CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA
EM SISTEMAS PRODUTIVOS

JACKSON GOMES SOARES SOUZA

ANÁLISE DE TRATAMENTO DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE RISCOS DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO DE UMA INSTITUIÇÃO DE ENSINO PÚBLICO FEDERAL

São Paulo
Abril/2017

JACKSON GOMES SOARES SOUZA

ANÁLISE DE TRATAMENTO DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE RISCOS DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO DE UMA INSTITUIÇÃO DE ENSINO PÚBLICO FEDERAL

Dissertação apresentada como exigência parcial para a obtenção do título de Mestre em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a orientação do Prof. Dr. Carlos Hideo Arima

São Paulo

Abril/2017

Souza, Jackson Gomes Soares
S729a Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal / Jackson Gomes Soares Souza. – São Paulo : CEETEPS, 2017.
82 f. : il.

Orientador: Prof. Dr. Carlos Hideo Arima
Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, 2017.

1. Segurança da informação. 2. Gestão de riscos. 3. Governança de T.I. 4. Governança corporativa. I. Arima, Carlos Hideo. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

JACKSON GOMES SOARES SOUZA

ANÁLISE DE TRATAMENTO DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DE RISCOS DA GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO DE UMA INSTITUIÇÃO DE ENSINO PÚBLICO FEDERAL

Prof. Dr. Carlos Hideo Arima

Prof. Dr. Antonio Benedito Silva Oliveira

Prof. Dr. Getulio Kazue Akabane

São Paulo, 10 de abril de 2017

Dedico essa dissertação aos meus pais, esposa
e amigos que estiveram ao meu lado nesta
jornada.

AGRADECIMENTOS

Ao Prof. Dr. Carlos Hideo Arima, que, acreditando em minha capacidade, presenteou-me com esta oportunidade e me orientou no caminho da ciência.

Ao Prof. Dr. Getúlio Akabane por estar sempre disposto a aconselhar, direcionar e por ser um grande amigo.

Aos professores da Unidade de Pós-Graduação, Extensão e Pesquisa do Centro Estadual de Educação Tecnológica Paula Souza. Em especial aos professores Dr. Napoleão Verardi Galegale, Dr. José Manoel Souza das Neves, Dr. Carlos Vital Giordano e Dr. Antonio Benedito Silva Oliveira por me auxiliarem no desenvolvimento desta pesquisa.

Aos colegas de trabalho do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo que sempre me incentivaram.

Aos colegas mestrandos por me aturarem.

“Embora ninguém possa voltar atrás e fazer
um novo começo, qualquer um pode começar
agora e fazer um novo fim.”
Francisco Cândido Xavier

RESUMO

SOUZA, J. G. S. **Análise de tratamento da segurança da informação na gestão de riscos da governança de tecnologia da informação de uma instituição de ensino público federal**. 82 f. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2017.

A informação é um recurso crescente para o desenvolvimento do ciclo de negócios das organizações, e a Tecnologia da Informação (T.I.), assim como as pessoas envolvidas nesse ciclo, desempenha um papel significativo. A governança de T.I. consiste em aspectos de liderança, estrutura e processos para que a área de tecnologia da informação suporte e aprimore estratégias e objetivos organizacionais, tratando também dos riscos relacionados à segurança dos ativos de informação, uma vez que sua identificação e mensuração proporciona maior controle quanto às incertezas e oportunidades. Portanto, o presente trabalho tem por objetivo verificar o tratamento dado à segurança da informação dentro da gestão de riscos na governança de T.I. em uma instituição de ensino público federal, analisando aspectos da gestão de risco, que envolvem princípios como organização de segurança e infraestrutura, políticas de segurança, normas e procedimentos, programa de segurança, treinamento e conscientização da cultura de segurança e adequação. Trata-se de uma pesquisa exploratória mista, com estudo de uma instituição de ensino público federal desenvolvido por meio de questionários para levantamento e análise dos dados relativos às práticas de segurança da informação dentro da governança de T.I. A partir dos dados analisados, observou-se que os componentes verificados possuem aplicação na instituição, permitindo a implementação e manutenção de princípios, compreensão do ambiente de riscos no qual opera e oportunidades que este oferece.

Palavras-chave: Segurança da informação. Gestão de riscos. Governança de T.I.. Governança corporativa.

ABSTRACT

SOUZA, J. G. S. **Information security analysis on the risk management of a federal public education institution's information technology governance.** 82 p. Thesis (Master's in Production Systems Management and Technology). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2017.

Information is a growing asset in businesses life cycle, while Information Technology (I.T.) and the people involved in this cycle play a significant role. I.T. governance consists on aspects of leadership, structure and processes by enabling information technology to improve business strategies and objectives while securing the risks related to information assets, since their identification and measurement provides greater control over uncertainties and opportunities. Thus, this study aims to verify how is information security processed through risk management within I.T. governance in a federal public education institution, by analyzing risk management aspects involving principles such as security organization and infrastructure, security policies, standards and procedures, security program, security culture awareness and training and monitoring compliance. As a mixed exploratory research, this study was developed in a federal public education institution through questionnaires for data survey and analysis regarding information security practices within I.T. governance. Data analysis suggests that the verified components are applicable to the institution, enabling principles implementation, maintenance and acknowledgement of its risk environment and opportunities.

Keywords: Information security. Risk management. I.T. governance. Corporate governance.

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CGU	Controladoria Geral da União
COBIT	*Control Objectives for Information and Related Technology*
CPI	Comissão Parlamentar de Inquérito
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	*International Electrotechnical Commission*
IFSP	Instituto Federal de Educação, Ciência e Tecnologia de São Paulo
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
I.T.	*Information Technology*
ITGI	*I.T. Governance Institute*
MPOG	Ministério do Planejamento, Orçamento e Gestão
OECD	*Organisation for Economic Co-operation and Development*
SGSI	Sistema de Gestão de Segurança da Informação
TCU	Tribunal de Contas da União
T.I.	Tecnologia da Informação

