SEGURANÇA DA INFORMAÇÃO: A PERCEPÇÃO DO USUÁRIO ACADÊMICO

ANSCHAU, Jader Hericks[1]
PEREIRA, José Andres Telles[2]
SZCZUK, Bruno Henrique Pereira[3]
BRITO, Patrick Lucas Gruhlke de[4]
SILVA, Ivan Vieira da[5]

RESUMO

Neste artigo busca-se analisar a partir da revisão da literatura e pesquisa de campo qual o papel da informação nas organizações, seja no planejamento estratégico, na tomada de decisões ou no funcionamento operacional. Assim, a informação deve ser íntegra, confidencial, disponível quando necessária e estratégica para o funcionamento das organizações. A informação pode oportunizar, gera competitividade, analisar o mercado. O fator humano ainda representa a maior vulnerabilidade da informação. Assim, a segurança da informação busca preservá-la contra ameaças. Considerando a importância da segurança da informação e o papel do fator humano, foram desenvolvidas pesquisas de campo, através de um questionário, para verificar a percepção dos usuários em relação à segurança da informação. E neste artigo busca descrever os resultados obtidos nesta pesquisa a fim de auxiliar em novas pesquisas na área.

Palavras-chave: Informação. Segurança. Vulnerabilidade.

---

[1]Graduando em Sistemas de Informação no Centro Universitário Fundação Assis Gurgacz (FAG); Graduação em Tecnologia em Gestão Financeira pela FASUL (2010). E-mail: sistemasjader@gmail.com

[2]Graduando em Sistemas de Informação no Centro Universitário Fundação Assis Gurgacz (FAG). E-mail: joseandrestellespereira@gmail.com

[3]Graduando em Sistemas de Informação no Centro Universitário Fundação Assis Gurgacz (FAG); E-mail: brunoszczuk@gmail.com

[4]Graduando em Sistemas de Informação no Centro Universitário Fundação Assis Gurgacz (FAG); E-mail: patricklucas524@gmail.com

[5]Graduação em Matemática UNIPAR (2006); Especialista em Matemática Financeira e Estatística pela UNIPAR (2008); Especialista em Gestão Escolar pela FAESI - DINÂMICA (2016); Especialista em (TGD) Transtornos Globais de Desenvolvimento pela FAESI - DINÂMICA (2016); Mestrando Em Gestão do Conhecimento nas Organizações (UNICESUMAR - Maringá). E-mail: vieira_ivan@yahoo.com.br

INTRODUÇÃO

A era da informação é o período que sucedeu a década de 1980, e é marcada pela grande capacidade de armazenamento de dados, informações e conhecimentos. A informação é considerada um ativo essencial para as organizações. Está diretamente ligada ao planejamento estratégico, e por desempenhar papel de suma importância necessita de segurança. Para Dantas (2011) a informação possui características fundamentais que devem ser protegidas. Beal (2005) afirma que essas características são protegidas pelo processo de segurança da informação. Segundo Dantas (2011), o fator humano representa a maior vulnerabilidade da informação. A falta de capacitação, a falta de consciência de segurança, omissões, erros e desleixo quanto às senhas no ambiente de trabalho são algumas das origens de tal vulnerabilidade.

Tendo em vista a importância da informação e o fator humano como maior vulnerabilidade, este artigo busca evidenciar, através de uma pesquisa de campo, a percepção dos usuários quanto à segurança da informação.

O artigo está organizado conforme segue. Na seção 1 apresenta-se uma revisão de conceitos de dados e informação, também a importância da informação, suas classificações e ciclo de vida. Na seção 2 são apresentados conceitos da segurança da informação. A seção 3 traz uma relação com as principais normas ISO 27000. Na seção 4 apresenta-se a metodologia utilizada. A seção 5 apresenta os resultados e discussão. Finalmente é apresentada a conclusão deste estudo.

1 DADOS E INFORMAÇÃO

Dados e informação são conceitos distintos. Segundo Dantas (2011), os dados são a mais baixa classe da informação. Já a informação são os dados que passam por algum processamento para serem utilizados.

Para Laudon & Laudon (2004), dados são fatos brutos, eventos ocorrendo em uma organização antes de serem tratados e organizados de forma que possam ser compreendidos e utilizados. Já informação refere-se aos dados já organizados e apresentados de forma significativa para as pessoas.

