SEGURANÇA DA INFORMAÇÃO: UMA INVESTIGAÇÃO NA PERSPECTIVA DO USUÁRIO DE SISTEMAS DE INFORMAÇÃO CORPORATIVOS EM UMA ORGANIZAÇÃO DE SAÚDE

Luciana Emirena dos Santos Carneiro
Escola da Ciência da Informação, Universidade Federal de Minas Gerais
Avenida Antônio Carlos, 6627 – Campus Pampulha – Belo Horizonte - MG

Maurício Barcellos Almeida
Escola da Ciência da Informação, Universidade Federal de Minas Gerais
Avenida Antônio Carlos, 6627 – Campus Pampulha – Belo Horizonte - MG

RESUMO

Questões que envolvem Segurança da Informação sempre estiveram dentre as preocupações das organizações. Com o advento da Internet, a disseminação da informação foi amplamente incrementada. Sistemas de informação que antes trabalhavam isoladamente passaram a se comunicar facilmente com outras organizações, como por exemplo, sistemas de informação de parceiros comerciais ou do governo. Essa facilidade de comunicação e disseminação da informação trouxe benefícios, mas tem exigido novas estratégias para lidar a questão da segurança da informação. No presente artigo, propõe-se uma investigação sobre segurança da informação do ponto de vista da percepção do usuário de sistemas de informação corporativos. Apresentam-se resultados de pesquisa qualitativa realizada em organização da área de saúde e discute-se a relação entre o elemento humano e a segurança da informação no contexto organizacional. Espera-se que esse trabalho promova melhor entendimento de questões que permeiam a segurança da informação, não apenas do ponto de vista tecnológico, mas a partir do ponto de vista das falhas causadas por pessoas.

PALAVRAS-CHAVE

Segurança da Informação; Comportamento Informacional; Gestão da Informação

1. INTRODUÇÃO

A disponibilidade da informação é um atributo da Sociedade da Informação, que traz consigo inúmeros benefícios e grandes preocupações, como por exemplo, a necessidade segurança dos ativos informacionais.

A evolução dos sistemas de informação possibilitaram às empresas ganhos com mobilidade, inteligência e real capacidade de gestão. O aumento da competitividade e da descentralização promovido pelos avanços tecnológicos gera a necessidade de gestão, controle, segurança da informação e a proteção do conhecimento crítico (Sianes, 2005). As empresas demandaram por tecnologias que garantissem aos seus negócios a confidencialidade, integridade e disponibilidade, fazendo com que a segurança da informação passasse a ser uma estratégia de gestão da informação (Wylder, 2004; Koskosas, Charitoudi & Louta, 2008; Kraemer, Carayon & Clem, 2009; Ghernaouti-Helie, 2009; Colwill, 2010).

Na atualidade, os investimentos em segurança da informação são crescentes, como de fato as tecnologias da informação conseguem solucionar parte do problema diminuindo as ameaças físicas ou virtuais frente a pessoas ou informações que estas possuem. Almeida (2007) ratifica esse posicionamento, afirmando que a expressão "segurança da informação" representa um conceito amplo que, geralmente, nas empresas e instituições, está associada a sistemas informatizados e aos dados que estes manipulam.

Em contrapartida observa-se que por mais investimentos que se faça em segurança, se o elemento humano não for devidamente considerado, falhas de segurança ocorrerão (Colwill, 2010). Solms (2008) ressalta que qualquer investimento em tecnologia não terá a eficiência esperada se os usuários não obtiverem

uma consciência de Segurança Informacional. Nesse sentido, busca-se nesse artigo mudar o viés de análise em relação às pesquisas que enfatizam aspectos tecnológicos da segurança da informação, focando na subjetividade inerente aos seres humanos, suas relações e seu comportamento informacional nas organizações. O problema de pesquisa aqui delineado diz respeito a como os incidentes de segurança da informação envolvem pessoas. Apresentam-se resultados de pesquisa conduzida em organização de saúde brasileira, a qual lida com dados confidenciais de clientes. Buscou-se entender qual é a percepção dos usuários de sistemas de informação em relação à segurança da informação e em relação ao tipo de falha que podem causar, independentemente de ações de cunho tecnológico. Espera-se identificar potenciais falhas de segurança da informação ocasionadas por pessoas para explorar as circunstâncias nas quais esses incidentes de segurança ocorrem e, consequentemente, poder reduzir custos financeiros com a perda de informações sigilosas, ganhar competitividade, além de reduzir ameaças, vulnerabilidade e riscos nas empresas.