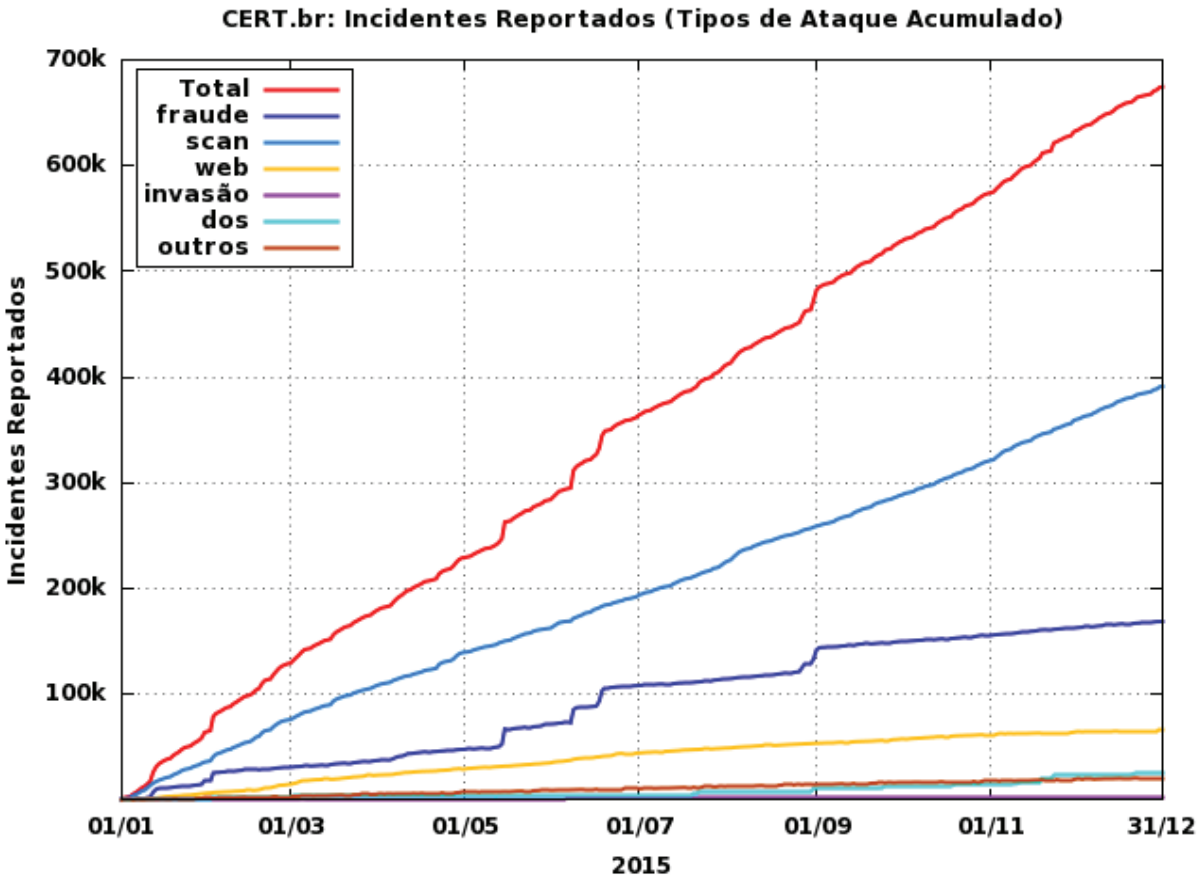
SUMÁRIO

INTRODUÇÃO

Ações para segurança da informação são praticadas desde tempos remotos. Singh (2001) apresenta várias situações na história da humanidade ao descrever esforços para proteger ou encontrar informações. Notícias sobre vazamento de informações sigilosas podem ser constatadas nos relatos de Ribeiro (2007) – informações de contribuintes da base dados da Receita Federal do Brasil – ou em O Globo (2012) – informações de uma CPI (Comissão Parlamentar de Inquérito) conduzida no Senado Federal (ARAÚJO, 2012).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil mantém estatísticas sobre notificações voluntárias e espontâneas de incidentes ocorridos em redes a ele reportados. A Figura 1 ilustra o cenário em que cerca de 600.000 ataques foram registrados no período de janeiro a dezembro de 2015 (CERT.BR, 2015).

Figura 1 – Incidentes reportados por tipos de ataque



Fonte: CERT.BR (2015)

A informação é, portanto, um recurso crescente para o desenvolvimento do ciclo de negócios das organizações. A Tecnologia da Informação (T.I.) e as pessoas envolvidas nesse ciclo desempenham um papel significativo, tendo em vista o avanço e a difusão de tecnologias nas organizações, nos ambientes sociais, públicos e corporativos. Tal atividade, destarte, deve ser tratada como um ativo estratégico (ISACA, 2012; NOBRE; RAMOS; NASCIMENTO, 2010).

A governança corporativa integra componentes de forma holística ao envolver princípios, processos, informação, serviços, infraestrutura, recursos humanos, além de *stakeholders* internos e externos responsáveis pela gestão destes componentes, proporcionando a estrutura pela qual os objetivos da organização são estabelecidos. Além disso, determina e monitora os meios para alcançar essas metas organizacionais e (OECD, 2015) permite, ainda, que as organizações trabalhem com eficiência e de forma produtiva, garantindo a transparência da responsabilidade gerencial, tanto em organizações privadas quanto no setor público. Desta forma, a T.I. é vista como um ativo, que age como uma força motriz provedora de soluções cada vez mais complexas, de modo que sua governança é um fator crítico de sucesso e está presente nos projetos executivos organizacionais para apoiar os objetivos do negócio (AKABANE, 2012; HARDY, 2006; VAN GREMBERGEN; DE HAES; GULDENTOPS, 2004; ITGI, 2003).

A T.I. se tornou, portanto, uma espécie de habilitador estratégico de negócio, sendo interessante que organizações ampliem ainda mais sua abrangência, de modo a agilizar o alinhamento dos objetivos do negócio e aprimorar produtos e serviços (LUNARDI *et al.* 2014).

Segundo o ITGI (2007), a governança de T.I. consiste em aspectos de liderança, estrutura e processos, para que a área de tecnologia da informação suporte e aprimore os objetivos e estratégias organizacionais. Além dessas características, integra e institucionaliza boas práticas, habilitando as organizações para melhor utilizarem seus ativos de informação, maximizando benefícios, capitalizando oportunidades e adquirindo vantagem competitiva. A Figura 2 ilustra as áreas de foco que contribuem para que haja transparência dos custos, do valor e dos riscos de T.I., conforme o modelo de Objetivos de Controle para Informação e Tecnologias Relacionadas (*Control Objectives for Information and Related Technology – COBIT*), versão 4.1.

Figura 2 – Áreas de foco na governança de T.I.

Fonte: ITGI (2007, p.8)

Ainda segundo o ITGI (2007), as áreas de foco ilustradas na Figura 2 contribuem com a governança de tecnologia da informação de modo que:

O alinhamento estratégico estabelece a relação entre os planos de negócios e de T.I., definindo, mantendo, validando e alinhando a proposta operacional de tecnologia da informação com as operações organizacionais.

Entrega de valor é a execução da proposta por meio do ciclo de entrega, que objetiva as entregas previstas na estratégia organizacional, concentrando-se em otimizar custos e promover o valor intrínseco de T.I..

Gestão de recursos busca a melhor utilização possível dos investimentos e o apropriado gerenciamento de recursos críticos, como aplicativos, informações, infraestrutura e pessoas. Refere-se, também, à otimização do conhecimento.

Mensuração de desempenho, por sua vez, diz respeito ao acompanhamento e monitoramento de processos, projetos, utilização de recursos, performance e entrega dos serviços que traduzem estratégias em ações voltadas a atingir os objetivos organizacionais.

Por fim, a gestão de risco trata do ambiente de riscos que envolve níveis, conformidade, transparência, funcionários, e seu gerenciamento nas atividades da organização, assim como lida com os riscos relacionados à segurança da informação. A identificação e mensuração desses riscos permitem que os gestores e demais envolvidos no processo tenham maior controle quanto às incertezas, impacto destas no objetivo do negócio e as oportunidades que proporcionam.

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

A governança de T.I. do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP) trata, dentro da gestão de risco, da política de segurança da informação, trabalhando diversos tipos de informações críticas diretamente relacionadas ao negócio, como informações acadêmicas dos alunos ou administrativas que influenciam na continuidade do negócio (BRASIL, 2016a). Essas informações circulam e são armazenadas em grandes volumes – tanto no ambiente interno como no externo –, em mídias físicas ou lógicas, utilizando, assim, um grande número de ativos, essenciais para o negócio da instituição. Assim, os recursos computacionais de rede, de comunicação, os documentos físicos gerados ou não por recursos computacionais e as informações desses recursos, como outros ativos da instituição, precisam ser protegidos (BRASIL, 2016b).

Questão de pesquisa

Qual tratamento é dado à segurança da informação dentro da gestão de riscos na governança de T.I. de uma instituição de ensino público federal?

Objetivo geral

Analisar os aspectos da segurança da informação dentro da gestão de risco dentro na governança de T.I. de uma instituição de ensino público federal.

Objetivos específicos

Identificar as variáveis de segurança da informação, consideradas aplicáveis para governança de tecnologia da informação.

Analisar o tratamento dado à segurança da informação dentro da gestão de riscos na governança de tecnologia da informação da instituição por meio de um estudo de caso.

Justificativa

Os problemas de vazamento de informações ou quebra de sigilo em organizações públicas são recorrentes, e o Governo Federal brasileiro vem implementando procedimentos para gestão de riscos da segurança da informação, com vistas a minimizar tais problemas. Grande parte dessas iniciativas está registrada em normas, decretos e leis (ARAÚJO, 2012).