Segundo Setzer (2015), dado é uma sequência de símbolos já quantificados, ou que podem ser quantificados. Podem ser considerados dados os textos, fotos, figuras, sons gravados e animação, pois podem ser quantificados e reproduzidos sem que se perceba diferença com o original. A informação, por sua vez, possui semântica, significado, e não pode ser manipulada por um computador, visto que a máquina é puramente sintática.

Dantas (2011) afirma que a informação possui três características fundamentais, a integridade, a disponibilidade e a confidencialidade. A integridade garante a exatidão e completeza da informação, ou seja, que ela não seja modificada, alterada ou destruída sem autorização, e que também seja legítima. A disponibilidade garante acesso à informação às pessoas autorizadas sempre que necessário. A confidencialidade garante que somente pessoas autorizadas tenham acesso à informação.

1.1 IMPORTÂNCIA DA INFORMAÇÃO

Para Silva (2010) a informação é uma necessidade para o funcionamento estratégico, tático e operacional das organizações. É necessário saber onde encontrar a informação, como apresentá-la e como usá-la para assim tornar-se um recurso estratégico.

Segundo Sêmola (2014), as constantes mudanças e novidades no mercado influenciam as empresas. A busca por inovação faz com que novas descobertas e conceitos surjam. Desde a revolução industrial a informação exerce um papel importante na gestão dos negócios. A partir dela, é possível melhorar produtividade, reduzir custos, aumentar a competitividade e ter um apoio fundamental no processo de tomada de decisão. Em diversos ramos de atuação de empresas, a informação serve como base para ações e planejamento. É fundamental para análise de mercado, análise de concorrência, dados operacionais e outros, e torna-se um diferencial competitivo.

De acordo com Dantas (2011), a informação é importante para manutenção dos negócios, bem como para realização de novos empreendimentos, e, por isso,

tem recebido atenção especial do mundo todo. Uma informação pode tanto abrir oportunidades como gerar competitividade, ouse já, é um fator essencial. Por outro lado, uma informação corrompida, ou ausência de informação, constitui ameaça às empresas. A partir disso, pode-se afirmar que a informação é um ativo fundamental aos negócios de uma organização.

1.2 CLASSIFICAÇÃO DA INFORMAÇÃO

A informação pode ser classificada de várias formas. De acordo com Beal (2005), uma dessas classificações ocorre pelo ponto de vista de suas exigências de confidencialidade, disponibilidade e integridade.

Beal (2005) afirma que, considerando a confidencialidade da informação, ela pode ser classificada como confidencial reservada ou pública. Uma informação confidencial não pode ser divulgada, e sua divulgação pode causar graves danos à organização. Uma informação reservada também não deve ser divulgada, porém se acontecer causa danos de menor gravidade à organização. Uma informação publica é uma informação de acesso livre.

De acordo com Beal (2005), quanto à disponibilidade, deve ser analisado o custo para se produzir a informação, o custo para recuperar e o impacto caso a informação seja completamente perdida. A partir dessa análise a informação então é classificada de acordo com a prioridade, por exemplo, quais devem ser prontamente recuperadas, quais poderiam ter um prazo maior para recuperação e quais possivelmente não necessitariam serem recuperadas.

Para Beal (2005), a falta de integridade da informação pode causar sérios danos à organização. Assim, é classificada em três categorias: alta exigência de integridade, média exigência, e baixa exigência de integridade. Informações com alta exigência de integridade que não estejam íntegras podem comprometer objetivos e trazer grandes prejuízos à organização, bem como descumprimento de leis. Informações de média exigência de integridade que não estejam íntegras não comprometem nem geram grandes impactos à organização, mas pode causar prejuízos. As informações de baixa exigência de integridade que não estejam

íntegras podem facilmente ser detectadas e não oferecem risco consideráveis à organização.

1.3 CICLO DE VIDA DA INFORMAÇÃO

A informação possui um ciclo de vida. Segundo Dantas (2011), o ciclo inicia na produção, tem um tempo de vida e depois é destruída. Este ciclo é composto de produção e manuseio, armazenamento, transporte e descarte.

