Revista Conhecimento Contábil

AMEAÇAS E MECANISMOS DE SEGURANÇA DA INFORMAÇÃO EM UM AMBIENTE ORGANIZACIONAL DE PLANOS DE SAÚDE

THREATS AND INFORMATION SECURITY MECHANISMS IN AN ORGANIZATIONAL HEALTH PLANNING ENVIRONMENT

Matheus Ronielli Alves de Souza
Graduando em Sistemas da Informação
E-mail:contato.mralvessouza@gmail.com

Adson Diego Lacerda Cavalcante
Graduando em Sistemas da Informação
E-mail: adson.diego@hotmail.com

Alane Izabel Bezerra da Silva
Graduanda em Sistemas da Informação
E-mail:alane_izabel@hotmail.com

Juliana Carvalho de Sousa
Doutoranda em Administração
E-mail:juli.cs1009@gmail.com

Raniela Ricarte Freitas Sampaio
Mestranda em Administração
E-mail: raniela.ricarte@gmail.com.

RESUMO
Dado a relevância do assunto da segurança da informação presente nos ambientes organizacionais, o presente artigo tem como objetivo geral compreender os mecanismos de segurança de informação utilizados na atuação de possíveis ameaças no ambiente organizacional de uma empresa que atua ofertando serviços de planos de saúde na cidade de Mossoró, Rio Grande do Norte. A pesquisa possui natureza descritiva e qualitativa, realizada por meio de entrevistas, utilizando a Análise do Núcleo de Sentidos (ANS) como método de análise dos dados. Através do estudo realizado foi possível concluir que a organização alvo da pesquisa utiliza um processo informal de segurança da informação, fazendo uso de recursos de segurança comumente presentes na maioria das organizações e possuindo pouco conhecimento sobre recursos mais avançados de segurança, mostrando assim uma necessidade de conhecimento mais aprofundado por parte dos entrevistados que atuam no setor de tecnologia da informação.

Palavras-chave: Segurança da Informação, Mecanismos de Segurança da Informação. Organização de Planos de Saúde.

ABSTRACT
Given the relevance of the fineness security of subjects present in organizational environments, this is one of the main information security tools used in the performance of potential threats in the organizational environment of a company offering health services in the city of Mossoró, Rio Grande do Sul. North. The research has a descriptive and qualitative nature, performed through interviews, using the Analysis of the Nucleus of Matters (ANS) as a method of data analysis. Through the study, it was possible to affirm that another organization uses an informal process of information security, making use of security resources commonly present in most organizations and having little knowledge about more advanced security features, demonstrating the need for a more in-depth knowledge of respondents working in the information technology sector.

Keywords: Information Security, Information Security mechanisms, Organization of Health Plans.

1 INTRODUÇÃO

O mundo está cada vez mais sistematizado com o avanço dos recursos tecnológicos da informação. Esses recursos deixaram de ser parte exclusiva de grandes corporações e atualmente fazem parte da vida de cidadãos comuns e, consequentemente, de organizações de pequeno e médio porte. As tecnologias digitais visam reinventar e mudar a forma como antigas e atuais tarefas eram e são realizadas, através do uso de aplicações e recursos de softwares, hardwares, redes etc. Com intuito de otimizar e tornar qualquer tarefa eficiente, cada vez mais são introduzidas as tecnologias de informação (TI) no cenário atual. Nesse contexto, emergiu instrumentos e tecnologias capazes de promover oportunidades e facilidades que beneficiam diversos usuários, como também, surgiram lacunas para grandes riscos e problemas, sejam para pessoas físicas ou jurídicas, principalmente no que tange as atividades do ambiente corporativo (MARCIANO; LIMA-MARQUES, 2006). Como consequência dessas ameaças, relacionadas com a sistematização tecnológica, novos meios de prevenção foram criados para identificar e reduzir os riscos à informação de seus usuários.