A política de segurança da informação do IFSP se caracteriza pela tentativa de manter a confidencialidade, a integridade e a disponibilidade das informações, independentemente de onde ela esteja – residente em memória de máquinas e dispositivos, armazenada em disco, em trânsito ou impressas em documentos, salvaguardando sua exatidão e completeza por meio dos métodos de processamento, além de garantir que a comunidade tenha acesso à informação e aos ativos correspondentes sempre que necessário e de acordo com a permissão atribuída a cada um (BRASIL, 2016b).

Uma consulta bibliométrica na base *Scopus* sobre o 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* e *Public Sector*), apenas 16 artigos foram encontrados, sendo que nenhum deles refere-se ao setor público federal brasileiro.

Este estudo se justifica, portanto, pela necessidade de instituições em analisar suas atividades, especialmente no que tange à segurança de seus ativos de informação e às possíveis vulnerabilidades da T.I.; legitima-se, ainda, pelo objetivo de contribuir para que as incertezas envolvidas nesse processo possam ser mitigadas ao verificar qual tratamento é dado à segurança da informação dentro da gestão de riscos na governança de T.I. de uma instituição de ensino público federal.

Estrutura do trabalho

Este estudo está organizado de forma a apresentar, em linhas gerais, o problema de pesquisa, a fundamentação teórica, o estudo de caso, e as conclusões gerais. A seguir, apresenta-se, em detalhes, o que a estrutura contempla.

Primeiramente, a introdução já vem abordando a questão-problema, os objetivos da pesquisa, a justificativa e as contribuições do estudo, bem como esta seção referente à estrutura da dissertação.

A fundamentação teórica, então, é apresentada, abrangendo os principais conceitos sobre governança corporativa, governança de tecnologia da informação, gestão de risco e segurança da informação no setor público brasileiro.

Em seguida, são descritos os procedimentos metodológicos utilizados para a realização do estudo de caso, sua caracterização, protocolo, informações sobre a instituição, o estudo quantitativo e o estudo qualitativo, sendo também relatada a análise de resultados obtidos.

Por fim, encontram-se as conclusões obtidas, limitações desta pesquisa, sugestões de estudos futuros e as referências que foram utilizadas como base para o desenvolvimento deste trabalho, assim como materiais complementares – apresentados como apêndices.

1 FUNDAMENTAÇÃO TEÓRICA

Componente da governança corporativa, a governança de T.I consiste em aspectos de liderança, estrutura organizacional e processos que asseguram que a área de T.I. dê suporte e aprimore objetivos e estratégias. Portanto, é o campo capaz de habilitar a organização a melhor utilizar ativos de informação de forma segura, preservando sua confidencialidade, integridade, autenticidade e disponibilidade, a fim de maximizar benefícios, oportunidades e capacidade competitiva.

1.1 Governança corporativa

Governança é uma palavra que traz consigo a conotação de sabedoria e responsabilidade sobre o que é apropriado. Pode ser definida como o sistema pelo qual as empresas são dirigidas e controladas, e tem como significado tanto a ação quanto o método de governar, sendo este último o mais utilizado como referência pelas empresas (CADBURY, 1992).

Artero (2007) afirma que, dentre as possíveis definições para governança, estão as de controlar, direcionar e regular, ou seja, a maneira como algo é administrado, gerenciamento e o sistema de regulação. Destaca, ainda, que a definição do termo *corporação* inclui um corpo de pessoas unidas, autorizadas legalmente a agir como um único indivíduo, assim como criadas e regidas por certos direitos e deveres.

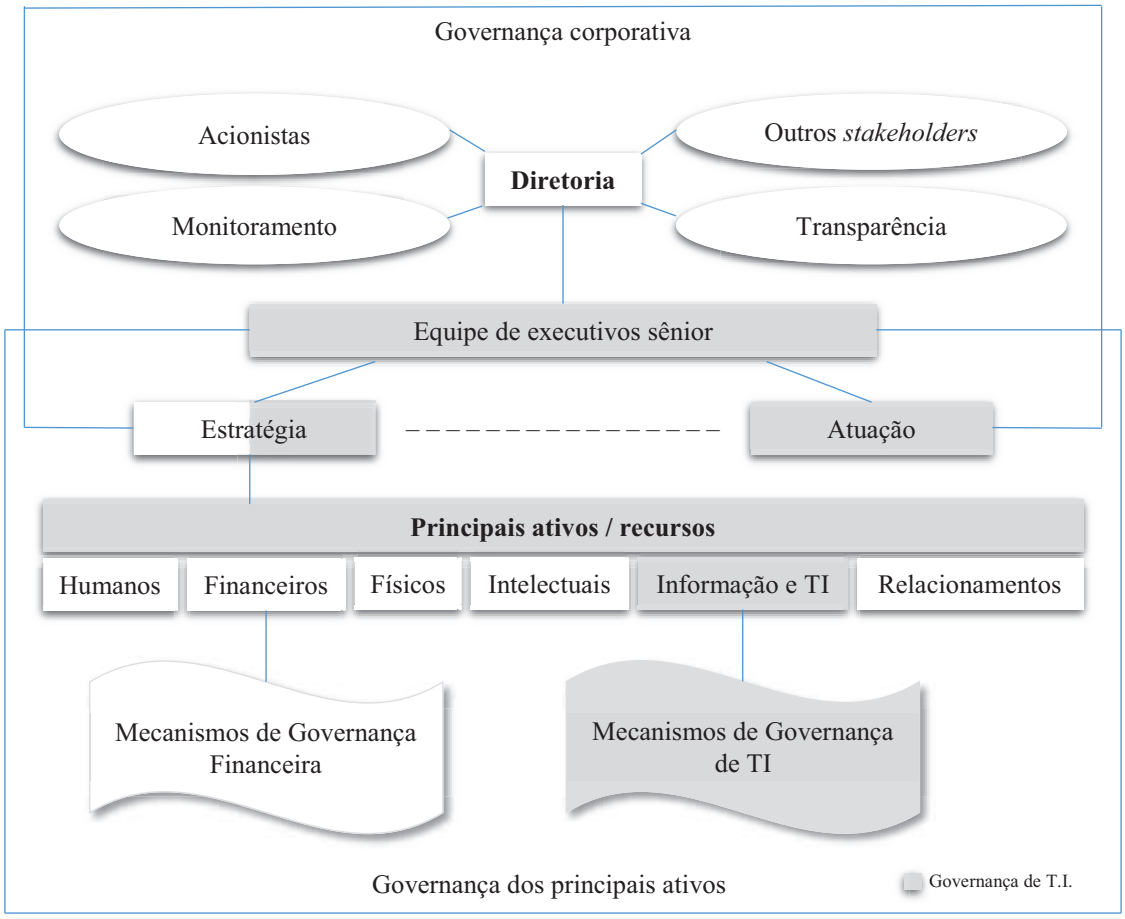
Para o Instituto Brasileiro de Governança Corporativa – IBGC, governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, o que facilita seu acesso a recursos e contribui para a sua longevidade (IBGC, 2014, p.18). Ainda segundo o instituto, os princípios básicos de governança envolvem transparência, equidade, prestação de contas e responsabilidade pela disponibilização de informações relevantes, tratamento justo de todas as partes interessadas, atuação dos

associados, conselheiros, executivos, conselhos fiscais e auditores, além de abranger a sustentabilidade das organizações visando sua longevidade.

A governança corporativa é também um processo metódico de avaliação moldada para os sistemas de decisão e, apesar de não haver um modelo único, é possível identificar elementos em comum que delimitam as boas práticas de governança corporativa (OECD, 2015; BRIS; BRISLEY; CABOLIS, 2008; ALEXANDER, 2000). Pode ser aplicada a diversas áreas da empresa e a direção da organização geralmente possui como foco a eficiência, redução de custos e ampliação da receita e capacidades, os quais estão interligados às informações e ao T.I., sendo vital considerar esta como um ativo (HARDY, 2006).

De forma a integrar os principais ativos ou recursos de governança corporativa e governança de T.I., Weill e Ross (2004) propõem o modelo representado pela Figura 3, ilustrando as relações da diretoria e a equipe de executivos sênior como agentes articuladores de estratégias, atuando para executá-las conforme a necessidade da diretoria.