O restante do presente artigo está organizado conforme segue. Na seção 2 apresenta-se uma breve revisão de literatura que discute as várias facetas da segurança da informação no contexto organizacional. Na seção 3, após uma breve descrição da pesquisa realizada, apresentam-se e discutem-se os principais resultados obtidos de pesquisa sobre segurança em organização de saúde. Finalmente, a seção 4 traz conclusões e perspectivas de trabalhos futuros.

2. SEGURANÇA DA INFORMAÇÃO E TECNOLOGIA: PERSPECTIVAS

No âmbito e na variedade dos sistemas de informação é que a informação é processada no ambiente organizacional.

O propósito de um sistema de informação, segundo Buckland (1991), é esclarecer os questionamentos que venham a surgir e despertar a curiosidade. Um sistema de informação é um recurso para a investigação e um veículo para procurar informar pessoas sobre determinado assunto. Por esse motivo, um sistema de informação é proposital. Dependendo do valor de cada usuário, pode-se concordar ou discordar com um determinado propósito, mas os serviços de informações são baseados em um tipo de escopo mesmo que eles sejam caracterizados como partidários, altruístas, frívolos ou ineficazes. A característica de uma gestão eficaz de um sistema de informação é o esforço contínuo para tornar os recursos de informação disponíveis no momento e no local nos quais forem necessários.

Nesse sentido, é importante destacar que a necessidade e uso da informação são determinados pelo usuário e ele utiliza os sistemas de informação para satisfazer suas necessidades informacionais. O ato de informar, segundo Allen (1996), envolve tanto uma atividade realizada quanto um processo vivenciado por alguém. Sendo que, na perspectiva do usuário, a informação é algo que acontece com este usuário, ou seja, pessoas se informam ou informam alguém.

Complementar a essa abordagem, destaca-se a contribuição de Ingwersen (1992) que coloca que o conceito de informação deve incluir o processo no qual o conhecimento do informante é transformado pelo ato da comunicação e, da parte de quem busca a informação, o conhecimento é transformado pelo processo de percepção, avaliação, interpretação e aprendizado.

As duas perspectivas apontadas são arcabouço para discutir a definição de sistemas de informação apontada pelos dois autores Buckland (1991) e Allen (1996). O primeiro aponta que os sistemas de informação usados por seres humanos são sistemas abertos e complexos, que interagem com outros sistemas de informação ao redor do mundo. Adicionalmente, outro aspecto importante e relevante é o fato desses sistemas terem habilidade de responder a mudanças, de adaptar seus ambientes e manter a estabilidade para sobreviver. Já o segundo autor destaca os sistemas de informação como a junção de um ou mais dispositivos de informação que promovem acesso a um ou mais repositórios de conhecimento, além de se constituírem de ações através de mecanismos nos quais pessoas podem informar outras ou se informarem.

Efetivamente, trata-se de definições complementares, uma vez que apontam abordagens concernentes ao ambiente e seu dinamismo no mundo globalizado, aos usuários, suas necessidades e possibilidade de acesso a informações através das tecnologias num curto espaço de tempo e, por último, às informações que se confirmam como ativo de valor, sendo artefato de busca dos usuários e item de ação por parte das tecnologias.

Complementar a essa visão, Marchionini (1998) ressalta que infraestruturas de informação se desenvolvem à medida que os usuários da informação ganham conhecimento acerca dos fatores condutores

da busca de informações e também das habilidades para gerenciar esse processo de busca informacional. Desta forma, entender qual o conhecimento e as habilidades necessárias em ambientes manuais e eletrônicos levará a melhores projetos para futuros sistemas de informação e melhores treinamentos, tanto para profissionais quanto para usuários.

As reflexões sobre o elemento sistemas de informação e as variantes que o compõem apontam para o paradigma da tecnologia da informação que contextualiza a sociedade da informação e as empresas como parte da sociedade, sob a perspectiva tecnológica. Nesse sentido, Castells (2000) aponta que as tecnologias são desenvolvidas para agir sobre a informação e que essa informação é elemento presente tanto no contexto coletivo quanto individual, sendo moldado pelo *blogs, facebook, twitter, youtube* novo meio tecnológico. Esse novo meio tecnológico traz consigo a lógica das redes como fator unificador de sistemas ou conjunto de relações, sendo preponderantemente flexível. Essa característica de flexibilidade e sistematização em redes propicia a convergência das tecnologias para um sistema integrado e global.

