GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO NUMA INSTITUIÇÃO PÚBLICA FEDERAL: UM ESTUDO DE CASO

MANAGEMENT OF INFORMATION SECURITY RISKS IN A FEDERAL PUBLIC INSTITUTION: A CASE STUDY

Recebimento: 31/08/2016- Aceite : 01/10/2016- Publicação: 29/11/2016
Processo de Avaliação: Double Blind Review

Jackson Gomes Soares Souza[1]
Graduação em Ciência da Computação pela Universidade Federal de Uberlândia
Professor do Instituto Federal de São Paulo.
jackson@ifsp.edu.br

Carlos Hideo Arima
Doutorado em Controladoria e Contabilidade pela Universidade de São Paulo (USP)
Professor do Mestrado do Centro Paula Souza e da Pontifícia Universidade Católica de São Paulo (PUC-SP)
charima@uol.com.br

Renata Maria Nogueira de Oliveira
Mestre em Gestão e Tecnologia de Sistemas Produtivos
Centro Paula Souza
renata_mno@hotmail.com

Getulio Kazue Akabane
Pós-Doutorado Tokyo University of Marine Science and Technology,Tokyo-Japão (TUMST)
Doutorado em Administração – Fundação Getúlio Vargas
Professor da Pontifícia Universidade Católica de São Paulo (PUC-SP)
getulio@akabane.adm.br

Napoleão Verardi Galegale
Doutorado em Controladoria e Contabilidade pela Universidade de São Paulo
Professor do Mestrado do Centro Paula Souza e da Pontifícia Universidade Católica de São Paulo (PUC-SP)
nvg@galegale.com.br

[1] *Autor para correspondência: IFSP AESP: Instituto Federal de São Paulo – Escola de ciências e tecnologia de São Paulo. R: Pedro Vicente, 625, Canindé, São Paulo – SP – Brasil – CEP: 01109-010.*

RESUMO

As instituições públicas vinculadas ao setor público federal brasileiro devem aplicar uma série de medidas de segurança, políticas, procedimentos e diretrizes como medidas de proteção de seus ativos de informação. Este estudo de caso único buscou verificar como a gestão de riscos de segurança da informação se apresenta numa instituição pública federal conforme a percepção dos gestores de Tecnologia da Informação (T.I.) e os resultados encontrados demonstram a importância dos papéis desempenhados pelas pessoas, as responsabilidades, o desenvolvimento de políticas, normas, procedimentos e implementação destes visando maior controle dos riscos e também das diversas oportunidades que envolvem a segurança de tecnologia da informação.

PALAVRAS-CHAVE: Governança Corporativa, Governança de T.I., Gestão de Riscos, Segurança da Informação.

ABSTRACT

Public institutions bound to the Brazilian federal public sector must apply security measures, policies, procedures and guidelines as information assets protection measures. This case study sought to determine whether the management of information security risks is applied in a federal public institution according to Information Technology (I.T.) managers perceptions and the results expose the importance of the roles played by people, responsibilities, policies, standards, procedures and their implementation aiming greater control of information security risks and opportunities related to information technology security.

KEYWORDS: Corporate Governance, I.T. Governance, Risk Management, Information Security.

INTRODUÇÃO

A segurança da informação trata da proteção dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados à informação, preservando a confidencialidade, integridade / autenticidade e disponibilidade de informações. O objetivo é mitigar riscos e proteger a informação das ameaças que têm impacto negativo sobre a continuidade do negócio e, em última instância maximizar o retorno sobre investimentos e oportunidades de negócios. (DA VEIGA; MARTINS, 2015; ISO/IEC 27002, 2013).

Uma consulta bibliométrica na base *Sopus* do termo segurança da informação (*Information Security*) referente ao período dos últimos 5 anos mostra que as produções

científicas vêm tendo um aumento significativo no meio acadêmico com aproximadamente 17.000 artigos. Porém, no que se refere à gestão de riscos de segurança da informação, especialmente no setor público (*Information Security Risk Management + Public Sector*), apenas 16 artigos foram encontrados.

No Brasil, mais especificamente no setor público, a segurança da informação é agenda estratégica, existindo uma gama de dispositivos legais e normas que tratam de sua aplicação nos órgãos vinculados ao Governo Federal e cuja observância é obrigatória. Aliado a isto, recentes estudos como o de Araújo (2012) apresentam a importância do tema e como o mesmo é ainda pouco explorado neste âmbito.

O volume de informações eletrônicas utilizadas pelas empresas é cada vez maior, tornando complexo seu gerenciamento produtivo e adequação da qualidade de acesso, confiabilidade e conformidade com vistas a atender os objetivos organizacionais, assim como há a preocupação com sua exposição, cuja segurança pode ser comprometida por incidentes que representariam prejuízos financeiros ou para a imagem das organizações (POSTHUMUS, 2004; ALEXANDRIA, 2009).