Figura 3 – Governança corporativa e dos principais ativos



Fonte: Weill e Ross (2004, p.5)

O ITGI (2003) destaca que são as decisões das partes interessadas que impulsionam o empreendimento, de modo que a definição da estratégia, o desempenho, os recursos e a gestão de riscos são núcleos de responsabilidade da governança corporativa. Engloba, assim, as relações entre a administração da entidade e seu corpo diretivo, seus proprietários e demais partes interessadas, fornecendo a estrutura pela qual os objetivos globais da entidade são definidos, além de determinar o método para se atingir esses objetivos e a maneira como o desempenho é mensurado. Promovendo essas práticas, os recursos são utilizados de forma responsável em favor de uma gerência adequada dos riscos.

Portanto, a governança corporativa é o sistema pelo qual as empresas são dirigidas e controladas ao envolver os relacionamentos entre agentes e princípios – como transparência, equidade, prestação de contas, responsabilidade e eficiência –, integrando a estrutura organizacional.

A organização geral do IFSP compreende Órgãos Superiores, Órgãos Colegiados, Órgãos Descentralizados e Órgãos Executivos. Este último compreende, além de outros, a Reitoria, os Órgãos de Apoio e as Pró-Reitorias de Ensino, de Extensão, de Pesquisa, Inovação e Pós-graduação, de Administração e a de Desenvolvimento Institucional, que é responsável pela governança de tecnologia da informação da instituição. (BRASIL, 2015b). Essas diversas áreas, assim como a de T.I., dão suporte e auxiliam no alcance dos objetivos da organização como um todo.

1.2 Governança de tecnologia da informação

A informação é vista cada vez mais como um ativo nas organizações, sejam elas públicas ou privadas. Agem como uma força motriz que provê soluções complexas e, consequentemente, tornam sua governança um fator crítico de sucesso (HARDY, 2006).

Em sua forma ampla, a tecnologia da informação inclui os sistemas de informação, o uso de *hardware* e *software*, telecomunicações, automação e recursos multimídia, utilizados pelas organizações para fornecer dados. A governança de T.I. auxilia, portanto, no alcance dos objetivos e metas de negócio, buscando maior eficácia organizacional e vantagem competitiva (LUFTMAN, 2003; LAURINDO *et al.*, 2001).

Como consequência, as organizações e seus executivos se esforçam para manter informações de alta qualidade, que irão apoiar decisões corporativas. Agrega-se, dessa forma,

valor ao negócio a partir dos investimentos em T.I., atingindo objetivos estratégicos por meio da eficiência (ISACA, 2012).

Visando aprimorar o foco nesse sentido, integrantes do *Joint Technical Committee* desenvolveram um guia de governança para gerenciamento de processos e decisões relativas à informação e serviços de comunicação utilizados pelas organizações, de modo que esses processos pudessem ser controlados por especialistas de T.I. (ISO/IEC 38500, 2015).

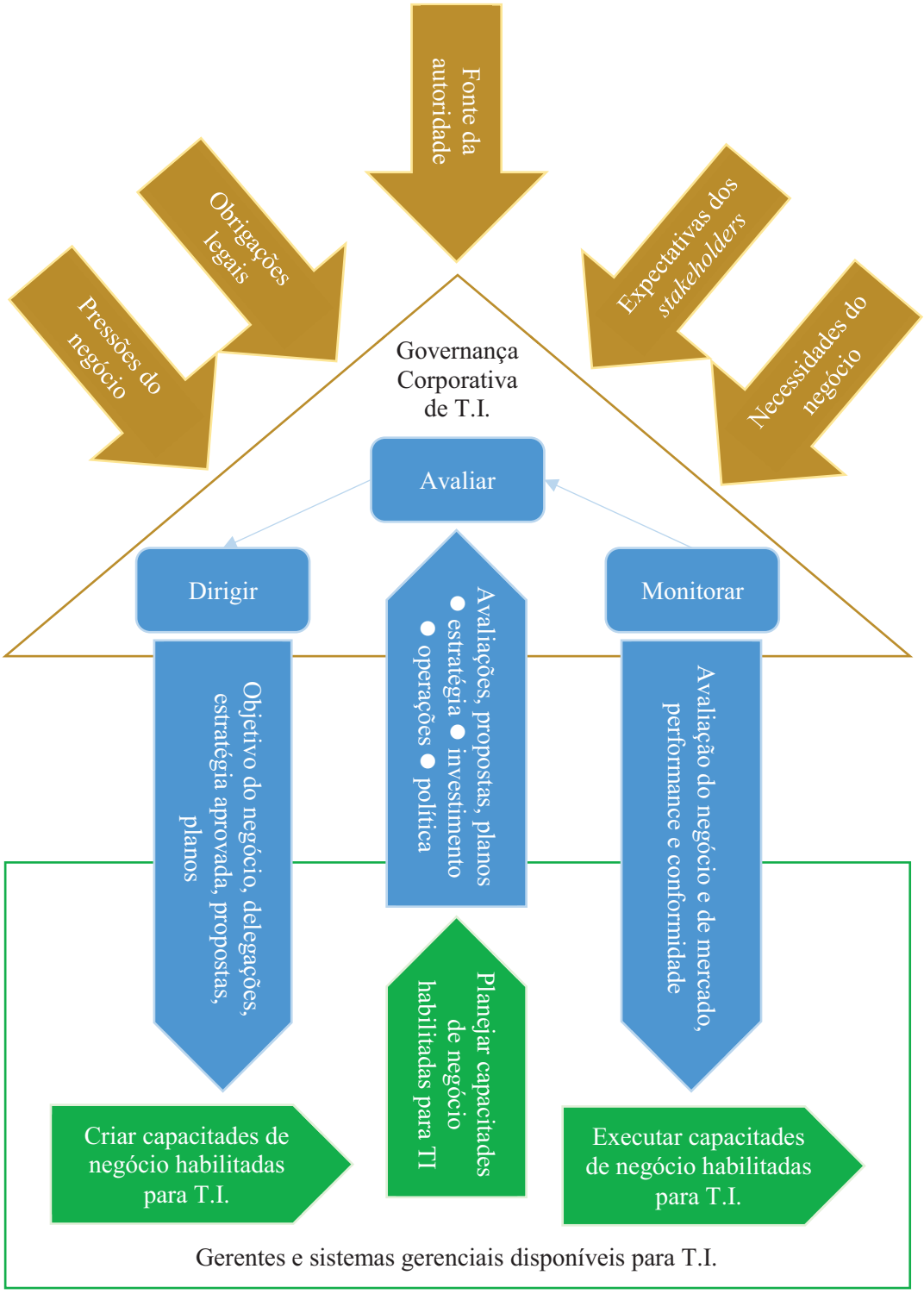
Baseando-se na norma supracitada, a Associação Brasileira de Normas Técnicas (ABNT) elaborou a NBR ISO/IEC 38500. O objetivo do documento é fornecer uma estrutura de princípios que possam ser utilizados pelos dirigentes na avaliação, tomada de decisão, gerenciamento e monitoramento do uso da T.I. em suas organizações.

Os princípios elencados pela norma são:

- Responsabilidade: os indivíduos e grupos da organização compreendem suas responsabilidades e atuam respeitando a demanda de T.I.
- Estratégia: a estratégia de negócio considera as capacidades atuais e futuras de T.I.
- Aquisição: as aquisições de T.I. possuem razões válidas embasadas em análises transparentes, contínuas e apropriadas.
- Desempenho: a T.I. se adequa e apoia a organização, fornecendo serviços baseados em níveis e com qualidade.
- Conformidade: a T.I. cumpre com toda a legislação e regulamentos obrigatórios, possuindo políticas e práticas claramente definidas, implementadas e fiscalizadas.
- Comportamento humano: as políticas, práticas e decisões de T.I. apresentam respeito pelo comportamento humano, incluindo as necessidades atuais e futuras das pessoas.

