa. Vale ressaltar que essas interações (conversas) não ocorriam via rede sociais, conforme mais de 90% das respostas.

Para finalizar, destaca-se que mais de 50% dos colaboradores relataram não estar cientes das avaliações de atualizações de riscos, prejudicando assim o corpo de conhecimento e aprendizado da empresa.

6 CONSIDERAÇÕES FINAIS

A perspectiva de segurança da informação desenvolvida nesse artigo relatou questões envolvendo as fontes de informações corporativas, as necessidades de uso da informação por usuários corporativos e as diretrizes corporativas que permeiam toda a vida da organização. Descreveram-se brevemente as variáveis envolvidas na criação de um comportamento seguro para o usuário da informação, bem como a segurança da informação sob o ponto de vista da gestão de recursos humanos. Dessa forma, concluiu-se que a importância da educação e do aprendizado organizacional nas questões de segurança da informação é fundamental. Finalmente, foram apresentados resultados parciais de uma pesquisa em andamento, enfatizando pessoas e segurança da informação em uma empresa do ramo de saúde.

Enquanto muitas iniciativas relativas à segurança da informação são conduzidas por departamentos de tecnologia da informação, os verdadeiros motivos das falhas continuam permeando toda a organização. As pessoas estão presentes em todos os locais, seja como usuários ou como desenvolvedoras de sistemas de informação, e cabe a elas atentar para políticas e diretrizes organizacionais criadas para manter a segurança. À organização e ao seu corpo gerencial, cabe tornar tais políticas e diretrizes conhecidas e valorizar sua adoção.

Empresas de saúde, como a mencionada nesse artigo, a qual se submeteu a pesquisa, são organizações em que a informação confidencial de pessoas, de caráter médico, circula livremente em sistemas de informação. Tal disseminação ocorre intra e extra organização, uma vez que outras empresas parceiras comerciais e seus colaboradores tem acesso a informações sigilosas relativas à saúde de terceiros. Essa constatação se torna ainda mais critica em instituições de saúde pública, que muitas vezes lidam com a produção de informação médica através da oferta de serviços de saúde. Nesses casos, cabe uma abordagem, como a sugerida no âmbito do presente trabalho, que extrapole as fronteiras dos departamentos de tecnologia da informação.

Da avaliação dos dados parciais apresentados na seção 5, foi possível concluir que o elemento “pessoas” é uma variável crítica na gestão de segurança informacional nas organizações. As políticas de informação devem ser acessíveis

aos funcionários e passíveis de execução. Com relação à tecnologia, é valida a continuidade dos investimentos, mas eles devem ser equilibrados com o desenvolvimento de controles informais (envolvendo as pessoas) e controles formais (envolvendo políticas e processos) para que haja uma gestão de segurança informacional efetiva e eficaz.

REFERÊNCIAS

ALLEN, B. L. *Toward a user-centered approach to information systems.* Los Angeles: Academic Press, 1996.

ALMEIDA, M. B. Aplicação de Ontologias em Segurança da Informação. *Fonte*, Belo Horizonte, v.4, n.7, p.75-83, 2007.

ANDALÉCIO, A. L.; SOUZA, R. R. Ciência Cognitiva e Ciência da Informação: Paralelos. *Inf. Inf.*, v.13, n.1, p.72- 80, jan./jul.,2008.

BABBIE, E. *Métodos de Pesquisa Survey*. Belo Horizonte: UFMG, 1999.

BARBOSA, R. R. *Inteligência Empresarial*: uma avaliação de fontes de informação sobre o ambiente organizacional externo. Disponível em: <http://www.dgz.org.br/dez02/Art_03.htm>. Acesso em:10 dez. 2011.

BEAUTEMENT, A.; SASSE, M.A. (2010). The Compliance Budget: The economics of user effort in information security. *Computer Fraud & Security*, v.29, n.10, P. 8-12, 2009.

CHOO, C. W. *A organização do conhecimento*. São Paulo: SENAC, 2006.

COLWILL, C. *Human factors in information security*: The insider threat & Who can you trust these days? Disponível em: <http://www.infosec.co.uk/files/istr_article_on_risk.pdf>. Acesso em: 22 jan. 2010.

DA VEIGA, A.; ELOFF, J.H.P. A framework and assessment instrument for information security culture. *Computer & Security*, v.29, p.196-207, 2010.

EVERETT, C. Cover Story: Education, Education, Education. *Infosecurity*, n.6, v.5, p. 14-18, 2008.

GHERNAOUTI-HÉLIE, S. *An inclusive information society needs a global approach of information security*. Disponível em: <http://ieeexplore.ieee.org/ >. Acesso em: 15 jan. 2009.

HUANG, D. L.; RAU, P. L. P.; SALVENDY, G. Perception of information security. *Behaviour & Information Technology*, v.29, n.3, p. 221-232, 2010.

KRAEMERA,S.; CARAYON, P.; CLEM, J. Human and organizational factors in

computer and information security: Pathways to Vulnerabilities. *Computer & Security*, v.28, p. 509-520, 2009.

MALHOTRA, N. K. *Pesquisa de Marketing*: Uma Orientação Aplicada. Porto Alegre: Bookman, 2012.

MARCHIONINI, G. Digital Library Research and Development. *Encyclopedia of Library and Information Science,* v.63, p.611-19, 1998.

MEADOW, C. T. *Text information retrieval systems*. San Diego: Academic Press, 1992.

NARITA, T.; KITAMURA, Y. Persuasive Conversational Agent with persuasion tactics. *Lecture Notes on Computer Science*, v. 6137, p.15-26, 2010.

NIEKERK, J.F.V.; SOLMS, R.V. Information Security Culture: A management perspective. *Computer &Security*, v.29, n.4., p.476-486, 2010.

PEREIRA, F. C. M. *Uso de fontes de informação: um estudo em micro e pequenas empresas de consultoria de Belo Horizonte*.155f. Mestrado em Ciência da Informação – Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2006.

RICHARDSON, R. J. *Pesquisa social:* métodos e técnicas. São Paulo: Atlas, 2007.

SVEEN, F. O.; TORRES, J. M.; SARRIEGI, J. M. Blind Information Security Strategy. *International Journal of Critical infrastructure Protection*, v.2, p.95-109, 2009.

WILSON, T.D. Revisiting user studies and information needs. *Journal of Documentation*, v.62, p.680-684, 2006b.

WILSON, T.D. On user studies and information needs. *Journal of Documentation*, v.62, p.658-670, 2006c.

WORKMANN, M. Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of American Society of Information Science and Technology*, v.59, n.4, p. 662–674, 2007.