As características de flexibilidade e de integração das informações em sistemas globais apontam para uma mudança de costume dos indivíduos. As pessoas demandam por tecnologias e essas tecnologias passam a ficar cada vez mais presentes na vida dos cidadãos. Nesse sentido, as novas tecnologias vêm mudando as atitudes sociais, tornando os dados e comunicações móveis cada vez mais disponíveis e de fácil uso.

Por isso, é importante entender o conceito de tecnologia da informação. A técnica denota o caminho de como fazer algo e a tecnologia pode ser descrita como o recurso físico que serve como ferramenta para realizar algo. Assim, as tecnologias da informação podem ser delineadas como aquelas utilizadas para "manejar" a informação (Buckland, 1991).

A totalidade desta conjuntura faz perceber a incontestável relação entre tecnologia e sociedade. Entretanto, é respeitável perceber, através da análise pela ótica dos recursos humanos no âmbito dos sistemas, redes e tecnologias da informação, que a tecnologia é projetada uma vez que é implementada e operada por pessoas. Assim, é o fator humano que determina as formas como usamos sistemas de informação ou o uso indevido destes (Lacey, 2009).

Analogamente, faz-se notar que os sistemas de segurança da informação são desenvolvidos visando minimizar riscos decorrentes de acesso não autorizado e posse de informação e, nessa perspectiva na qual o ativo são os dados, a estratégia é garantir às bases de dados segurança através dos critérios de integridade, confidencialidade e autenticidade (Koskosas, Charitoudi & Louta, 2008).

Os autores Sveen, Torres & Sariegi (2009) esclarecem que controles técnicos são ferramentas de hardware e software, tais como dispositivos biométricos, bloqueios, software antivírus, firewalls etc. que restringem o acesso a prédios, sistemas de computador, programas e etc. a fim de evitar seu uso indevido. Já Colwill (2010) contribui trazendo uma especificação dos controles técnicos contra invasores não somente externos, mas também internos à empresa, e diz que estes devem incluir, minimamente, criptografia, controle de acesso, privilégio mínimo, acompanhamento, auditoria e relatórios. Já Kraemer, Carayon & Clem (2009) enfatizam a utilização de métodos específicos de segurança da informação, como os *smart cards*, dispositivos biométricos, software de criptografia PGP 5.0, senhas, segurança nos navegadores web básico, indicadores de identificação, análise das aplicações de desktop, tais como o Word 2007 e Internet Explorer.

Hoje em dia, as pessoas usufruem dos benefícios do uso de computadores e da Internet para a comunicação e para fazer negócios. Por isso, o problema da segurança da informação está se tornando cada vez mais relevante (Huang, Rau & Salvendy, 2010). Muitas abordagens foram desenvolvidas para auxiliar na gestão da segurança da informação e na limitação de ocorrências de incidentes e violação de segurança.

A maioria dos controles desenvolvidos implica em *check lists*, análise de risco, avaliação e métodos. Entretanto, há a necessidade de se questionar essas abordagens com foco estreito, soluções tecnicamente orientadas que ignoram os aspectos sociais dos riscos e da estrutura informal de organizações (Koskosas, Charitoudi & Louta, 2008). Apesar de toda evolução nos controles técnicos, promovida por mudanças tecnológicas constantes, as organizações devem ter em mente que sua maior vulnerabilidade é seu colaborador, por isso as empresas devem enfocar os fatores humanos, suas percepções e expectativas, em detrimento da objetividade inerente à tecnologia (Colwill, 2010).

Nessa vertente, Koskosas, Charitoudi & Louta (2008) ressaltam a importância dos cursos de educação e formação de membros para adequada percepção dos riscos em matéria de segurança e pontuam que esta percepção reflete no sucesso global dos projetos de segurança de informação em sistemas. Compartilhamento de informações e experiências sobre o tema segurança também foram ressaltados e os autores concluem enfatizando que cultura e estabelecimento de metas são inter-relacionados e podem ter um efeito sobre sistemas na gestão de segurança da informação.

A ameaça dos empregados por negligência ou ignorância frente a questões de segurança é susceptível de ser exacerbada quando as pessoas fundem trabalho e vida pessoal. O Centro Nacional de Computação afirma que os indivíduos têm dificuldade em ter uma verdadeira fronteira entre o trabalho e a vida pessoal e que eles gastam tempo compartilhando informações pessoais e profissionais em sites e redes sociais com a "inocência e confiança". Esta constatação deixa o colaborador e, consequentemente, a organização abertos a uma gama de downloads de pornografia e música e a uma variedade de ataques de *malware*. Existe uma crescente pressão sobre as empresas para dar liberdade maior aos colaboradores, entretanto essa medida precisa do aparato tecnológico apoiado a regras claras e regulamentos definidos para prevenir uma descida ao caos (Colwill, 2010).