Juiz e Toomey (2015) destacam, em seus estudos, que agregar valor envolve planejamento, liderança, controle, corroborando com a abordagem desses princípios de modo a orientar a governança de T.I. e apoiar líderes no planejamento, construção e execução das capacidades de T.I. Baseando-se na norma ISO/IEC 38500, apresentam um modelo conceitual de governança de T.I., que ilustra (conforme a Figura 4) as atividades de governança, gerenciamento e objetivo do negócio para a utilização efetiva de T.I., pela perspectiva dos diretores.

Figura 4 – Modelo para a governança de T.I. baseado na norma ISO/IEC 38500



Fonte: Modificado por Juiz e Toomey (2015, p.61)

A T.I. se tornou, portanto, uma espécie de habilitador estratégico de negócio, sendo interessante que organizações ampliem ainda mais sua abrangência, a fim de agilizar o alinhamento dos objetivos do negócio e aprimorar produtos e serviços (LUNARDI *et al.* 2014).

Segundo Raghupathi (2007), a governança de T.I. é refletida na liderança, nas estruturas organizacionais e nos processos, enquanto que Lunardi, Becker e Maçada (2012) apontam para o fato de que algumas empresas podem melhorar seu desempenho por meio da governança de T.I. Seus estudos permitiram concluir que o desempenho organizacional de um grupo de empresas que havia adotado mecanismos formais de governança de T.I., quando comparado ao grupo que não os adotava, melhorou significativamente. Essencialmente, a adesão de empresas a esses mecanismos está relacionada ao interesse em aumentar sua eficiência, reduzir custos e aprimorar a utilização da infraestrutura de T.I..

Em diversos países, mais de 1/3 da economia consiste em organizações governamentais, incluindo educação, saúde e serviços que, de forma similar às organizações com fins lucrativos, utilizam serviços e infraestrutura de T.I. adquiridos por meio de seus recursos. Porém, o desempenho da governança nessas organizações é geralmente baixo, e uma governança de T.I. efetiva deve abordar os seguintes questionamentos: quais decisões devem ser tomadas? Quem deveria tomar estas decisões? Como tomar e monitorar essas decisões? (WEILL, 2004).

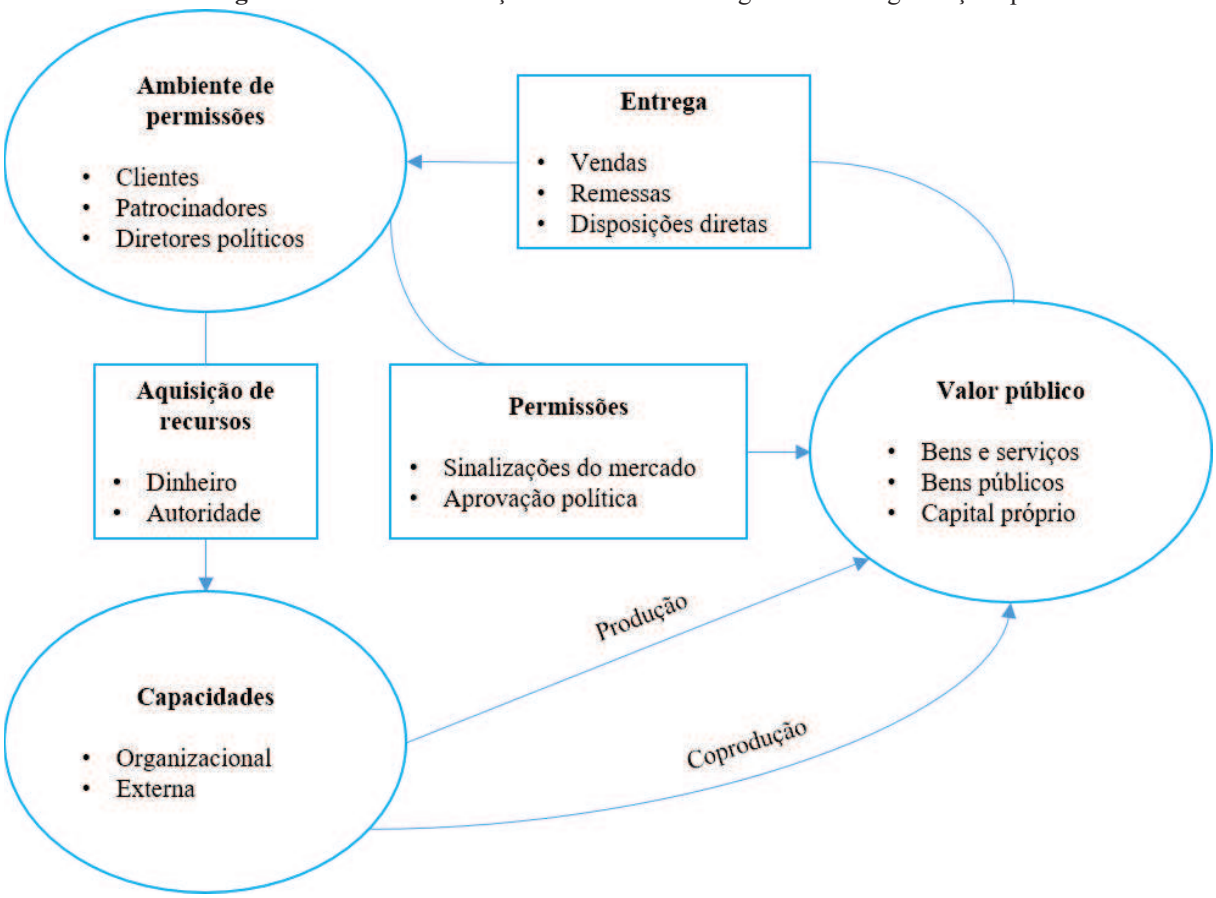
Weill e Woodham (2002) reiteram que a governança de T.I. não pode ser considerada de forma isolada, pois se relaciona com a governança de outros ativos da empresa que, por sua vez, estão interligados à governança corporativa. Os autores destacam as cinco principais decisões a serem tomadas pela governança de T.I.:

- Princípios de T.I.: demonstrações de alto nível quanto à utilização de T.I. nos negócios.
- Arquitetura de T.I.: organização lógica para os dados, aplicações e infraestruturas, visando integrar os negócios à tecnologia de forma padronizada.
- Infraestrutura de T.I.: serviços de T.I. centralizados e coordenados como alicerces das capacidades de T.I. da organização.
- Aplicações de T.I.: especificação das necessidades do negócio para a aquisição de aplicações de T.I. ou implementação de aplicações de T.I. internas.
- Priorização de investimentos em T.I.: quando e onde investir em T.I., incluindo aprovações de projetos e justificativas técnicas.

Diante dessas decisões, verifica-se que criar valor por parte da T.I. é bastante complexo. O próprio conceito de valor, no ambiente público, é extremamente amplo e, segundo Weill e Ross (2004), as complexidades a serem mensuradas podem abordar

performance, transparência, investimento em infraestrutura, liberdade de atuação, redução de custos e outros. As habilidades, o conceito de valor e o ambiente no qual atuam essas organizações criam desafios para a governança de T.I. Buscando alinhar tais fatores, os autores adaptaram um modelo de criação de valor (ilustrado pela Figura 5) voltado a gerentes de organizações públicas.

Figura 5 – Modelo de criação de valor voltado a gerentes de organizações públicas



Fonte: Weill e Ross (2004, p.191)

Thompson *et al.* (2013) salienta ainda que é papel dos gestores alinhar os investimentos de T.I. à estratégia da organização, buscando minimizar custos de tecnologia. A partir daí, assegura-se que a infraestrutura de T.I. possa acomodar e se adequar à utilização crescente de novas aplicações.

Para que a Governança de T.I. esteja alinhada ao negócio da organização, ela deve ser vista como uma ferramenta estratégica que pode dar suporte aos interesses dos *stakeholders* e, por meio da atuação dos gestores, pode ter o mesmo nível de atenção despendido aos demais ativos da organização.