Toda organização produz grande quantidade de informações, essas dizem respeito a seus colaboradores e funcionários, sendo geradas através de processos administrativos, pesquisas, planos estratégicos, bem como as demais atividades dentro e fora do seu ambiente laboral. Essas informações devem ser exclusivas da organização e geralmente são utilizadas em suas atividades administrativas, em seus planos estratégicos e tomadas de decisão do negócio (JANSSEN, 2008).

Levando em conta que tecnologias, processos de negócio e pessoas mudam constantemente, e assim alteram o nível de riscos atuais, podem gerar novas ameaças à organização. A avaliação crítica e metódica dos controles relacionados à segurança da informação torna-se necessária (RIGON; WHESTPALL, 2013).

A existência de uma gestão de segurança da informação no departamento de Sistemas de Informação (SI) se torna de relevância significativa, uma vez que medidas e ações

precisam ser tomadas para garantir a segurança das informações da organização. Levando-se em consideração o tipo de negócio e as atividades da organização alvo da pesquisa desse artigo, a questão central consiste em identificar quais os mecanismos que a gestão de SI da empresa de planos de saúde da cidade de Mossoró/RN utiliza para manter controle sobre essas ameaças.

O presente artigo tem por objetivo geral compreender os mecanismos de segurança de informação na atuação de possíveis ameaças no ambiente organizacional de uma empresa que atua prestando serviços de planos de saúde da cidade de Mossoró, Rio Grande do Norte. São objetivos específicos: a identificação de possíveis ameaças presentes no ambiente do negócio; conhecer os mecanismos usados que visam combater essas ameaças; analisar esses mecanismos em função das ameaças que visam combater.

Considerando esses fatores, a escolha da segurança da informação como tema para esse artigo se mostra indispensável, pois tão relevante quanto à evolução das tecnologias de informação dentro das organizações, é a segurança da informação. Uma vez que essas tecnologias estão integradas dentro de um ambiente organizacional, a inexistência de formas de controle de riscos e políticas de segurança eficazes transformam esses sistemas em ferramentas que passam a contribuir com riscos de falhas que comprometem a segurança das informações, resultando em custos que poderão ir além de valores monetários, e colocando em risco a existência do negócio (MARCIANO; LIMA-MARQUES, 2006).

2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO– DEFINIÇÃO E PRINCIPIOS

Para Silva Neto: Abner da & Pinheiro da Silveira: Marco Antônio (2007) pode-se definir a Segurança da Informação como sendo a área do conhecimento que visa à proteção da informação, essa proteção por sua vez traz como objetivo combater as ameaças contra a integridade, disponibilidade e confidencialidade das informações, afim de minimizar os riscos e garantir a continuidade do negócio. Já no manual da ABNT NBR ISO/IEC 17799 (2005, p.9) encontramos a seguinte definição: “A proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Para Marciano e Lima-Marques (2006) focam no aspecto social da segurança da informação, onde por vezes a gestão e a literatura disponível careciam de uma abordagem melhor, pois ocasionavam falhas nos processos dos mecanismos de segurança implantados, além de contribuírem para o aumento de vulnerabilidades presentes em sistemas.

Problema evidenciado nas conclusões da pesquisa de Silva Neto et al. (2007), onde dividiu cerca de 20 a 24 controles da norma ABNT NBR ISO/IEC 17799 (2005) por camadas, sendo elas: físicas, lógicas e humanas. Mostrando que a camada humana seria a que possui menos controles implantados nas empresas alvo da pesquisa, no qual para diminuir os riscos de incidentes de segurança da informação, essas empresas investem mais em controles tecnológicos, resultando no enfraquecimento do fator humano, grande responsável por falhas de segurança.

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

Marciano e Lima-Marques (2006) elenca uma definição que envolve os seguintes componentes: (1) atores do processo, que são os usuários; (2) o ambiente de atuação, que envolve os sistemas de informações; (3) o alcance da atuação, que se resume na própria sociedade.