Para Sêmola (2014), o manuseio é o momento em que a informação é criada. Pode ser digitando informações, folheando papéis ou utilizando uma senha de acesso. O armazenamento ocorre quando a informação é armazenada, seja em bancos de dados, mídias como CD's e DVD's ou pendrives. O transporte é o momento que a informação é transportada, ocorre quando se encaminha por e-mail, internet, ou ainda falada ao telefone. Descarte ocorre quando a informação é descartada, seja eliminando um arquivo do computador ou descartando um CD ou material impresso. A Figura 1 apresenta o ciclo de vida da informação de acordo com Sêmola (2014).

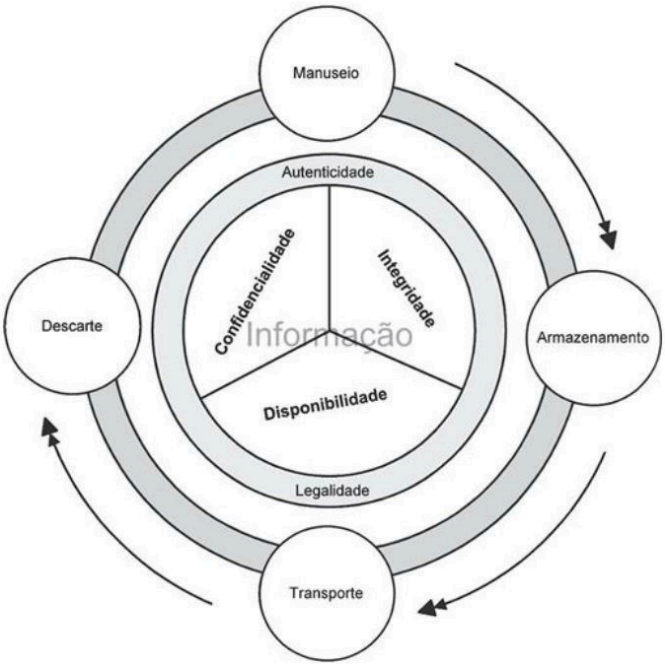

Figura 1. Ciclo de vida da informação segundo Sêmola (2014)

2 SEGURANÇA DA INFORMAÇÃO

De acordo com a norma ISO/IEC 27001 NBR (2006), segurança da informação é preservação da confidencialidade, integridade e disponibilidade da informação. Podem estar envolvidas também outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade. Os termos: ativo, disponibilidade, confidencialidade, integridade são também definidos pela norma como segue. Ativo: qualquer coisa que tenha valor para organização. Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados. Integridade: propriedade de salvaguarda da exatidão e completeza de ativos.

Segundo Beal (2005) segurança da informação é um processo de proteção da informação das ameaças para sua integridade, disponibilidade e confidencialidade. Confidencialidade garante que o acesso será restrito a informação. Integridade garante que a criação é legitima e que não haverá alteração ou destruição não autorizada dos dados e informações. Disponibilidade garante que a informação esteja disponível aos usuários quando necessário.

Para Sêmola (2014), segurança da informação é uma área do conhecimento que se dedica à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Ou seja, uma gestão de riscos incidentes que possam comprometer os principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação. Assim, são regras que incidem sobre o ciclo de vida da informação, identificando e controlando ameaças e vulnerabilidades.

Os termos: risco de segurança da informação, ameaça e vulnerabilidade são definidos pela norma ISO/IEC 27005 NBR (2008). Risco de segurança da informação refere-se à possibilidade de uma ameaça explorar vulnerabilidades de um ativo. Ameaça é a causa potencial de um incidente, podendo gerar danos à organização. Vulnerabilidade é uma fragilidade de um ativo que pode ser explorado

por ameaças. O Anexo D da norma ISO/IEC 27005 NBR (2008) apresenta uma lista com exemplos de ameaças e vulnerabilidades. São exemplos de vulnerabilidades: Manutenção insuficiente/Instalação defeituosa de mídia de armazenamento, armazenamento não protegido, falta de cuidado durante o descarte, realização de cópias não controlada, falhas de software, interface de usuário complicada, datas incorretas, gerenciamento de senhas mal feito, inexistência de cópias de segurança, download e uso não controlado de software, entre outros. São exemplos de ameaças: destruição de equipamento ou mídia, abuso de direitos, comprometimento de dados, defeito do software, forjamento de direitos, alteração de software, e outros.