O termo Tecnologia da Informação (T.I.) em sua forma ampla inclui os sistemas de informação, o uso de *hardware* e *software*, telecomunicações, automação e recursos multimídia, utilizados pelas organizações para fornecer dados, informações e conhecimento; e as organizações utilizam cada vez mais a T.I. como apoio para alcançar os objetivos e metas de negócio, buscando maior eficácia organizacional e vantagem competitiva (LAURINDO *et al.*, 2001; LUFTMAN, 2003).

Uma boa governança corporativa permite que as organizações trabalhem com eficiência e de forma produtiva, garantindo a transparência da responsabilidade gerencial tanto em organizações privadas como no setor público (AKABANE, 2012) e, desta forma, a T.I. é vista pelas organizações como um importante ativo, agindo como uma força motriz que provê soluções cada vez mais complexas, de modo que sua governança é um fator crítico de sucesso e está presente nos projetos executivos organizacionais apoiando aos objetivos do negócio (HARDY, 2006; ITGI, 2003; VAN GREMBERGEN *et al.*, 2004).

Este estudo se justifica, portanto, pela dificuldade encontrada por algumas organizações em aplicar boas práticas, especialmente no que tange à segurança de seus ativos de informação e a governança de T.I. e busca identificar, por meio de um estudo de caso, se a gestão de riscos de segurança da informação é aplicada numa instituição pública federal na percepção dos gestores de T.I. e responder ao seguinte questionamento: Os princípios de segurança da informação que envolvem a gestão de riscos são aplicados em uma instituição pública federal?

1. . REFERENCIAL TEÓRICO

A presente pesquisa se apoia nos conceitos de segurança da informação e gestão de riscos, bem como o tratamento do assunto pelo setor público brasileiro que são apresentados na sequência.

1.1. Segurança Da Informação E Gestão De Riscos

O risco é inerente a toda atividade humana. A capacidade de definir o que acontecerá no futuro e optar entre várias alternativas é central às sociedades contemporâneas. A administração do risco nos guia por uma ampla gama de tomada de decisões, sendo necessária atenção às possíveis falhas ou erros e isto inclui a informação e a complexa tecnologia envolvida em seu processo (BERNSTEIN, 1997).

Ainda segundo o autor, grande parte do ato de correr riscos baseia-se em oportunidades desenvolvidas a partir de desvios da normalidade e, se todos avaliassem o risco exatamente da mesma forma, fatos considerados negativos não seriam transformados em verdadeiras oportunidades.

A prevenção da perda, dano, destruição ou acesso não autorizado à informação processada por organizações é uma evolução contínua e a segurança da informação tem chamado cada vez mais a atenção de pesquisadores, profissionais, jornalistas, legisladores e cidadãos. Governos e organizações se sensibilizam e investem cada vez mais na segurança de seus ativos de informação, auxiliando não somente a tomada de decisões, mas também a melhoria e continuidade de suas operações (JOURDAN *et al*., 2010).

A tecnologia é um artefato geralmente visível na organização. Tal evidência é o resultado da implementação de componentes de segurança da informação tais como de riscos e política de segurança (SCHEIN, 1985).

A T.I. em sua forma ampla inclui os sistemas de informação, o uso de *hardware* e *software*, telecomunicações, automação e recursos multimídia, utilizados pelas organizações para fornecer dados, informações e conhecimento; e as organizações utilizam cada vez mais a T.I. como apoio para alcançar os objetivos e metas de negócio, buscando maior eficácia organizacional e vantagem competitiva (LAURINDO *et al.*, 2001; LUFTMAN, 2003).

Os sistemas de informação estão sujeitos a ameaças que podem tanto oferecer oportunidades como ter impactos negativos sobre as operações da organização, incluindo missão, funções, imagem, reputação, os ativos, os indivíduos, assim como comprometer a confiabilidade, integridade, autenticidade e disponibilidade de informações que estão sendo processados, armazenados ou transmitidos por esses sistemas (NIST, 2010).

A segurança da informação trata da proteção dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados à informação. Ele preserva a confidencialidade (a informação é acessível somente por pessoas autorizadas), a integridade e autenticidade (exatidão e completude da informação), a disponibilidade (deve estar acessível, sempre que necessário, a pessoas autorizadas) de informações. O objetivo é proteger a informação das ameaças que têm impacto sobre a continuidade do negócio e, em última instância maximizar o retorno sobre investimentos e oportunidades de negócios (DA VEIGA; MARTINS, 2015; ISO/IEC 27002, 2013).