> Segurança da informação é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso (MARCIANO; LIMA-MARQUES, 2006, p.7).

Conforme Dantas (2011) para que se utilize a informação, deve respeitar três características básicas, são elas: (1) integridade, que consiste em permitir que a informação não sofra modificação e que permaneça consistente; (2) disponibilidade: disposição da informação para aqueles que foram autorizados a possuí-la; (3) confidencialidade: garantir que a informação seja disponibilizada apenas para os indivíduos autorizados.

2.2 SEGURANÇA DA INFORMAÇÃO - AMEAÇAS

Com a popularização dos recursos de informática, os problemas relacionados a ameaças, tentativas de ataques e invasões, tornam-se a principal preocupação das organizações, pois afetam os requisitos básicos dos sistemas computacionais (KROLL; D'ORNELLAS, 2009).

A preocupação das empresas com as ameaças aos negócios corporativos, perpassa pelos seguintes elementos: tirá-las do cenário competitivo, seja comprometendo sua imagem, ocasionando perdas financeiras, comprometendo demais ativos tecnológicos da empresa, ou qualquer fator que tenha consequências direta na sua segurança (DANTAS, 2011).

Segundo a norma ABNT NBR ISO/IEC 17799:2005, diversos tipos de ameaças à segurança da informação estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. Nos ambientes organizações os sistemas de informação e redes de computadores estão cada vez mais expostos a essas ameaças, como fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação, danos causados por códigos maliciosos, hackers e ataques de *denialofservice* (Negação de Serviço).

Sêmola (*apud* DANTAS, 2011) define ameaças como sendo agentes ou condições que comprometem os negócios de uma organização por meio da exploração de suas vulnerabilidades, causando incidentes que comprometem as informações e seus ativos, provocando perdas de confiabilidade, integridade e disponibilidade. Embora não seja uma regra, colaboradores e usuários tendem a apresentar-se como as maiores ameaças à segurança da informação, seja por negligência ou por falta de conhecimento (KLETTENBERG, 2016).

Nesse sentido ressalta Peixoto (2004, p.46):

> Dado os inúmeros tipos de ameaças, podemos então classificar sua natureza nos seguintes itens:1.Naturais: são todas as ameaças que se originam de fenômenos da natureza, tais como terremotos, furacões, enchentes, maremotos, tsunamis;2.Involuntárias: não intencionais, geralmente são causadas por acidentes,

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

> erros, ou por ação inconsciente de usuários, tais como vírus eletrônicos, que são ativados pela execução de arquivo anexado às mensagens de e-mail;3.Intencionais: são aquelas deliberadas causadas por um agente humano, que objetivam causar danos, tais como hackers, fraudes, vandalismo, sabotagens, espionagem, invasões e furtos de informações, dentre outras.

Alguns dos itens anteriormente citados podem ainda ser classificados como sendo ameaças do tipo interna ou ameaças do tipo externa. Conforme SCUA – Segurança e Gestão de TI (*apud* GABBAY, 2003):Internas: onde os responsáveis por causar danos internos geralmente são funcionários insatisfeitos que querem prejudicar o desenvolvimento do trabalho ou obter vantagens financeiras. Prestadores de serviços e funcionários terceirizados também são potenciais responsáveis por esse tipo de conduta. Como exemplo de ameaças internas o roubo de informação, a alteração ou destruição de informações, os danos físicos a hardware e alteração de configurações e danos lógicos à rede. Externas: causadas por indivíduos externos à organização, que não fazem parte dela, e/ou que realizam ataques de maneira remota. Geralmente os objetivos dos ataques vão, desde indisponibilizar serviços ou máquinas até roubar informações sigilosas.

2.3MECANISMOS DE SEGURANÇA DA INFORMAÇÃO

Dentre os diversos mecanismos mais comuns adotados por empresas para a segurança de informações, irá se abordar os mais importantes, ressaltando que muitos não vieram a ser ordenados, configurando-se como parte integrante de normas de gestão de segurança de informação.