Um ponto interessante constatado na pesquisa de Colwill (2010) são as falhas de segurança geradas pelo uso de dispositivos de dados portáteis por parte dos "*insiders*" da organização, facilitando assim o comprometimento da informação da organização. Fazendo uma leitura da pesquisa de Kavanagh (2006), Colwill (2010) observou que 89% dos trabalhadores usavam dispositivos portáteis de cunho pessoal na rede das empresas nas quais trabalhavam pelo menos uma vez por semana e que mais da metade das empresas pesquisadas do Reino Unido não tinham controles para gerenciar o uso de dispositivos de mídia removível. Paralelamente, pessoas que trabalhavam em uma empresa financeira em Londres carregavam livremente CDs nos sistemas da empresa apesar das orientações e advertências. O fato é que a política de segurança, os controles, as orientações e os treinamentos não recebem prioridade de ação, alteração e atualização por parte das empresas.

Através da gestão da segurança, vê-se que as atuais abordagens gerenciais não atendem requisitos de transparência e controle de segurança. Fica a necessidade das tecnologias serem menos vulneráveis para diminuir o número de potenciais ameaças que podem ser desenvolvidas (Ghernaouti-Helie, 2009) e, paralelamente, vale ressaltar a necessidade de uma conscientização prévia sobre questões da segurança da informação, uma vez que se constatou que a referida "consciência" sobre questão de segurança da informação, na maioria dos casos, não ocorreu com a introdução de novas tecnologias, mas sim através de incidentes vivenciados após a sua introdução (Sveen, Torres & Sariegi, 2009). Conforme afirmam Kraemer, Carayon & Clem (2009), a tecnologia e segurança da informação têm se concentrado em soluções tecnológicas para evitar vulnerabilidades e ataques, entretanto essas áreas precisam se relacionar, através de uma abordagem sócio-técnica, com aspectos humanos e organizacionais, uma vez que estes corroborarão diretamente na eficácia de outros sistemas críticos, tais como segurança e redução de incidentes.

3. MÉTODOS E RESULTADOS

Buscando entender a interferência do elemento humano na segurança da informação, uma pesquisa foi realizada em uma organização privada brasileira na área de saúde do estado de Minas Gerais, localizada na cidade de 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.

Trata-se de uma pesquisa quali-quantitativa e exploratória, cujos meios de investigação são a pesquisa de campo e o estudo de caso. No que concerne ao raciocínio lógico empregado na pesquisa, ele pode ser caracterizado como dedutivo.

Desenvolveu-se um questionário estruturado com base em um conjunto de variáveis que compõe cada arena – pessoas, processos e tecnologias previamente levantadas na literatura. Esse instrumento quantitativo foi aplicado através de link encaminhado ao e-mail dos colaboradores componentes da amostra por conveniência, na instituição pesquisada. Foram obtidas 35 respostas ao questionário, sem identificação do respondente, que foram armazenadas no site http://www.kwiksurveys.com/, ao qual somente o pesquisador teve acesso. Ressalva-se que os instrumentos tiveram como característica o anonimato, de modo que não se corresse o risco de obter uma análise individual do colaborador que venha a prejudicá-lo, no sentido de sanções e/ou mesmo demissões. Outra característica importante foi a não interferência do pesquisador na condução das perguntas junto aos respondentes.

O instrumento quantitativo de coleta de dados denominado questionário, foi estruturado em duas partes. A primeira com o objetivo de obter o perfil do entrevistado, com relação ao sexo e escolaridade. A segunda parte, composta por 49 afirmativas, seguiu uma estrutura matricial com uma escala tipo 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 cada uma de uma série de afirmações. Os dados geralmente são tratados como intervalares, assim, a escala Likert possui as características de descrição, ordem e distância (Malhotra, 2012). É importante salientar que, neste trabalho, optou-se por trabalhar com quatro itens, sem ponto neutro, sendo: (1) Discordo totalmente, (2) Discordo parcialmente, (3) Concordo parcialmente, e, por fim, (4) Concordo totalmente. A escala utilizada, segundo categorização de Malhotra (2012) pode ser classificada como 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.