Beal (2005) define risco, ameaça, vulnerabilidade e ataque. Risco é uma combinação da probabilidade de um evento e sua consequência. Ameaça é uma expectativa de um acontecimento proposital ou não, que pode afetar um sistema, ambiente ou informações. Vulnerabilidade pode ser definida como uma fragilidade de possível exploração por uma ameaça. Ataque é o evento decorrente da exploração da vulnerabilidade por uma ameaça.

3 NORMAS ISO 27000

As normas pertencentes à família ISO 27000 tratam da segurança da informação. As principais normas são: ISO/IEC 27000 é uma introdução à família ISO 27000. Inclui um glossário de termos. ISO/IEC 27001 define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI). ISO/IEC 27002 é um código de práticas com controles que auxiliam aplicação do SGSI. ISO/IEC 27003 contém diretrizes para a implementação do SGSI. ISO/IEC 27004 possui métricas de medição para a gestão da segurança da informação. ISO/IEC 27005 aborda a gestão de riscos. ISO/IEC 27006 possui requisitos para organizações que trabalham com auditoria e certificação de SGSI.

ISO/IEC 27007 contém diretrizes para auditoria do SGSI. ISO/IEC 27008 é focada na auditoria dos controles em segurança da informação. ISO/IEC 27010 é um guia para a comunicação em gestão da segurança da informação. ISO/IEC 27011 é um guia de gestão da segurança da informação para empresas de

telecomunicações. ISO/IEC 27014 são técnicas para gestão da segurança da informação. ISO/IEC 27015 é focada em gestão da segurança da informação para serviços financeiros. ISO/IEC 27016 é focada em gestão da segurança da informação para setores econômicos. ISO/IEC 27017 aborda controles para *cloud computing*. ISO/IEC 27018 aborda especificamente a privacidade. ISO/IEC 27032 trata de *Cybersecurity*. ISO/IEC 27033 é dividida em seis partes para tratar segurança em redes. ISO 27034 é dividida em partes também, e aborda a segurança da informação em aplicações.

4 METODOLOGIA DA PESQUISA

Para elaboração deste artigo, utilizou-se a pesquisa bibliográfica para conceituação dos termos e assuntos abordados. Para Lakatos e Marconi (1991) a pesquisa bibliográfica engloba toda bibliografia publicada, tanto em livros, teses, revistas jornais ou outros como rádios, filmes e demais meios de comunicação oral. A finalidade de tal pesquisa é colocar essas informações escritas, gravadas, ditas ou filmadas em contato direto com o pesquisador.

Foi realizada uma pesquisa de campo com um questionário. Para Fonseca (2002), em uma pesquisa de campo realiza-se a coleta de dados junto às pessoas. Gil (2002) afirma que um questionário é uma técnica de investigação composta por questões apresentadas às pessoas, com o objetivo de conhecer opiniões, interesses, situações vivenciadas, e outros. Assim, para o levantamento dos dados da pesquisa, foi aplicado um questionário aos acadêmicos dos quartos anos dos cursos de Administração e Ciências Contábeis da Faculdade Sul Brasil (FASUL) do ano de 2016. Foram coletados 43 questionários, sendo 16 do curso de Ciências Contábeis, representando 37% dos resultados, e 27 do curso de Administração, representando 63% dos resultados.

O questionário foi composto de 16 assertivas. Em cada assertiva, o respondente era questionado em duas categorias de resposta. A primeira, chamada de identificação, o respondente identificava a assertiva de acordo com a organização em que trabalha. Foram apresentadas três opções nessa categoria: “sim”, “não” e

"não sei". A segunda categoria, avaliação, o respondente avaliava de acordo com sua opinião o quão importante ele considerava tal assertiva. Nessa categoria as opções disponíveis eram: "sem importância", "pouca importância", "importante" e "muito importante". O questionário foi preenchido de forma anônima, apenas era identificado o curso que o respondente cursava. A partir dessas assertivas buscou-se identificar se esses respondentes possuem conhecimento quanto às praticas de segurança da informação na organização que trabalha, o quanto consideram importante cada uma, considerando que são essenciais para garantir a segurança da informação, e como estas organizações lidam com as práticas de segurança da informação. A Tabela 1 apresenta as 16 assertivas presentes no questionário.