2.3.1O profissional de Segurança

A contratação ou capacitação de um profissional para exercer o papel do *Security Officer* é um dos mecanismos mais comumente utilizados pelas empresas, o mesmo deve conhecer a fundo o negócio da empresa, seu Plano de Negócios, seus modelos de gestão, tecnologias disponíveis e, obviamente, conhecimento de Segurança da Informação (GABBAY, 2003).

Para Marinho (*Apud* GABBAY, 2003, p.57) o *Security Officer* dever possuir os seguintes atributos: organizar toda a infraestrutura organizacional para o tratamento da segurança da empresa; planejar os investimentos para a segurança da informação; definir índices e indicadores para análise de retorno do investimento; montar, orientar e coordenar a equipe de segurança ou a consultoria terceirizada; definir, elaborar, divulgar, treinar, implementar e administrar juntamente com a sua equipe o plano estratégico de segurança, os relatórios de avaliação do nível de segurança, a conformidade e atendimento a legislação vigente e investigações sobre incidentes de segurança.

2.3.2Análise/Avaliação de Riscos

O risco poderá gerar perdas de confidencialidade, integridade e disponibilidade das informações. Acerca da avaliação dos riscos, este envolve a identificação dos ativos, das

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

ameaças e das vulnerabilidades, avaliando e selecionando medidas de segurança para reduzir os riscos e para implementar medidas que assegurem a segurança (KROLL; D'ORNELLAS, 2009).

A norma ABNT NBR ISO/IEC 17799:2005 aborda que o processo de avaliação de risco juntamente com a seleção do controle poderá ser realizado várias vezes, de forma periódica, a fim de gerar resultados comparáveis e que possam ser reproduzidos.

2.3.3 Normas de sistema de gestão de segurança da informação (SGSI)

Um sistema de segurança segundo Dantas (2011, p.199) "compõe todo um arcabouço de políticas, procedimentos, recursos humanos, tecnologia de suporte e infraestrutura necessários ao funcionamento das atividades voltadas para a segurança de uma organização".

A norma ISSO/IEC 17799:2005, estabelece as principais diretrizes para implementar e melhorar o processo de segurança da informação. A norma visa atender aos requisitos estabelecidos através de análise e variação de risco.

3 PROCEDIMENTOS METODOLÓGICOS

A pesquisa desse artigo é do tipo descritiva e qualitativa. Conforme Gil (2008) uma pesquisa do tipo descritiva utiliza técnicas padronizadas de coleta de dados e tem como objetivo primordial a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Ainda segundo Gil (2008) a análise dos dados em pesquisas qualitativas passa a depender muito da capacidade e do estilo do pesquisador, que ao contrário do que ocorre nas pesquisas de natureza quantitativa, não há fórmulas ou receitas predefinidas para orientar os pesquisadores. Para Flick (2009) esse tipo de abordagem consiste nas reflexões do pesquisador a respeito de sua pesquisa como parte do processo de produção do conhecimento, demonstrando as variações na perspectiva sobre o objeto de estudo.

A pesquisa foi realizada em uma organização que atua com serviços de planos de saúde, localizada na cidade de Mossoró, Rio Grande do Norte. Para a realização da pesquisa os autores elaboraram um questionário contendo 10 questões, objetivando identificar os mecanismos de segurança utilizados e as possíveis ameaças presentes na organização. A pesquisa foi realizada por meio de um dos pesquisadores, onde foi realizada uma entrevista presencial com um analista de sistemas e um gestor do departamento de TI. A coleta dos dados se deu por meio de gravações das falas, sendo realizadas no mês de setembro de 2017. Segue as informações dos participantes da pesquisa no quadro 1.