Cabe esclarecer que a pesquisa foi planejada como pesquisa quantitativa, o que explica o uso de variáveis estatísticas na descrição da pesquisa. Entretanto pela dificuldade em conseguir, nessa etapa da pesquisa, uma amostra de significância quantitativa, optou-se por apresentar análises de natureza qualitativa.

No restante da presente seção, apresentam-se os resultados conclusivos obtidos, além de inferências sobre esses resultados que nos permitiram visualizar os cenários de utilidade no contexto da segurança da informação organizacional. Propõem-se então cruzar as respostas das perguntas do instrumento de coleta de dados primários e fazer análises.

A primeira parte do questionário continha questões relativas ao entendimento do colaborador sobre o significado de segurança da informação e, na sequência, seu sentimento como forma de se reconhecer como parte responsável pela segurança da informação na instituição pesquisada. As respostas para esses dois questionamentos receberam 100% de concordância total da parte dos participantes. Destarte, a discrepância começa a aparecer quando os colaboradores são questionados sobre suas capacidades de identificar as atuais medidas que estão sendo tomadas em relação à segurança da informação na instituição, quando questionados sobre as atuais medidas que estão sendo tomadas em relação à segurança informacional na instituição na qual o participante trabalha, 57% afirmam que conseguem identificar essas medidas e 43% afirmam que não conseguem identificar essas medidas. A partir desse resultado, cabe uma análise: como entender o que é segurança da informação e se sentir parte dela sem haver uma maioria expressiva que compreende as ações que estão sendo desenvolvidas pela empresa como corroborativas à gestão de segurança informacional na organização na qual trabalham?

Buscando entender com clareza como os colaboradores compreendem seu papel na segurança informacional da empresa, os novos dados obtidos indicam que pouco mais da metade dos respondentes (55%) concordam que sabem com clareza qual é o seu papel, embora 34% deste total concordam parcialmente com a afirmativa, ou seja, em mais da metade dos concordantes ainda há dúvidas.

Doravante, quando questionados sobre os responsáveis pela segurança informacional da empresa, 77% sabem quem são essas pessoas, sendo que 51% sabem com total certeza (concordo totalmente). Complementar a essa reflexão está o fato de que 43% dos respondentes concordam que a segurança da informação é responsabilidade do setor de tecnologia da informação e 57% discordam da afirmativa.

Nota-se que um número muito alto de pessoas acredita na abordagem técnica às questões de segurança da informação e talvez seja esse um dos motivos pelos quais os colaboradores não consigam identificar com clareza seu papel na segurança informacional da organização. Apesar de saberem com lucidez quem são os responsáveis pela segurança informacional corporativa, eles não conhecem com a mesma transparência as atuais medidas em vigor na instituição no que concerne à segurança da informação.

Um cenário com forte fundamentação na abordagem tecnológica não poderia ter outro resultado, ou seja, pessoas se estruturando totalmente nas tecnologias e fazendo delas a solução cômoda para todos os problemas de insegurança informacional.

Avaliando um pouco mais a fundo a percepção dos colaboradores com relação aos investimentos que são feitos pela empresa, sendo um montante maior para tecnologias e menor para treinamentos de pessoas no que concerne à segurança da informação corporativa, os resultados demonstraram que 80% dos entrevistados, têm a percepção de que a instituição investe mais em tecnologias do que em pessoas para garantir a segurança da informação empresarial. Quando são questionados se são treinados para terem um comportamento seguro, mais de 65% dos respondentes afirmam que não, observando-se que 50% deles tem total segurança de sua resposta (discordo totalmente). Esse parecer vem a se ratificar um pouco mais à frente no questionário, quando se pergunta aos colaboradores se existem na instituição programas de educação para formar pessoas, no que concerne à segurança da informação e 77% dos respondentes afirmam que não. Outro ponto importante de se mencionar é que 45% dos respondentes discordaram totalmente da afirmativa,

ratificando que na organização não se investe na formação do colaborador sob o aspecto da segurança informacional.

Respectivamente, quando os participantes foram questionados se as ações de segurança da informação na instituição geram conhecimento e promovem o aprendizado, e, se ocorrem interações sociais entre eles e demais colaboradores para discutir temas sobre segurança da informação, as respostas obtidas destacam mais de 90% de discordância, nenhuma resposta que concordasse totalmente e pouco mais de 8% que concordam parcialmente, levando os pesquisadores a traçar um cenário no qual quase nunca ocorrem interações sociais com o objetivo de discutir a temática segurança da informação, ou seja, a instituição não tem aproveitado as ocorrências (ou fatos) do dia-a-dia para discutir de forma integrativa ações de segurança informacional.