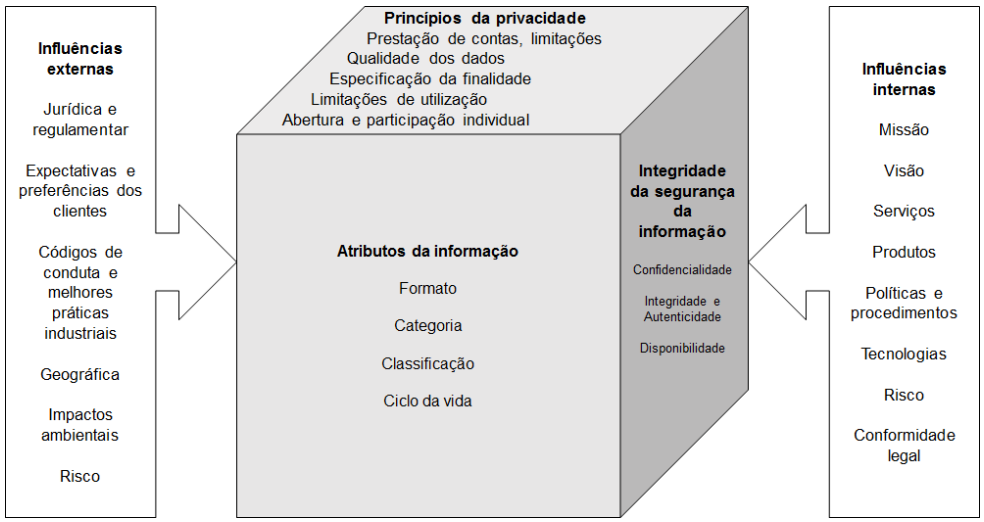
Influenciadas por suas necessidades, objetivos, exigências de segurança, processos, tamanho e estrutura, as organizações tendem a especificar e implementar estrategicamente um Sistema de Gestão de Segurança da Informação (SGSI) que atenda às necessidades da organização. Em sua recente atualização, a norma ISO/IEC 27001:2013 padroniza definições e estruturas de diferentes padrões ISO, alinhando-se com outros importantes padrões já existentes e propiciando uma gestão de riscos ainda mais efetiva ao incluir requisitos para a avaliação e tratamento de riscos de segurança da informação (ISO/IEC 27001, 2013).

Há também a proposta de uma abordagem de melhoria contínua por meio de um processo de criação, implementação, operação, monitoramento, revisão, manutenção e melhoria do SGSI da organização e adota o modelo Planejar-Executar-Monitorar-Agir, do inglês *Plan-Do-Check-Act (PDCA)*, considerando requisitos de segurança da informação e ações necessárias para atender as expectativas dos *stakeholders*. A adoção do modelo reflete, além de outros, os princípios de governança dos sistemas de informação e redes, análise de risco, especificação, implementação, administração e reavaliação da segurança (DA VEIGA; ELOFF, 2007; ISO/IEC 27001, 2005).

A privacidade da informação e sua segurança são dois conceitos inter-relacionados à proteção e ambos devem ser considerados ao se tratar dos riscos da informação. A dimensão da privacidade alinha as necessidades específicas da organização ao verificar princípios que estão em consonância com preferências organizacionais em diversos contextos. Além disto, um bom planejamento e implementação da segurança da informação requer não somente cooperação de toda a organização, como também por parte dos gestores (DA VEIGA, 2015; MONTESDIOCA; MAÇADA, 2015).

A Figura 1 apresenta o conjunto de atributos que representa uma visão abrangente da perspectiva de segurança e privacidade da informação.

Figura 1 – Atributos da informação pela perspectiva da privacidade e segurança da informação



Fonte: Da Veiga (2015), p. 6

Diversas abordagens de segurança da informação podem ser utilizadas no que se refere à implementação de controles de segurança (componentes) e ameaças aos ativos de informação. A ISO/IEC 27002:2005, reconhecida como uma norma essencial para a segurança da informação, define uma série de controles necessários à maioria das situações que envolvem T.I. (DA VEIGA, 2010).

Uma outra abordagem apresentada por Eloff e Eloff (2005) é denominada PROTECT, que é um acrônimo para Políticas, Riscos, Objetivos, Tecnologia, Execução, Conformidade e Time.

Tudor (2000), por sua vez, propõe uma abordagem abrangente e flexível de uma Arquitetura de Segurança da Informação para proteger os ativos de uma organização. Sua abordagem destaca cinco princípios fundamentais, listadas na Tabela 1, que são utilizadas para compreender o ambiente de risco em que as organizações operam, a fim de avaliar e implementar controles para mitigar tais riscos, assim como há também um foco na legislação do país para garantir que informações confidenciais de cada organização esteja protegida em conformidade.

Tabela 1 – Princípios da Arquitetura de Segurança da Informação

1. **Organização de segurança e infraestrutura:** Papéis desempenhados pelas pessoas e responsabilidades são definidas e o suporte por parte da gerência executiva é estabelecido.
2. **Políticas de segurança, normas e procedimentos:** Políticas, normas e procedimentos são desenvolvidos.
3. **Programa de segurança:** Um programa de segurança da informação é organizado tendo em conta a gestão de riscos.
4. **Conscientização para a segurança da cultura e da formação:** Os usuários são treinados e há reflexo da conscientização nas diversas atividades desenvolvidas. Há confiança entre os usuários, a gerência e os terceiros.
5. Adequação: Existe um controle interno e externo da segurança da informação.