1. A organização possui especialistas em segurança da informação.
2. As pessoas da organização conhecem as ferramentas e práticas de segurança da informação.
3. Os SIGs da empresa raramente são violados por acesso não autorizado.
4. Os SIGs estão disponíveis apenas para usuários autorizados.
5. A organização possui políticas adequadas que definem quando e como as informações internas podem ser compartilhadas.
6. A organização investe em segurança da informação quando necessário.
7. A organização possui uma estratégia bem definida de segurança da informação e é divulgada adequadamente.
8. A organização possui recursos adequados de segurança da informação contra ameaças internas e externas aos SIGs.
9. A organização mantém cópias de segurança (backup) dos SIGs, as quais estão disponíveis sempre que necessário.
10. A organização possui políticas adequadas quanto à identificação de usuários, senhas e privilégios de acesso aos SIGs.
11. A organização dispõe de recursos tecnológicos adequados para apoiar a segurança da informação.
12. A identidade dos usuários é verificada antes de permitir acesso aos SIGs.
13. As informações geradas pelos SIGs da organização raramente apresentam erros ou distorções.
14. A privacidade dos dados confidenciais de fornecedores, clientes e funcionários são protegidos pela organização.
15. Os SIGs estão sempre disponíveis quando necessário.
16. Os colegas de trabalho nunca compartilham suas senhas (acesso aos SIGs, internet...) com seus outros colegas

Tabela 1. Questionário com as 16 assertivas

5 RESULTADOS E DISCUSSÕES

A primeira análise é quanto ao conhecimento sobre as práticas de segurança da informação na organização na qual trabalha, de acordo com a categoria “identificação” do questionário. Foram contabilizadas as quantidades de “sim”, “não” e “não sei” de cada assertiva. A Figura 2 representa o gráfico com o resultado da pesquisa da primeira categoria. Cada assertiva é representada pela letra “A” seguida do seu respectivo número.