O primeiro fator direcionador de comportamento seguro é entender se os colaboradores conhecem e compreendem as políticas, procedimentos, normas e diretrizes de segurança da informação adotadas pela instituição. Os dados obtidos com a aplicação do instrumento de coleta de dados demonstram um equilíbrio muito grande entre concordâncias (51%) e discordâncias (48%), sendo que quando os dados são desdobrados, observa-se que os maiores percentuais estão em concordo parcialmente (40%) e discordo parcialmente (31%). Outro ponto interessante é que, apesar de todo o cenário traçado até agora no que concerne à segurança da informação e sua aplicação nas políticas de segurança informacional da instituição pesquisada, 77% das respostas obtidas indicam que os colaboradores têm consciência que devem cumprir todas as políticas de segurança da informação instituídas e não escolher algumas ou as que consideram mais fáceis para cumprir. Entretanto, apesar da existência de uma política determinando a necessidade de se fazer *backups* frequentes dos dados e informações contidos em máquinas e equipamentos, quando questionados sobre a existência de orientação ou obrigação para fazer *back-ups* diários das informações processas pelo usuário, 74% dos respondentes discordam da afirmativa, ou seja, não se sentem orientados e nem obrigados a fazer *backups*. Mais um elemento que indica a necessidade de equilíbrio de investimentos da organização entre as variáveis, recursos humanos, políticas e procedimentos, e, tecnologias da empresa. De que adianta investir maciçamente em tecnologias se o usuário permitir a entrada de um desconhecido nas bases de dados da empresa? Como equalizar o progresso na segurança tecnológica se os usuários não fazem *backups*? Mesmo diante de uma fortaleza tecnológica digital e física, os seres humanos continuam sendo uma vulnerabilidade em potencial, haja vista que eles transformam os dados e informações e não estão preparados para agir, efetivamente, com a proteção dos ativos informacionais da empresa.

Acredita-se que um dos caminhos, diante desse cenário, seja olhar para pessoas, processos e tecnologias de forma equitativa e equilibrada.

A dúvida sobre o desenvolvimento da gestão de segurança informacional equitativa entre os pilares pessoas, processos e tecnologias, se confirma quando 60% dos respondentes concordam parcialmente, que o desenvolvimento da segurança da informação na instituição na qual trabalham inclui proteção de hardware, software, pessoas e processos, contra ameaças e vulnerabilidades presentes no ambiente corporativo, sejam elas internas e/ou externas à organização.

Os incidentes de segurança da informação podem ser derivados de invasões na máquina ou equipamento no qual se processa as informações, contudo, muitas das vezes essa invasão tem a permissão, intencional ou não, do usuário. Observa-se que 89% discordam que postem em redes sociais fatos ou ocorrências que acontecem na organização ou no setor para alertar amigos. Não obstante, 9% dos respondentes afirmaram que fazem essas postagens. Percebe-se que, por falta de definição do comportamento que a empresa espera do colaborador em relação à segurança da informação, algumas informações relevantes ou estratégicas de fragilidade do sistema da empresa podem estar sendo compartilhadas com pessoas estranhas ao ambiente institucional, gerando verdadeiras ameaças aos ativos informacionais da empresa.

Outro ponto importante de se mencionar é o déficit comunicacional da empresa, no que concerne às informações sobre segurança informacional. Assim, quando questionados se os colaboradores ficam cientes de todas as atualizações de avaliação de riscos de seu departamento, setor ou área, identificou-se uma deficiência na comunicação entre empresa e trabalhadores, uma vez que menos da metade dos trabalhadores afirmaram ter ciência de todas as atualizações de avaliação de riscos de seu departamento, setor ou área, ratificando que os colaboradores constantes nessa amostra trabalham no setor de tecnologia da informação que é responsável pela segurança das informações da organização pesquisada.

Apesar desse cenário de valorização da tecnologia e de desfavorecimento do elemento humano, nota-se que 65% dos respondentes têm interesses em absorver os valores, missão e visão da empresa para a qual trabalham, contra 35% que concordaram que, em primeiro lugar, dedicam atenção à sua profissão e à especialidade do computador com o qual trabalham, para depois absorver os valores, missão e visão da

empresa. Esse cenário demonstra que se deve dedicar especial atenção a esse fator, uma vez que 72% dos respondentes concordaram ou discordaram parcialmente da afirmativa, demonstrando dúvidas com relação a suas respostas, podendo ser este um indicativo que o elemento *pessoas* precisa de atenção devida para que haja efetividade nas ações de segurança da informação da instituição.