Fonte: Tudor (2000) adaptado por Da Veiga e Eloff (2007)

Os princípios abrangem aspectos de processos e de tecnologia para direcionar necessidades de segurança das organizações.

O primeiro princípio diz respeito à organização de segurança e infraestrutura com funções e responsabilidades definidas, bem como a apoio gerencial.

O segundo princípio diz respeito às políticas de segurança, normas e procedimentos de gestão, destacando a importância de seu desenvolvimento e implementação. Os requisitos de

controle de segurança estabelecidos nas políticas de segurança não podem ser implantados de forma isolada, devendo considerar os riscos para a organização.

Portanto, como um terceiro princípio, as avaliações de risco devem ser realizadas em todas as plataformas, bancos de dados, aplicativos e redes, assim como um processo deve ser instituído visando fornecer um orçamento adequado de recursos para enfrentar os riscos e implementar controles. Para que os controles atuem de forma eficaz, os usuários precisam estar cientes da sua responsabilidade e incentivados a participar de programas de treinamento.

O quarto princípio visa estabelecer um ambiente de confiança entre os usuários, gestão e terceiros para permitir transações e proteger a privacidade.

O quinto e último princípio concentra-se na verificação da conformidade e auditorias por auditores internos e externos para monitorar a eficácia do programa de segurança.

2. SEGURANÇA DA INFORMAÇÃO NO SETOR PÚBLICO BRASILEIRO

Independentemente de serem governamentais, privadas ou públicas, a maioria das instituições está aplicando uma série de contramedidas de segurança, políticas, procedimentos e diretrizes como medidas de proteção (JOURDAN *et al*., 2010).

Esta consciência deve-se ao fato de que incidentes de segurança podem causar consequências adversas para organizações, podendo afetar ativos de informação, a reputação organizacional, a confiança do cliente, a produtividade dos empregados e até mesmo riscos de âmbito legal (DZAZALI et al., 2009; SHEDDEN et al., 2011).

Não somente os requisitos regulamentares estão aumentando, mas também as responsabilidades de governança em supervisionar cada vez mais a segurança da informação, uma vez que esta provê uma forte ligação entre o corpo diretivo, a gerência executiva e os responsáveis pela implementação e operação de um sistema de gestão de segurança da informação que irá apoiar os objetivos da organização (ISO/IEC 27001, 2013).

Um levantamento da legislação brasileira relacionada à Segurança da Informação e Comunicações (SIC) feito por Vieira e Fraga (2014), elenca regulamentos abrangendo a legislação de caráter federal, estadual e municipal e, conforme demonstra a Tabela 2, existe uma grande quantidade de dispositivos legais, decretos, leis, instruções normativas e projetos de lei relacionados ao tema.

Araújo (2012) aponta também por meio de uma revisão na legislação que, quando atualizado para 2016 apresenta a existência de 2 instruções normativas e 14 normas complementares cujo conteúdo dos documentos deve ser observado por todos os órgãos da gestão pública federal e reitera, portanto, o fato de que as organizações públicas e arquivos públicos são também fortemente regulados e fiscalizados por órgãos de regulação e controle da Administração Pública, como Ministério do Planejamento, Orçamento e Gestão (MPOG), Controladoria Geral da União (CGU) e Tribunal de Contas da União (TCU) (ALBUQUERQUE JR.; SANTOS, 2014).

Tabela 2 – Legislação relacionada à segurança da informação

Regulamento	Quantidade
Dispositivos legais de caráter federal	83
Legislação específica federal	50
Legislação específica estadual/distrital	6
Legislação específica municipal	2
Normas Técnicas	8
Projetos de lei	13
TOTAL	**162**

Fonte: Adaptado de Vieira e Fraga (2014)

3. MÉTODO

A pesquisa realizada neste trabalho pode ser classificada como qualitativa e exploratória baseada em um processo indutivo que explora, descreve e em seguida gera perspectivas teóricas (SAMPIERI *et al.*, 2006). Desta forma, consiste em um estudo de caso único que tem como objetivo verificar se a gestão de riscos de segurança da informação é aplicada em uma instituição pública de ensino na percepção dos gestores de T.I..