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

Quadro 1 - Caracterização dos sujeitos e pesquisa

Código do entrevistado	Sexo	Idade	Estado civil	Escolaridade	Cargo	Tempo de trabalho na organização
E1	M	38	Casado	Pós-graduado	Gerente de ti	14 anos e 2 meses
E2	M	37	Casado	Graduado em bsi	Analista de sistemas	3 anos e 5 meses

Fonte: elaborado pelos autores (2017).

Essa pesquisa utiliza o método ANS – Análise do Núcleo de Sentido para a análise dos dados. Segundo Mendes (2007) é uma técnica de análise de textos produzidos pela comunicação oral e/ou escrita, consistindo no desmembramento do texto em unidades, em núcleos de sentido formados a partir dos temas do discurso. Aplicado por meios sistemáticos envolvendo definição de critérios para análise, com a finalidade de agrupar o conteúdo latente e manifesto do texto, baseando-se em temas constitutivos de um núcleo de sentido, em definições que deem maior suporte às interpretações.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 Utilização de programas de segurança

Conforme visto dentre os inúmeros tipos de ameaças existentes e as diferentes classificações que especialistas dão a essas ameaças, basicamente uma parte significativa das ameaças envolve como exemplo: espionagens, invasões, códigos maliciosos por meio de correio-eletrônico, entre outras, tendo como canal as redes de computadores para a realização de suas ações danosas.

Na entrevista os participantes confirmam que fazem uso de um dos tipos de programas de segurança mais básicos.O E2 chega a acrescentar o uso de outros recursos de segurança, porém não informa do que realmente se trata, conforme trecho a seguir:

> E1: Apenas o antivírus.
> E2: A gente utiliza apenas os antivírus e algumas rotinas de segurança interna.

Na obra de Dantas (2011), menciona-se a 9ª Pesquisa Nacional de Segurança da Informação, abordando as três medidas de segurança mais implementadas pelas empresas: antivírus (90%), sistemas de *backup* (76,5%) e *firewall* (75,5%). Considerando o que foi relatado pelos entrevistados, os mesmos devem apresentar esse mesmo conjunto básico de segurança.

Também importante é a questão do treinamento que visa reduzir as chances de casos onde usuários mal instruídos cometem danos aos ativos da organização. Conforme a classificação dada por Peixoto (2004) esses usuários se apresentariam como uma ameaça de natureza involuntária no qual poderiam causar acidentes.

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

As respostas dos entrevistados evidenciam que se tratando de software, os únicos recursos de segurança que possuem são de fato os descritos anteriormente, e que dada a forma como os softwares operam, treinamentos não são necessários, vejamos:

> *E1: Não foi feito nenhum treinamento, já que o programa opera automaticamente.*
> *E2: A gente não necessita de treinamento, pois os membros já são operados automaticamente e com isso dispensa a questão de treinamento.*

4.2 Realização da análise e avaliação dos riscos

Nessa fase ocorre à identificação dos ativos da empresa, de vulnerabilidade, ameaças e probabilidade dos riscos ocorrerem, onde a gestão estabelecerá critérios para a aceitação dos riscos, com base nos níveis alto ou baixo, considerando, ainda, a questão de orçamento. Questionando os entrevistados se a gestão responsável pela segurança da informação realiza a análise e avaliação dos riscos, ambos chegam a confundir a gestão de segurança da informação como um setor físico e apropriado para tal função. O E1 não confirmou a realização da atividade, confundindo-a com software, que é realizado pelo o setor de TI da organização, o que talvez implique em despreparo ou simples desconhecimento, vejamos:

> E1: A equipe não possui um setor responsável apenas pela segurança, todo o setor de informática faz todo trabalho responsável pelo o software.
> E2: Não há. A gente não tem nenhum setor especifico somente para a área de segurança, a equipe de TI é quem realiza os procedimentos necessários periodicamente.