A governança de T.I. do IFSP é vinculada à Pró-Reitoria de Desenvolvimento Institucional, responsável por planejar, definir, acompanhar e avaliar o desenvolvimento das políticas definidas pela reitoria. Levantando e analisando os resultados obtidos, visa o aprimoramento do processo educacional e administrativo, em consonância com as diretrizes definidas pelo Ministério da Educação e disposições do Conselho Superior (BRASIL, 2015b). Sua estrutura conta, além de outras, com a Assessoria de Tecnologia da Informação, Diretoria de Infraestrutura e Redes, Diretoria de Sistemas de Informação e Diretoria Adjunta de Suporte à Tecnologia da Informação (BRASIL, 2015b).

1.3 Gestão de riscos

A administração do risco nos guia por uma ampla gama de tomada de decisões, tornando necessária a atenção às possíveis falhas uma vez que a informação e a complexa tecnologia estão envolvidas nesse processo (BERNSTEIN, 1997). Ainda segundo este autor, grande parte do ato de correr riscos está baseado 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.

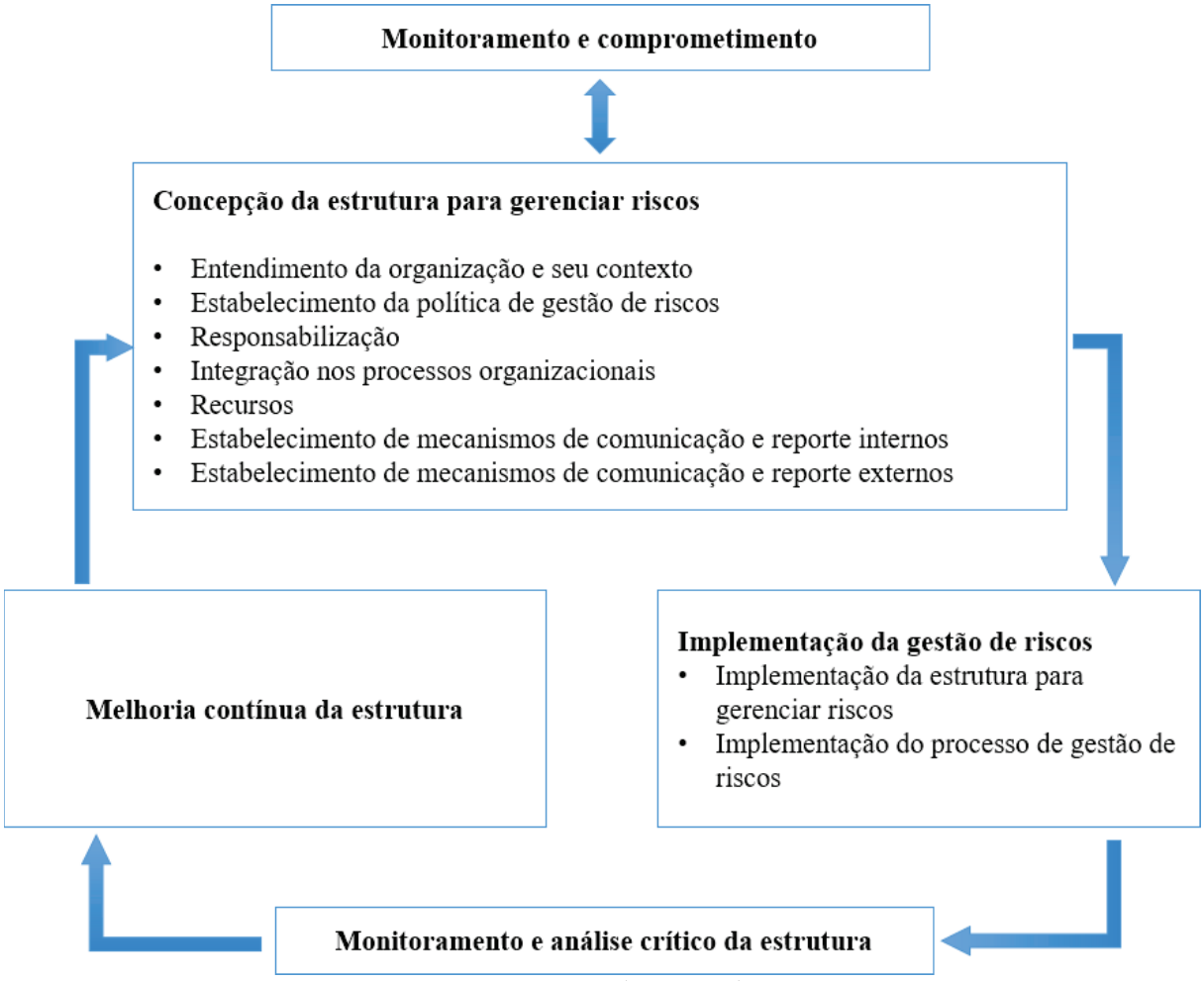
As organizações enfrentam influências de fatores incertos que afetam seus objetivos. De modo a reduzir incertezas, é necessário monitorar e identificar o risco, avaliando se este deve ser modificado ou tratado, uma vez que sua compreensão nos permite tomar decisões de modo racional (ISO 31000, 2009).

Atualmente, os padrões de governança de risco tendem a ser de alto nível, porém existe margem para sua aplicação em diferentes empresas e situações (AKABANE, 2012). Segundo Bromiley *et al*. (2015), as potenciais particularidades e desafios na avaliação do risco oferecem também oportunidades para que as organizações observem problemas em seus processos internos.

A norma ABNT NBR ISO 31000:2009 fornece princípios e diretrizes para a gestão de riscos e pode ser aplicada tanto no setor público ou privado, assim como para avaliar qualquer tipo de risco, independentemente de sua natureza. Conforme a norma, o sucesso da gestão de riscos depende da estrutura de gestão (ilustrada pela Figura 6), que fornece fundamentos e arranjos capazes de incorporar esses processos a toda a organização. Dessa maneira, o gerenciamento de risco é satisfatoriamente auxiliado por meio de sua aplicação em diferentes

níveis e contextos organizacionais, assegurando que o risco seja adequadamente identificado e reportado, o que possibilita utilizá-lo como base na tomada de decisões.

Figura 6 – Relacionamento entre os componentes da estrutura de gerenciamento de riscos



Fonte: ABNT (2009a, p.9)

Segundo a OECD (2014), as instituições públicas podem adotar práticas de governança similares às adotadas por empresas privadas. Para tanto, é crucial haver o controle de risco, tanto pela ação direta dos gestores como por delegações dos diretores, que podem se utilizar de qualquer oportunidade para formular diretivas estratégicas e de liderança. O objetivo da governança é criar valor por meio da realização de benefícios e otimização dos riscos e recursos. Portanto, uma governança de T.I. eficiente gerencia e avalia constantemente as atividades e os riscos relativos à T.I., de modo a mantê-los em um nível aceitável (ISACA, 2012; ITGI, 2007).

Hardy (2006) afirma que uma pequena brecha, roubo, erro, violação de sistema ou ataque de vírus na T.I. podem resultar em sérios danos ao orçamento e reputação da

organização. Por consequência, os gerentes, *stakeholders*, funcionários e clientes se preocupam com a segurança das informações. Os diretores e os conselhos de administração devem, por isso, buscar meios de assegurar a proteção dos ativos de informação organizacional.

A norma ABNT NBR ISO/IEC 27005:2011 fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação (GRSI). Pode ser aplicada em organizações públicas ou privadas que pretendam gerir riscos relacionados à segurança da informação organizacional. Segundo a referida norma, o processo de GRSI pode ser utilizado de forma iterativa na avaliação ou para atividades de tratamento de risco. Seu enfoque iterativo torna possível o detalhamento da avaliação a cada repetição, minimizando o tempo e esforço necessários na identificação de controles, além de assegurar que riscos de alto impacto e probabilidade sejam adequadamente avaliados.

A gestão de risco pode ser vista, portanto, como uma atividade holística que envolve todos os aspectos da organização. O processo de gestão busca fornecer, de forma sólida, a base para que seja possível determinar o nível de aceitação dos riscos, quais oportunidades estes oferecem e como obter informações necessárias para seu devido tratamento.