Conforme salienta Yin (2001), o estudo de caso é uma inquirição empírica que investiga fenômenos contemporâneos inseridos em algum contexto da vida real e permite a utilização de fontes de evidências como a observação direta e entrevistas. Ainda segundo o autor, os estudos de caso, em geral, possuem três etapas principais: definição e planejamento; preparação, coleta e análise de dados; e análise das informações e conclusão, conforme detalhados a seguir:

1) Definição e planejamento

- Escolha do caso: Informações obtidas no estudo bibliométrico mostram que existem poucas pesquisas sobre gestão de riscos de segurança da informação aplicadas no mesmo contexto do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. Além disto, a escolha se deu devido à facilidade de contato do autor com os diretores responsáveis pela governança de T.I., assim como limitações de tempo, recursos financeiros, materiais e pessoas (MATTAR, 1996). O processo de amostragem adotado nesta pesquisa pode ser classificado como não-probabilístico e por conveniência (FOWLER, 1991; MALHOTRA, 2001; SCHIFFMAN; KANUK, 2000). Amostras por conveniência podem ser facilmente justificadas em um estágio exploratório da pesquisa e para estudos em que o pesquisador aceita os riscos da imprecisão dos resultados do estudo (CHURCHILL, 1998; KINNEAR; TAYLOR, 1979).

- Critério de escolha dos entrevistados: A amostra consiste de entrevistados que, além de serem diretores de T.I. capacitados, possuem contato frequente com o tema e se disponibilizaram voluntariamente para participar da pesquisa (AAKER, *et al.*, 1995; FREITAS *et al.*, 2000; KISH, 1965; MATTAR, 1996).

- Elaboração do protocolo do estudo de caso: o protocolo para o estudo foi desenvolvido para a coleta de dados que, neste caso, foi realizada por meio de um questionário estruturado: instrumento de coleta de dados constituído por uma série ordenada de perguntas (LAKATOS, 2003).

2) Coleta e análise de dados

- Aplicação do questionário: com base nas questões apontadas no protocolo para o estudo de caso e no critério de escolha dos entrevistados, foi aplicado o questionário para o levantamento de informações. Buscando obter uma amostra variada, os questionamentos foram aplicados a diretores responsáveis por diferentes áreas de T.I., durante o segundo semestre de 2015.

- Elaboração de relatório preliminar: a partir das informações obtidas do questionário aplicado, um relatório preliminar do caso é elaborado para análise detalhada.

3) Análise das informações e conclusão

- Análise das informações: a partir do relatório preliminar elaborado, é realizada uma análise detalhada das respostas obtidas.

- Elaboração das conclusões: registro das observações decorrentes da análise dos resultados.

O protocolo de estudo, além de aumentar a confiabilidade da pesquisa, contém os procedimentos e as regras gerais para conduzir e realizar o estudo e oferece segurança de que o trabalho científico foi realizado com planejamento e execução que garantiram resultados que de fato possibilitaram explicações sobre a realidade investigada. (YIN, 2001; MARTINS, 2006; MARTINS; THEÓPHILO, 2007)

As seguintes seções compõem o protocolo do estudo de caso:

- Visão geral do projeto do estudo de caso: contém os objetivos, as questões do estudo de caso etc.
- Procedimentos de campo: apresentação das credenciais do pesquisador, locais de estudo, fontes de informação etc.
- Questões do estudo de caso: questões específicas para a coleta de dados.

Os Institutos Federais de Educação, Ciência e Tecnologia são vinculados diretamente ao Ministério da Educação e fazem parte da Rede Pública Federal de Educação Profissional, Científica e Tecnológica, cobrindo todos os estados brasileiros, oferecendo cursos técnicos, superiores de tecnologia, licenciaturas, mestrado e doutorado. São instituições de educação superior, básica e profissional, especializadas na oferta de educação profissional e tecnológica gratuita em diferentes modalidades, bem como realização de pesquisa aplicada e promoção do desenvolvimento tecnológico de novos processos, produtos e serviços, especialmente de abrangência local e regional, oferecendo mecanismos para a educação continuada com estreita articulação com os setores produtivos e a sociedade (BRASIL, 2015).

Integrante desta rede, a estrutura *multicampi* do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, conta com aproximadamente 1.100 (mil e cem) docentes, 600 (seiscentos) administrativos e possui aproximadamente 24 mil alunos matriculados nos 38 *campi*, mais 4 mil alunos nos 19 polos de educação a distância distribuídos pelo estado de São Paulo. Sua estrutura organizacional é composta pelo Gabinete do reitor, Pró-reitoria de Administração, Pró-reitoria de Desenvolvimento Institucional, Pró-reitoria de Ensino, Pró-reitoria de Extensão e Pró-reitoria de Pesquisa e Inovação (BRASIL, 2015).

A área de T.I. do IFSP está vinculada à Pró-reitoria de Desenvolvimento Institucional e conta com Assessoria de Tecnologia da Informação, Diretoria de Sistemas da Informação, Diretoria de Infraestrutura e Redes e Diretoria adjunta de Suporte em Tecnologia da Informação (BRASIL, 2015).