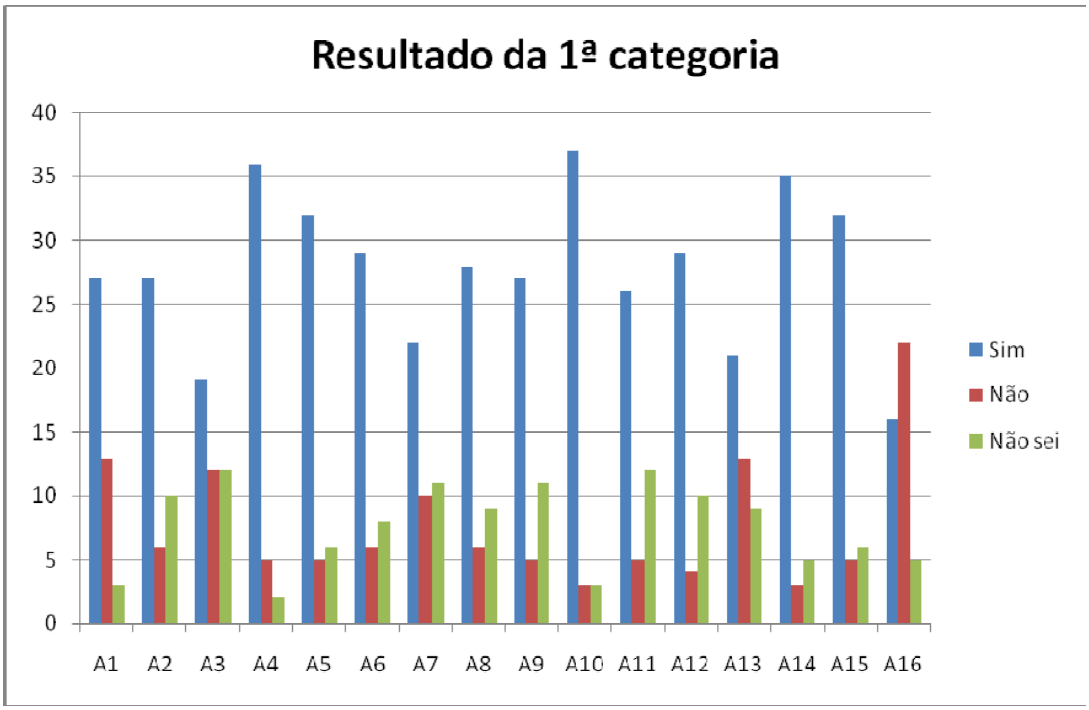

Figura 2. Resultado da primeira categoria de respostas

Pode-se verificar que em 12 das 16 assertivas a quantidade de “sim” foi superior a 60% (25), ou seja, de modo geral, as organizações representadas neste estudo tem se atentado à segurança da informação. Apesar de um resultado positivo, é importante ressaltar que algumas assertivas obtiveram um baixo resultado, como o caso da assertiva número 3 e número 13. Isso é preocupante, pois a assertiva número 3 diz respeito sobre violação dos sistemas de informações gerenciais (SIG’s) por acesso não autorizado, violando diretamente a confidencialidade da informação. Já a assertiva número 13 trata dos erros nas

informações geradas pelos SIG's, o que fere o princípio da integridade da informação. A assertiva número 7 também não obteve um resultado satisfatório, e é importante destacar que o projeto de segurança da informação deve ser bem definido e divulgado para melhor aceitação entre os usuários comuns, conforme Goodrich & Tamassia (2013). A assertiva número 16 foi a com pior resultado, refere-se ao compartilhamento de senhas pessoais, prática amplamente reprovável, evidenciando a vulnerabilidade humana nos projetos de segurança da informação.

A segunda análise é quanto à importância de cada assertiva na opinião dos respondentes. Foram contabilizadas as quantidades de "sem importância", "pouca importância", "importante" e "muito importante". Para o resultado, foram somados os valores obtidos de "sem importância" e "pouca importância", e somados também os valores obtidos de "importante" e "muito importante". A Figura 3 representa o gráfico com o resultado da pesquisa da segunda categoria.

Cada assertiva é representada pela letra "A" seguida do seu respectivo número.