Em seu processo de gestão de risco, o IFSP trata da política de segurança da informação, trabalhando diversos tipos de informações críticas. Estas são permanecem diretamente relacionadas ao negócio, como informações acadêmicas dos alunos ou administrativas, que influenciam na continuidade do negócio (BRASIL, 2016a).

1.4 Segurança da informação

A prevenção da perda, dano, destruição ou acesso não autorizado à informação processada por organizações é um processo contínuo e, a segurança da informação tem chamado cada vez mais a atenção. Isso porque a constante evolução dos riscos internos e externos pode resultar em violações e perdas para a organização como um todo. Governos e organizações se sensibilizam e investem gradativamente na segurança de seus ativos de informação e sua classificação por meio de treinamentos e conscientizações, auxiliando não somente a tomada de decisões, mas também a melhoria e continuidade de suas operações (DA VEIGA; MARTINS, 2015; JOURDAN *et al*., 2010; NIST, 2010; PURDY, 2010).

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

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. Ademais, pode comprometer a confiabilidade, integridade, autenticidade e disponibilidade de informações que estão sendo processadas, armazenadas ou transmitidas por esses sistemas (NIST, 2010).

A segurança da informação lida com a proteção dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados, preservando, também, 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).

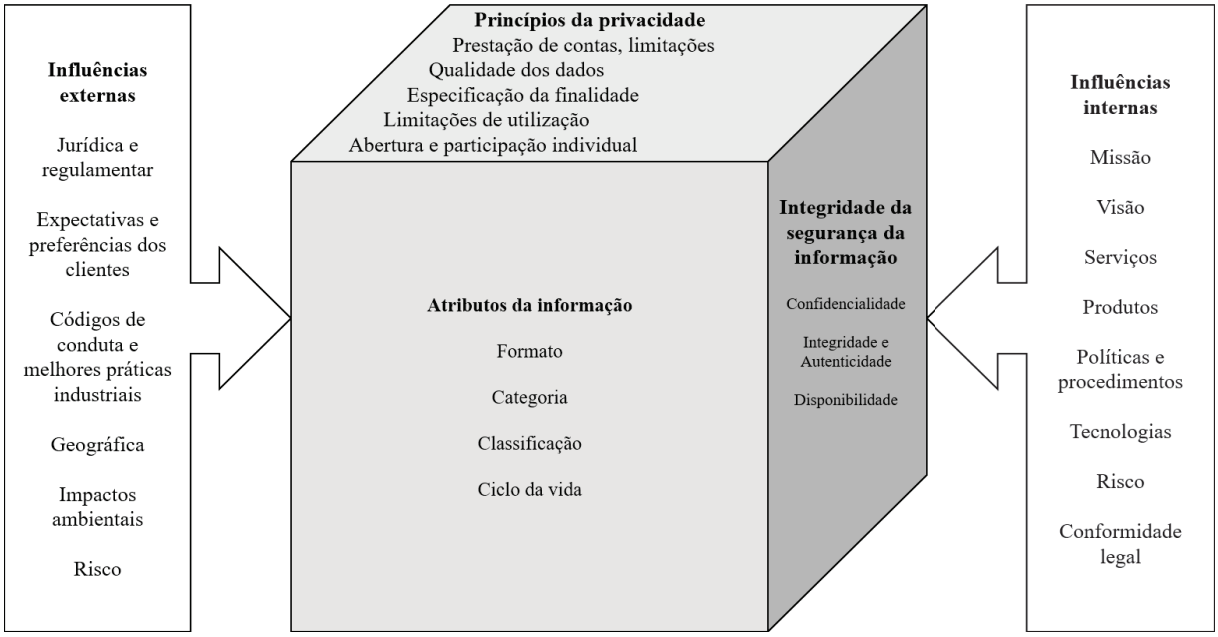
O volume de informações eletrônicas utilizadas pelas empresas é cada vez maior, tornando complexo seu gerenciamento produtivo e adequação da qualidade de acesso, confiabilidade e conformidade. O interesse é atender aos objetivos organizacionais e cuidar de sua exposição, cuja segurança pode ser comprometida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

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 suas necessidades. Em sua recente atualização, a norma ISO/IEC 27001:2013 padroniza definições e estruturas de diferentes padrões ISO, alinhando-se com outros padrões já existentes. A norma também proporciona 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. Nela, adota-se o modelo Planejar-Executar-Monitorar-Agir – do inglês, *Plan-Do-Check-Act (PDCA)* –, considerando requisitos de segurança da informação e ações necessárias para atender às 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. Esse conjunto de atributos que representa uma visão abrangente da perspectiva de segurança e privacidade da informação é apresentado pela Figura 7 (ISO/IEC 27001, 2013; DA VEIGA; ELOFF, 2007).

Figura 7 – Atributos da informação pela perspectiva da privacidade e segurança da informação



Fonte: Da Veiga e Martins (2015, p. 6)

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, se há conscientização quanto à aplicação destes princípios e demais contextos. Além disso, um bom planejamento e uma boa implementação de uma cultura de segurança da informação requer não somente cooperação de toda a organização, mas também por parte dos gestores (DA VEIGA; MARTINS, 2015; MONTESDIOCA; MAÇADA, 2015).

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 27002:2013, reconhecida como uma norma das melhores práticas de segurança da informação, define uma série de controles necessários à maioria das situações que envolvem T.I. (DA VEIGA; ELOFF, 2007).

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 perspectiva destaca cinco princípios fundamentais (listados na Tabela 1), que são utilizados para compreender o ambiente de risco em que as organizações operam. Os fatores destacados pelo autor são motivados pelo interesse de avaliar e implementar controles para mitigar 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. **Treinamento e conscientização da cultura de segurança**: 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 e, o primeiro deles diz respeito à organização de segurança e à infraestrutura, com funções e responsabilidades definidas, bem como a apoio gerencial. O segundo princípio é referente às políticas de segurança, normas e procedimentos de gestão, destacando o 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. 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 estimular o treinamento e 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.

1.5 Segurança da informação no setor público brasileiro

A segurança da informação é agenda estratégica no setor público brasileiro, 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 isso, recentes estudos, como o de Araújo (2012), apresentam a essência do tema e como o mesmo é ainda pouco explorado neste âmbito.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) mantém estatísticas sobre notificações voluntárias e espontâneas de incidentes ocorridos em redes, que a ele foram reportados. A Figura 1, apresentada na introdução desta pesquisa, ilustra o cenário onde cerca de 600.000 ataques foram registrados no período de janeiro a dezembro de 2015 (BRASIL, 2015a).

Independentemente de ser governamental, privada ou pública, a maioria das instituições está aplicando uma série de contramedidas de segurança, políticas, procedimentos e diretrizes como medidas de proteção (JOURDAN *et al.*, 2010). Tal cenário é justificado pelo fato de que incidentes de segurança podem causar consequências adversas para as 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; SULAIMAN; ZOLAIT, 2009; SHEDDEN *et al.*, 2011).

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. Conforme apresenta a Tabela 2, existe uma grande quantidade de dispositivos legais, decretos, leis, instruções normativas e projetos de lei relacionados ao tema.

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)

Não somente os requisitos regulamentares estão aumentando, mas também as responsabilidades de governança em supervisionar progressivamente 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 deve apoiar os objetivos da organização (ISO/IEC 27001, 2013).

Araújo (2012) aponta também, por meio de uma revisão na legislação, a existência de duas instruções normativas e 14 normas complementares, cujo conteúdo dos documentos deve ser observado por todos os órgãos da gestão pública federal, conforme indicado no Quadro 1.