Para esta pesquisa, busca-se responder à seguinte pergunta: A gestão de riscos de segurança da informação é aplicada na instituição pública de ensino na percepção dos gestores de T.I.? Dessa forma, para definir o constructo foi utilizada a arquitetura de segurança da informação proposta por Tudor (2000) e adaptada por Da Veiga (2007), por destacar cinco princípios chave utilizados para compreender o ambiente de riscos na qual as organizações operam a fim de que estas possam avaliar e implantar controles para mitigar estes riscos. Além de avaliar os aspectos do risco de segurança da informação, a arquitetura foca também em garantir que informações confidenciais estejam protegidas em conformidade com a legislação.

4. ANÁLISE DOS DADOS E DISCUSSÃO

Conforme o Quadro 3, as respostas obtidas por meio dos 4 questionamentos referentes ao perfil dos respondentes são relativamente variadas, sendo que dois deles atuam há menos de 2 anos como diretores de T.I. e o restante há mais de 2 anos.

QUADRO 3 – Perfil dos respondentes

DIRETORES	TEMPO	ESCOLARIDADE	FAIXA ETÁRIA
D1	até 2 anos	Pós-Graduação (Extensão)	40 anos ou mais
D2	até 3 anos	Mestrado	20 anos ou mais
D3	até 3 anos	Pós-Doutorado	40 anos ou mais
D4	até 1 ano	Pós-Graduação (Extensão)	20 anos ou mais
D5	até 3 anos	Pós-Graduação (Extensão)	20 anos ou mais

Fonte: Resultado da Pesquisa

Foi possível também verificar que o nível de escolaridade dos diretores de T.I. é de no mínimo Pós-Graduação *lato-sensu* em nível de extensão, mostrando que todos possuem especialização.

Na Tabela 3 constam as respostas classificadas de 1 (discordo totalmente) a 5 (concordo totalmente) dos 5 blocos de questionamentos referentes à organização de segurança e infraestrutura (P01, P02 e P03), políticas de segurança (P04, P05 e P06), normas e procedimentos (P07), programa de segurança, treinamento e conscientização da cultura de segurança (P08, P09 e P10) e, por fim, adequação (P11 e P12), contendo um total de 12 perguntas enumeradas de P01 a P12.

TABELA 3 – Respostas

DIRETORES	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12
D1	3	2	2	3	3	3	2	4	4	3	3	4
D2	2	2	3	4	4	4	2	3	2	2	3	1
D3	3	3	4	4	3	3	4	2	2	3	3	3
D4	5	5	4	5	5	4	3	2	4	3	1	2
D5	3	3	4	4	4	2	2	3	1	1	1	5
TOTAL	**16**	**15**	**17**	**20**	**19**	**16**	**13**	**14**	**13**	**12**	**11**	**15**

Fonte: Resultado da Pesquisa

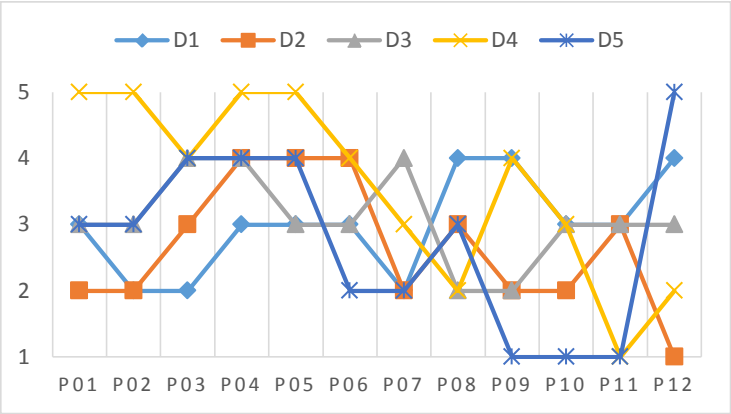
Ao analisar as respostas no que diz respeito à organização de segurança e infraestrutura, verifica-se que uma quantidade considerável destas está na faixa neutra e as demais divergem principalmente no que se refere à definição dos papéis desempenhados pelas pessoas e quanto à definição das responsabilidades, observa-se também uma maior discordância por parte dos

respondentes. Por outro lado, conforme a Figura 2, três respondentes concordam que há apoio por parte da gerência executiva.

Seria recomendável que fossem feitos estudos internos de forma a verificar como tornar mais claros os papeis desempenhados e as responsabilidades das pessoas neste contexto.

Quanto às políticas de segurança, normas e procedimentos de segurança da informação, os respondentes concordam em grande parte de que políticas e normas são desenvolvidas. Já no que se refere aos procedimentos as respostas apresentam certa neutralidade ou concordância.