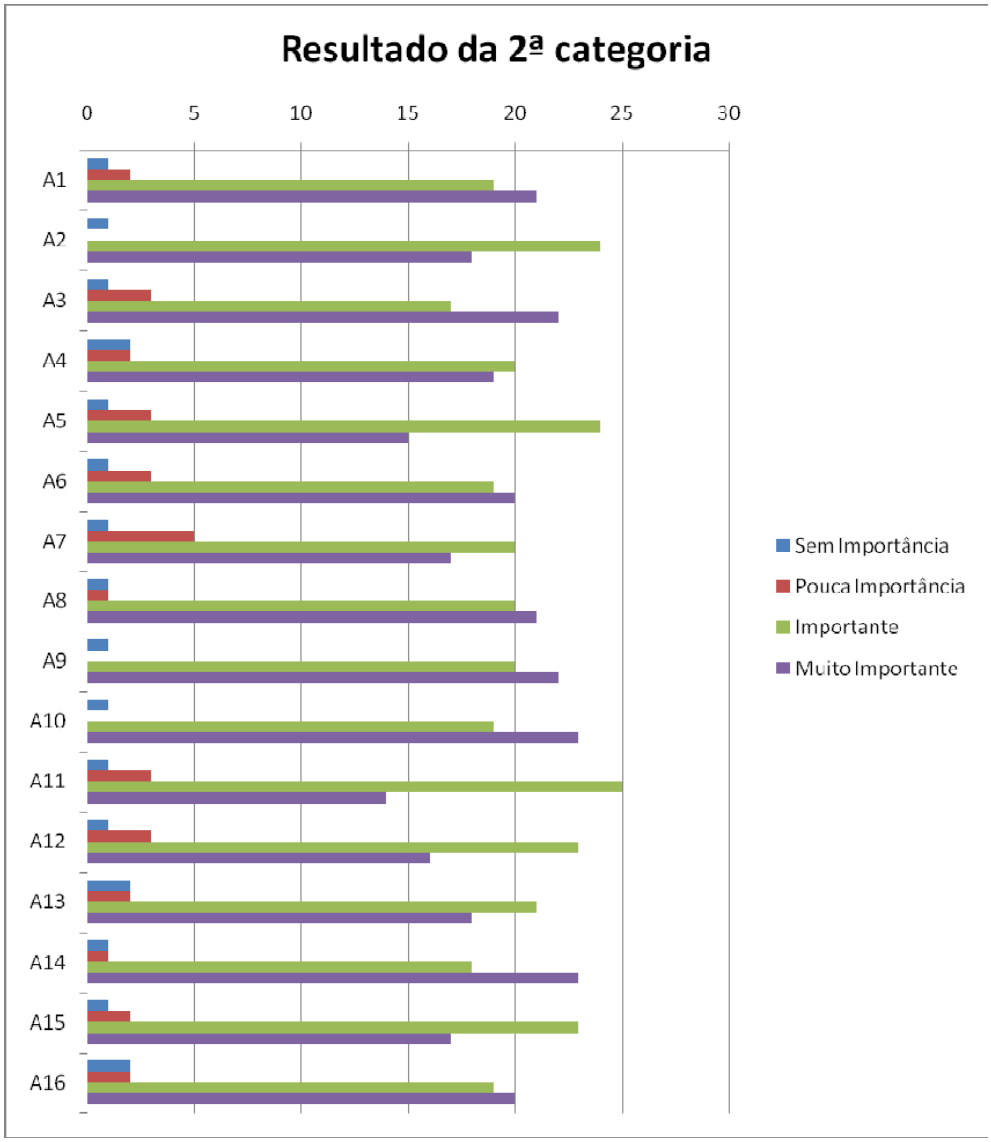

Figura 3. Resultado da segunda categoria de respostas

Após a contagem, nove das 16 assertivas obtiveram um número de “sem importância” e “pouca importância” notável: quatro ou mais. Essas questões são as de números: 3, 4, 5, 6, 7, 11, 12, 13 e 16. Apesar de o valor obtido não representar a maioria dos votos, ele deixa claro que a segurança da informação é vista como pouco relevante para parte dos entrevistados. Ainda é importante salientar que as assertivas número 3, 7, 13 e 16 tem um resultado notório nas duas categorias, devendo assim receber atenção especial em projetos de segurança da informação.

CONSIDERAÇÕES FINAIS

Este artigo apresentou uma pesquisa bibliográfica sobre a segurança da informação e uma pesquisa de campo para avaliar a percepção do usuário quanto à segurança da informação.

É evidente que os usuários não têm ciência da relevância da segurança da informação, apesar de muitos afirmarem que as organizações possuem políticas de segurança da informação. Considerar pouco importante a violação por acesso não autorizado aos SIG's e o compartilhamento de senhas demonstra a vulnerabilidade humana. Ainda pode-se verificar que em algumas organizações a política de segurança de informação não é bem definida divulgada, prejudicando a percepção e prática pelos usuários.

A partir disso, pode-se concluir que os acadêmicos dos cursos supracitados possuem pouca percepção da segurança da informação, alcançando o objetivo deste estudo. Desta forma percebe-se que as políticas de segurança da informação precisam ser mais bem desenvolvidas nas organizações.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006.** Trata sobre sistema de gestão de segurança da informação - requisitos. Rio de Janeiro, 2006.

_____. **NBR ISO/IEC 27005:2008.** Trata sobre gestão de risco de segurança da informação. Rio de Janeiro, 2008.

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

DANTAS, Marcus Leal. **Segurança da informação: uma abordagem focada em gestão de riscos.** Olinda: Livro Rápido, 2011.

FONSECA, João José Saraiva. **Metodologia da pesquisa científica.** Fortaleza: UEC, 2002. Apostila.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa.** 4. Ed. São Paulo: Atlas, 2002.

GOODRICH, Michael T; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Trad. Maria Lucia Blanck Lisboa; revisão técnica: Raul Fernando Weber. Porto Alegre: Bookman, 2013.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica.** 3. Ed., São Paulo: Atlas, 1991.

LAUDON, Kenneth C; & LAUDON, Jane P. **Sistemas de Informações Gerenciais.** São Paulo: Prentice Hall, 2004.
SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva.** 2. Ed. Rio de Janeiro: Elsevier, 2014.

SETZER, Valdemar W. **Dado, Informação, Conhecimento e Competência.** Disponível em: <https://www.ime.usp.br/~vwsetzer/dado-info.html>.
Acesso em 18 de Agosto de 2016.

SILVA, Rodrigo Gomes da. **A Importância da Informação.** Disponível em: <http://www.administradores.com.br/producao-academica/a-importancia-da-informacao/2820/>.
Acesso em 27 de Agosto de 2016.