Ainda sobre o mesmo questionamento, foram indagados se a análise e avaliação dos riscos eram realizadas periodicamente. Percebeu-se na fala do E2 quando diz que "os procedimentos necessários são realizados pelo setor de TI", porém não afirmou a existência de tais procedimentos, contudo abordou que esse tipo de tarefa (ou semelhante) é realizada de maneira periódica. No final acaba-se por não identificar uma existência concreta dessa atividade, o que não é bom, já que tecnologias, processos de negócio e pessoas mudam constantemente, o que faz com que alterem o nível de riscos atuais, gerando novos à organização, conforme Rigon e Whestpall (2013) fazendo-se necessária a análise e avaliação dos riscos de forma metódica.

Quando questionados sobre o sentimento de segurança da empresa, após a implantação de novos mecanismos de segurança, ambos os entrevistados não souberam dá uma resposta exata para esse questionamento. Com base nisso, é possível constatar que existe uma ausência de implantação de novos mecanismos de segurança, o que revela que implementações desse recurso no departamento não é frequente, implicando em aumento significativo no nível de riscos.

4.3 Adesão a normas de gestão de segurança da informação

A adesão a normas que envolvem a segurança da informação é muito útil às organizações que buscam dar seus primeiros passos no desenvolvimento e implantação de controles de segurança da informação. Tem por objetivo estabelecer diretrizes e princípios

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

gerais, ajudando ainda a manter e melhorar a gestão de segurança da informação da organização. Questionando os entrevistados sobre a existência de adesão a normas por parte da organização, ambos apresentaram respostas semelhantes.

> E1: O único conjunto de boas práticas que a gente faz é não utilizar os computadores em sites maliciosos.
> E2: A única prática que a gente segue é o bloqueio de todos os terminais e acessos a sites maliciosos, a gente não dá abertura.

Como observado ambas as respostas se assemelham, dando destaque ao E2 quando fala a respeito do bloqueio de todos os terminais e acesso a sites maliciosos, pois tal comportamento se encaixa dentro das rotinas de segurança interna.

Conforme relatado pelos participantes, a organização não utiliza nenhuma norma de gestão de segurança da informação, atendendo apenas a procedimentos considerados "boas práticas de segurança". Aparentemente a organização utiliza os mecanismos mais adotados em organizações que ainda não possuem muito conhecimento em segurança da informação, então fazem usos dos recursos considerados mais básicos e essenciais e não seguem um modelo de gestão específico. A seguir, os entrevistados abordam sua percepção em relação a mudanças proporcionadas em função de seus recursos de segurança:

> E1: Não foi possível notar nenhuma melhoria... a melhoria acontece em segundo plano.
> E2: O programa que a gente trabalha opera em segundo plano, e com isso, não foi possível notar nenhuma melhoria.

Ainda segundo os entrevistados, a organização nunca teria sofrido um incidente que tivesse causado perdas de confiabilidade, integridade ou disponibilidade da informação, conforme os trechos que se seguem:

> E1: A empresa nunca sofreu um problema que causasse perda de confiabilidade.
> E2: A gente nunca sofreu nenhum incidente.

Desta forma, percebe-se que a organização investigada possui confiabilidade no processo informacional.

5. CONSIDERAÇÕES FINAIS

O presente estudo teve por objetivo compreender os mecanismos de segurança de informação utilizados na atuação de possíveis ameaças no ambiente organizacional de uma empresa que atua prestando serviços de planos de saúde, da cidade de Mossoró, Rio Grande do Norte.

Levando em conta a relevância do assunto de segurança da informação dentro do contexto organizacional, faz-se necessário a realização de estudos a fim de compreender como a organização atua quando o assunto é a segurança de suas informações que se mostram um de seus ativos mais importantes, servindo para compreender o atual cenário em que essas organizações se encontram e servindo também para o reconhecimento com o tema discutido.