Complementar a essa visão, apesar de 63% dos respondentes considerarem que o ambiente da empresa é seguro no que concerne às informações que nele são processadas, entretanto, 9% dos respondentes sentem vontade de explorar redes, invalidar códigos de segurança e desafiar os profissionais de segurança para mostrar o quão frágil é a segurança da informação da instituição. Já 58% dos respondentes se sentem prejudicados pela alta carga de trabalho imposta pela instituição, indicando que esse fator os prejudica com relação à percepção e ações relativas à segurança da informação.

Com relação ao fato da instituição permitir o acesso à rede corporativa, para gravar dados em *pen-drives*, CD´s, DVD´s e/ou imprimir informações para uso tanto no ambiente institucional quanto em casa, 80% dos respondentes discordaram enfatizando que essas não são ações permitidas. Os mesmos 80% dos respondentes observam, ao utilizar o *e-mail* corporativo, a supressão de mensagens que possuem anexos não solicitados. Concomitante, não há acesso irrestrito a sites de acordo com 80% dos respondentes e nem permissão de acesso remoto a sistemas de informação corporativos, de acordo com 75% dos respondentes.

Vinculando a parte tecnológica com as políticas de segurança da informação da empresa observa-se, conforme afirmam 77% dos respondentes, que não existe um *check list* de segurança informacional que os colaboradores devem seguir no seu dia-a-dia. Já com relação à alteração mensal das senhas de acesso aos recursos corporativos, 65% dos respondentes concordam que a senha de acesso deve ser modificada mensalmente, todavia, observa-se que se trata de uma concordância parcial, haja vista que o maior percentual, 37% concordantes, não tem total certeza sobre esse assunto.

4. CONCLUSÕES

Através da avaliação descritiva dos dados e da discussão dos resultados, pode-se concluir que o elemento pessoas é uma variável crítica na gestão de segurança informacional corporativa. As políticas de informação devem ser acessíveis aos funcionários e factíveis de serem executadas. Com relação à tecnologia, é válido que continuem os investimentos, entretanto eles devem ser equilibrados com o desenvolvimento de controles informais (pessoas) e controles formais (políticas e processos) para que haja uma gestão de segurança informacional mais efetiva e eficaz.

Dos resultados apresentados na seção 3, reúnem-se aqui, a título de resumo, impressões obtidas através da pesquisa, as quais caracterizam a segurança da informação do ponto de vista do usuário.

- Os colaboradores em geral acreditam que todos na organização entendem o que é segurança da informação e, conseguem identificar quais são as medidas de segurança da informação corporativa adotadas;
- Há duvidas entre uma boa parte dos colaboradores sobre o seu papel em segurança da informação, apesar de saberem identificar quem são os responsáveis pela segurança da informação na organização;
- Metade deles acredita que segurança da informação é assunto apenas para os responsáveis pela tecnologia da informação;
- A grande maioria dos colaboradores têm a percepção de que a instituição investe mais em tecnologias do que em pessoas para garantir a segurança da informação, e, acreditam que não há investimento suficiente na formação das pessoas no âmbito da segurança informacional;
- A grande maioria não identifica a existência de fórum, no âmbito da organização, apropriado para discutir a temática segurança da informação;
- Menos da metade dos colaboradores admitem conhecer e compreender políticas, procedimentos, normas e diretrizes de segurança da informação adotadas pela instituição; paradoxalmente, a maioria afirma que se sente obrigado cumprir as políticas de segurança da informação instituídas (mesmo considerando que não as entendem);
- A quase totalidade dos respondentes relata não postar informações sobre a organização em redes sociais e que, se o fazem, não incorrem em riscos de segurança;
- Grande maioria dos respondentes acredita na necessidade de considerar o elemento pessoas para que haja efetividade nas ações de segurança da informação;
- A maioria dos colaboradores reporta a falta de um *check list* de segurança para orientação.