Figura 2 – Gráfico de linhas



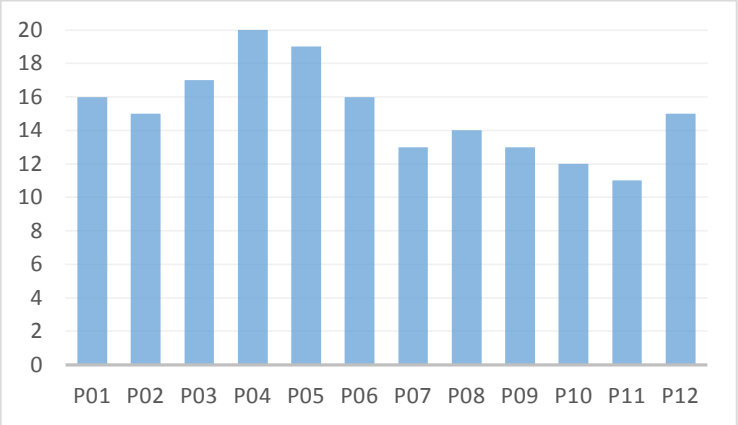
Fonte: Resultado da Pesquisa

Devido à sua relevância, seria recomendável que, além do desenvolvimento e implementação de políticas, normas e procedimentos, fosse dada atenção especial à implementação integrada dos requisitos de controle de segurança estabelecidos nestes de forma a reduzir riscos para a instituição.

A organização de um programa de segurança que leva em conta a gestão dos riscos para a instituição apresenta discordância por parte dos respondentes, o que pode sugerir a necessidade de uma maior atenção quanto à avaliação dos riscos que envolvem plataformas, bancos de dados, aplicativos em rede e outros, para que seja possível fornecer um orçamento adequado de recursos para atuar frente a possíveis riscos e implementar controles.

No que diz respeito à conscientização para a segurança da cultura e da formação, conforme apresentado na Figura 3, a soma das respostas indica baixa confiança entre os usuários, a gerência e os terceiros, apontando a necessidade de uma maior conscientização, e treinamento dos usuários de forma que estes estejam mais cientes de suas responsabilidades e incentivados a participar de programas de treinamento, aprimorando assim a proteção da privacidade.

Figura 3 – Gráfico de barras contendo a soma dos valores



Fonte: Resultado da Pesquisa

Por fim, quanto à adequação, as respostas sugerem que deve ser feita uma maior verificação da conformidade e auditorias, principalmente por auditores internos, de forma a monitorar a eficácia do programa de segurança da instituição.

CONSIDERAÇÕES FINAIS

Este estudo buscou identificar se a gestão de riscos de segurança da informação é aplicada numa instituição pública federal na percepção dos gestores de T.I.. Desta forma, os componentes de segurança da informação verificados podem ser descritos como os princípios que permitem a sua implementação e manutenção, tais como políticas de segurança da informação, avaliação de riscos, controles técnicos, e conscientização de segurança da informação.

A principal contribuição deste trabalho tanto na perspectiva prática quanto teórica reside na verificação de quais princípios de segurança da informação que envolvem a gestão de riscos são aplicadas na instituição em estudo. Tais princípios podem ser utilizados para entender o ambiente de risco em que as organizações operam, a fim de avaliar e implementar controles para mitigar estes riscos (DA VEIGA; ELOOF, 2007).

Não obstante, as limitações desta pesquisa referem-se à aplicação das técnicas para a coleta de dados, assim como restrições de tempo e recursos financeiros. Os resultados desta pesquisa foram baseados em uma amostragem não probabilística e não permitem generalizações a respeito da população em estudo, uma vez que a seleção de cada elemento dependeu do julgamento do pesquisador sendo, portanto, não aleatória (KISH, 1965; OLIVEIRA, 2001).

Sugere-se, desta forma, a ampliação desta pesquisa contemplando maiores amostras e a proposição de novos estudos dentro do contexto da gestão de riscos de segurança da informação no setor público federal.

REFERÊNCIAS

AAKER, D.; KUMAR, V. & DAY, G. Marketing research. John Wiley & Sons, Inc. 1995.

AKABANE, Getulio K.. Gestão estratégica da tecnologia da informação: conceitos, metodologias, planejamento e avaliações. São Paulo. Atlas, 2012.

ALBUQUERQUE JR., A. E.; SANTOS, E. M.. Análise das Publicações Brasileiras sobre Segurança da Informação sob a Ótica Social em Periódicos Científicos entre 2004 e 2013. XXXVIII Encontro da ANPAD, Rio de Janeiro, 13 a 17 set. 2014.

ALEXANDRIA, J. C. S. Gestão de segurança da informação – uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. Tese de Doutorado, Universidade de São Paulo, São Paulo, SP, Brasil, 2009.

ARAÚJO, Wagner J. LEIS, DECRETOS E NORMAS SOBRE GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL. Informação & Sociedade: Estudos, João Pessoa, v. 22, p.13-24, 2012.

BERNSTEIN, Peter L.. Desafio aos Deuses: A fascinante história do risco. Rio de Janeiro: Campus, 1997. 212 p. Tradução de: Ivo Korytowski.

BRASIL. Ministério da Educação. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. 2015. Disponível em: <http://www.ifsp.edu.br>. Acesso em: 11 nov. 2015.