Revista Conhecimento Contábil, ISSN 2447-2921,Mossoró/RN, UERN; UFERSA.
Vol. 06, n. 01, p. 70-80 Jan /Jun., 2018
Recebido em: 29/02/2018/Aprovado em: 29/05/2018

Com a realização do presente estudo foi possível concluir que a organização alvo da pesquisa utiliza mecanismos de segurança comuns, os quais se encontram presentes na maioria das organizações, porém a mesma possui limitações em demonstrar que não inovam em recursos de segurança, e acabam dependendoapenas dos já existentes.

O setor de TI da organização também não realiza tarefas importantes para diminuir a exposição de riscos que venham a surgir com mudanças nos requisitos das atividades do negócio, não seguindo nenhum conjunto de normas, e apresentando também pouco conhecimento sobre o assunto conforme mostram as falas dos entrevistados, mantendo assim um processo informal de segurança de informação, e mostrando a necessidade de aprofundamento no assunto por parte do setor de TI da organização.

Por fim, a pesquisa apresentou limitações, pois algumas das questões utilizadas no questionário não obtiveram resposta por parte dos entrevistados, dada a limitação existente nos recursos de segurança da informação utilizados pela organização, porém, não apresentando problemas para elaboração da análise dos resultados obtidos. Acerca das sugestões para trabalhos futuros, não fazia parte do escopo desta pesquisa a realização de estudos de casos visando à identificação de vulnerabilidades existentes por meio de processos de analises de riscos, o que embora fosse útil, não só para identificação de vulnerabilidades e ameaças, mas para o nível de exposição da organização.

REFERENCIAS

ABNT NBR ISO/IEC17799. **Tecnologia da informação** - Técnicas de segurança - Código de práticas para a gestão da segurança da informação. Rio de Janeiro, 2005.

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

FLICK, Uwe. **Introdução à pesquisa qualitativa**. 3ª edição. Porto Alegre: Artmed, 2009.

GIL, Antônio Carlos (2008)**. Métodos e técnicas de pesquisa social**. Editora Atlas S.A, São Paulo.

JANSSEN, LuisAntônio (2008). **Instrumento de avaliação de maturidade em processos de segurança da informação:** estudo de caso em instituições hospitalares. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul. Disponível em < http://repositorio.pucrs.br/dspace/handle/10923/1240 >. Acesso em: 16 julho 2017.

KLETTENBERG, Josiane, et al. **Segurança da informação:**Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias. Dissertação de Mestrado. Disponível em<https://repositorio.ufsc.br/handle/123456789/172575>Acesso em: 6 de setembro 2017.

KROLL, Josiane;DORNELLAS, Marcos Cordeiro. **Aplicação da Metodologia de Avaliação de Riscos para o Gerenciamento Estratégico da Segurança da Informação.** In: XLI

SIMPÓSIO BRASILEIRO DE PESQUISA OPERCIONAL, 2009, At Porto Seguro, BA. Santa Maria: Universidade Federal de Santa Maria, 2009. p.2254-2261.Disponível em <http://www.din.uem.br/sbpo/sbpo2009/artigos/55438.pdf>. Acesso em: 7 de setembro 2017.

MARCIANO, João Luiz Pereira; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação**. Ci. Inf., Brasília,** v. 35, n. 3, p. 89-98., 2006.

MENDES, Ana. **Psicodinâmica Do Trabalho:** Teoria, Método e pesquisas. Casa Psi Livraria, Itatiba/SP. All Books Casa do Psicólogo, São Paulo/SP, 2007.

PEIXOTO, Mário César Pintaudi. **Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas organizações.** Monografia (Bacharel em Ciências da Computação) - Centro Universitário do Triângulo, Uberlândia, 2004.

RIGON, Evandro Alencar; WESTPHALL, Carla Merkle. Modelo de avaliação da maturidade da segurança da informação. **Revista Eletrônica de Sistemas de Informação**, v. *12*, n. 1, 2013..

SILVA NETTO, Abner da;PINHEIRO, Silveira da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. JISTEM: **Journal of Information Systems and Technology Management.** *V. 4, n.* 3, 2007..