Ao se fazer uma leitura dos dados obtidos com a pesquisa, observa-se que tratar as questões de segurança informacional nas empresas requer ações em diversos campos. Entretanto, nem sempre as empresas possuem recursos para investir em soluções para todos os gargalos. Nesse sentido, há a necessidade de uma avaliação do cenário de segurança informacional corporativo, delimitando através dos pilares pessoas, processos e/ou tecnologias aquele que é mais crítico para a empresa. O plano de ação será traçado a partir desse panorama. As próprias perguntas apontarão para possíveis restrições, e, paralelamente para mecanismos de ação.

Conclui-se ainda que a inter-relação entre o usuário da informação e a segurança informacional institucional deve ser monitorada constantemente, para que se consiga agir antecipadamente frente à dinâmica dos incidentes de segurança. Como demonstrado na pesquisa de campo, uma das formas de se checar e controlar essa inter-relação é através da medição constante das ações de segurança informacional implementadas e a reação dos colaboradores frente a elas. Essa medição mostrará o cenário da instituição e que ajudará as organizações a se prevenir dos incidentes de segurança informacional sistemicamente.

Uma conclusão clara da pesquisa espelhada nas respostas dos funcionários, é que o tema segurança da informação ainda é controverso, e muitas vezes confundido com uma abordagem puramente tecnológica. O experimento testou a metodologia proposta, através de sua aplicação a um contexto específico. A amostra utilizada para o experimento não é passível de gerar capacidade de generalização dos resultados obtidos através de uma abordagem quantitativa, apesar de atender estatisticamente aos quesitos confiabilidade e validação de conteúdo . Espera-se propor o teste com amostra representativa junto a empresas e usuários que atenda a critérios estatísticos em trabalhos futuros de forma que tal amostra seja suficiente para determinar a capacidade de generalização do questionário. Mesmo assim, como a nascer um entendimento que o elemento pessoas é essencial para uma boa gestão de segurança informacional e desenvolvimento de políticas bem sucedidas.

REFERÊNCIAS

Allen, B. L. *Information Tasks: Toward a User-centered approach to information systems*. California,USA, A.P.,1996.

Almeida, M. B. Aplicação de Ontologias em Segurança da Informação. *Revista Fonte*. Ed.Fonte, Belo Horizonte: 2007.

Buckland, M. Information as a thing. *Journal of American Society for Information Science*, 1991, v. 42, n. 5, p. 351-360.

Castells, M. *The Rise of the Network Society*. New York: Wiley-Blackwell, 2000.

Colwill, C. R. Human factors in information security: The insider threat & Who can you trust these days? *Information Security Technical Report*, 2010, p. 01-11.

Ghernaouti-Hélie, S. An inclusive information society needs a global approach of information security. *International Conference on Availability, Reliability and Security*. Computer Society, 2009.

Huang, D. L., Rau, P. L. P. and Salvendy, G. Perception of information security. *Behavior & Information Technology*, 2010. v.29, n.3, p. 221- 232.

Ingwersen, P. The cognitive view and information. In: _____. *Information retrieval interaction*. London: Taylor Graham Publishing, 1992. Chapter 2. Disponível em: <http://vip.db.dk/pi/iri/files/Ingwersen_IRI_Chapter2.pdf>. Acesso em: 8 mar. 2010.

Koskosas, I. V., Charitoudi, G. and Louta, M. The role of organizational cultures in information-systems security management. *Journal of Leadership Studies*. Spring, 2008. v.2, issue 1, p.7–17.

Kraemer, S., Carayon, P. and Clem, J. Human and organizational factors in computer and information security. *Computer & Security*. 2009. v.28, p. 509-520.

Lacey, D. *Managing the human factor in information security*. Wiley. 2009.

Likert, R. A Technique for the Measurement of Attitudes. *Archives of Psychology*, 1932. V.140, p.1–55.

Malhotra, N. K. Pesquisa de Marketing: Uma Orientação Aplicada, Porto Alegre: Bookman, 2012, 4a edição.

Marchionini, G. *Digital Library Research and Development*. Enc. of Library and Information Science, 1998, v.63

Sianes, M. Compartilhar ou proteger conhecimentos? Grande desafio no comportamento informacional das organizações. In: *Gestão Estratégica da Informação e Inteligência Competitiva*. São Paulo: Saraiva, 2005.

Solms, R. V. *Information security governance*. South Africa, Springer, 2008.

Sveen, F.O., Torres, J.M. and Sarriegi, J.M. Blind Information Security Strategy. *International Journal of Critical infrastructure Protection*, v.2, 2009, p.95-109

Wylder, J. *Strategic Information Security*. [s.l.]: Auerbach Publications, 2004.