CHURCHILL, G.. Marketing research: methodological foundations. 2a ed. The Dryden Press. 1998.

DA VEIGA, Adéle; ELOFF J.H.P.. An information security governance framework. Information Systems Management. África do Sul, 2007. 13p.

DA VEIGA, Adéle; MARTINS, Nico. Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, [S.l.], v. 31, n. 2, p.243-256, abr. 2015.

DZAZALI, S., SULAIMAN, A. and ZOLAIT, A.H.. Information security landscape and maturity level: case study of Malaysian Public Service (MPS) organizations. Government Information Quarterly. 2009. 9p.

ELOFF J.H.P.; ELOFF M.. Integrated Information Security Architecture. Computer Fraud and Security. 2005. 11p.

FOWLER, F, Jr.. Survey research methods. 8 ed. 1991.

FREITAS, H.; OLIVEIRA, M.; SACCOL, A. Z.; MOSCAROLA, J. O método de pesquisa survey. Revista de Administração, São Paulo, v.35, n.3, jul./set. 2000

HARDY, Gary. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security Technical Report, [S.l.], v. 11, n. 1, p.55-61, jan. 2006. Disponível em: <http://dx.doi.org/10.1016/j.istr.2005.12.004>. Acesso em: 03 jun. 2015.

ISO/IEC 27001:2005. Information technology – Security techniques – Information security management systems – Requirements. 2005

ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. 2013

ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for information security management. 2013.

ITGI. Board Briefing on IT Governance, Second Edition. Rolling Meadows, IL (EUA): IT Governance Institute, 2003. 7 p.

JOURDAN, Z.; RAINER, R.K.; MARSHALL, T.E.; FORD, F.N.. An investigation of organizational information security risk analysis. Journal of Service Science. Alabama. 2010. 9p.

KINNEAR, T. C.; TAYLOR, J. R. Marketing research: an applied aproach. Mc Graw Hill. 1979.

KISH, L. Survey sampling. John Wiley & Sons, Inc. 1965. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1002/bimj.19680100122/abstract>. Acesso em: 26 out. 2015.

LAKATOS, E. M.; MARCONI, M. A. Fundamentos de metodologia científica. São Paulo: Atlas, 2003.

LAURINDO, F. J. B.; SHIMIZU, T.; CARVALHO, M. M.; RABECHINI JR., R. O papel da Tecnologia da Informação (T.I.) na Estratégia das Organizações. Gestão & Produção, v. 8, n. 2, p. 160-179, 2001.

LUFTMAN, J. N. Assessing IT-Business alignment. Information Systems Management, 20(4), 9-15, 2003

MALHOTRA, N. K. Pesquisa de marketing. Uma orientação aplicada. 3 ed. Porto Alegre: Bookman, 2001.

MARTINS, G. A. Estudo de caso: uma estratégia de pesquisa. São Paulo: Atlas, 2006.

MARTINS, G. A.; THEÓPHILO, C. R. Metodologia da investigação científica para ciências sociais aplicadas. São Paulo: Atlas, 2007.

MATTAR, F. Pesquisa de marketing. Ed. Atlas. 1996.

MONTESDIOCA G.P.Z.; MAÇADA A.C.G.. Measuring user satisfaction with information security practices, Computers & Security. 2015. 13p.

OLIVEIRA, T. M. V.. Amostragem não Probabilística: Adequação de Situações para uso e Limitações de amostras por Conveniência, Julgamento e Quotas. Revista Administração On Line. FECAP. v. 2, n. 3, jul/ago/set. 2001. Disponível em: <http://www.fecap.br/adm_online/>. Acesso em: 10 nov. 2015.

POSTHUMUS, S., VON SOLMS, R. A Framework for the Governance of Information Security. Computers & Security, 23(8), 638-646, 2004.

SCHEIN E.H.. Organizational culture and leadership. São Francisco: Jossey-Bass, 1985.

SCHIFFMAN, L.; KANUK, L. Comportamento do consumidor. LTC Editora. 6a ed. 2000.

SHEDDEN, P., SCHEEPERS, R., SMITH, W. and AHMAD, A.. Incorporating a knowledge perspective into security risk assessments. Journal of Information and Knowledge Management Systems. 2011. 14p.

TUDOR, J. K.. Information Security Architecture – An integrated approach to security in an organization. Boca Raton, FL: Auerbach, 2000.

VAN GREMBERGEN, W.; DE HAES, S.; GULDENTOPS, E. Structures, Processes and Relational Mechanisms for IT Governance. Idea Group Publishing, 2004

VIEIRA, Tatiana Malta; FRAGA, Josemar Andrade. Quadro da legislação relacionada à segurança da informação e comunicações. 2014. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 25 out. 2015.

YIN, Robert K. Estudo de caso: planejamento e métodos. Porto Alegre: Bookman, 2001.