Quadro 1 – Relação de instruções normativas e normas sobre segurança da informação

Instruções Normativas e Normas	Ementa
Instrução Normativa Nº 4 - SLTI/MPOG, de 12 de novembro de 2010	Dispõe sobre o processo de contratação de Soluções de Tecnologia da informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. (Publicada no DOU Nº 218, de 16 nov. 2010- Seção 1).
Instrução Normativa GSI Nº 1, de 13 de junho de 2008	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. (Publicada no DOU Nº 115, de 18 jun. 2008- Seção 1).
Instrução Normativa GSI Nº 2, de 5 de fevereiro de 2013	Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 32, de 18 fev. 2013- Seção 1).

Instrução Normativa GSI Nº 3, de 6 de março de 2013	Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. (Publicada no DOU Nº 50, de 14 Mar 2013- Seção 1).
Norma complementar nº 02/IN01/DSIC/GSIPR	Metodologia de Gestão de Segurança da Informação e Comunicações. (Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1).
Norma complementar nº 03/IN01/DSIC/GSIPR	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. (Publicada no DOU Nº 125, de 03 jul. 2009 - Seção 1).
Norma complementar nº 05/IN01/DSIC/GSIPR, e seu anexo	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 ago. 2009 - Seção 1).
Norma complementar nº 06/IN01/DSIC/GSIPR	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 223, de 23 nov. 2009 - Seção 1).
Norma complementar nº 08/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 ago. 2010 - Seção 1).
Norma complementar nº 10/IN01/DSIC/GSIP	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 fev. 2012 - Seção 1).
Norma complementar nº 11/IN01/DSIC/GSIPR	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. (Publicada no DOU Nº 30, de 10 fev. 2012 - Seção 1).
Norma complementar nº 12/IN01/DSIC/GSIPR	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 fev. 2012 - Seção 1).

Norma complementar nº 13/IN01/DSIC/GSIPR	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). (Publicada no DOU Nº 30, de 10 fev. 2012 - Seção 1).
Norma complementar nº 14/IN01/DSIC/GSIPR	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 30, de 10 fev. 2012 - Seção 1).
Norma complementar nº 15/IN01/DSIC/GSIPR	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 119, de 21 jun. 2012 - Seção 1).
Norma complementar nº 16/IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 224, de 21 nov. 2012 - Seção 1).
Norma complementar nº 17/IN01/DSIC/GSIPR	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 abr. 2013 - Seção 1).
Norma complementar nº 18/IN01/DSIC/GSIPR	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). (Publicada no DOU Nº 68, de 10 abril 2013 - Seção 1).
Norma complementar nº 19/IN01/DSIC/GSIPR	Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. (Publicada no DOU Nº 134, de 16 jul. 2014 - Seção 1).
Norma complementar nº 21/IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1).

Fonte: Adaptado de Araújo (2012)

Além da obrigatoriedade em observar os dispositivos supracitados, as organizações públicas e arquivos públicos são também fortemente regulados e fiscalizados por órgãos de 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).

No IFSP, a política de segurança da informação se caracteriza pela tentativa de manter a confidencialidade, a integridade e a disponibilidade das informações, independentemente de onde ela esteja, residente em memória de máquinas e dispositivos, armazenada em disco, em trânsito ou impressas em documentos. Além disso, salvaguarda a exatidão e completeza dessas informações por meio dos métodos de processamento, garantindo que a comunidade, sempre que necessário e de acordo com a permissão atribuída a cada um, tenha acesso a elas e aos ativos correspondentes.

2 PROCEDIMENTOS METODOLÓGICOS

A pesquisa realizada neste trabalho pode ser classificada como mista quanto à abordagem – quantitativa e qualitativa, e, segundo o objetivo geral, descritiva e exploratória, baseada em um processo lógico de investigação indutivo que explora, descreve e, em seguida, gera perspectivas teóricas (SAMPIERI; COLLADO; LUCIO, 2006).

As etapas desenvolvidas neste estudo englobam revisar a literatura relacionada à governança corporativa, governança de tecnologia da informação, gestão de risco e segurança da informação no setor público brasileiro, no sentido de estabelecer o objeto de pesquisa, Além disso, analisar os aspectos da segurança da informação dentro da gestão de risco dentro na governança de T.I., levantar dados da instituição por meio de protocolo do estudo de caso; tabular e analisar os dados coletados, identificando a percepção da aplicação de segurança da informação na instituição de ensino público federal para examiná-la.

Os fatores envolvidos englobam princípios como organização de segurança e infraestrutura, políticas de segurança, normas e procedimentos, programa de segurança, treinamento e conscientização da cultura de segurança e adequação da sua aplicação na respectiva entidade.

Dessa forma, consiste em um estudo de caso único, que tem como objetivo analisar os aspectos da segurança da informação dentro da gestão de risco dentro na governança de T.I. de uma instituição de ensino público federal.

2.1 Caracterização

A aplicação metodológica de um trabalho pode ser justificada pela necessidade de embasamento científico adequado e pela busca da melhor abordagem para endereçar as questões da pesquisa. Ademais, um estudo de caso único permite um maior aprofundamento na investigação e é frequentemente utilizado em pesquisa longitudinal (MIGUEL, 2007).

Conforme salienta Yin (2001), o estudo de caso é uma inquirição empírica que investiga fenômenos contemporâneos inseridos em algum contexto da vida real, permitindo a

utilização de fontes de evidências, como a observação direta e entrevistas, utilizando protocolos.

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

As seguintes seções compõem o protocolo do estudo de caso:

- Visão geral do projeto do estudo de caso com a descrição da pesquisa, etc.
- Procedimentos de campo, apresentação das credenciais do pesquisador, locais de estudo, fontes de informação, etc.
- Questões do estudo de caso com questões específicas para a coleta de dados.

Os procedimentos de campo, as questões do estudo de caso, a carta de autorização e o roteiro, utilizados na condução deste estudo, encontram-se nos APÊNDICES A – CARTA DE AUTORIZAÇÃO, APÊNDICE B – ROTEIRO PARA QUESTIONÁRIO ESTRUTURADO FECHADO e APÊNDICE C – ROTEIRO PARA QUESTIONÁRIO ESTRUTURADO ABERTO. Os instrumentos de coleta utilizados foram questionários digitais estruturados na plataforma *Google Forms,* disponível em: <https://docs.google.com/forms/>. A visão geral do protocolo de estudo de caso encontra-se descrita nas etapas a seguir.

2.2 Protocolo

Segundo Yin (2001), 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 descrito na introdução deste trabalho demostram a existência de poucas pesquisas referentes à gestão de riscos de segurança da informação aplicadas no contexto de instituições federais de educação. Além disso, a escolha se deu

devido à facilidade de contato do autor com os gestores responsáveis pela governança de T.I., assim como limitações de tempo, recursos financeiros, materiais e pessoas (MATTAR, 1996).

- Amostragem: o processo de amostragem adotado nesta pesquisa pode ser classificado como não probabilístico e por conveniência (MALHOTRA, 2001; SCHIFFMAN; KANUK, 2000; FOWLER, 1991). 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 desta pesquisa se restringiu à reitoria do IFSP, não se ampliando aos demais *campi*. Consiste de entrevistados que, além de atuarem como gestores de T.I. capacitados, possuem contato frequente com o tema e se disponibilizaram voluntariamente a participar da pesquisa (FREITAS *et al.*, 2000; MATTAR, 1996; AAKER; KUMAR; DAY, 1995; KISH, 1965).
- 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 questionários estruturados, instrumento de coleta de dados constituído por uma série ordenada de perguntas e, em seguida, questionários abertos (LAKATOS, 2003).

2) Coleta e análise de dados

- Aplicação dos questionários: com base nas questões apontadas no protocolo para o estudo de caso e no critério de escolha dos entrevistados, foi aplicado primeiramente um questionário estruturado fechado com tratamento estatístico das respostas para o levantamento de informações quantitativas. Em seguida, foi aplicado um questionário aberto de profundidade para o levantamento de informações qualitativas e maior análise dos dados obtidos. Os questionamentos foram aplicados a gestores responsáveis por diferentes áreas de T.I., durante o primeiro semestre de 2016.
- Elaboração de relatório preliminar: a partir das informações obtidas nos questionários aplicados, um relatório preliminar do caso foi elaborado para a análise detalhada.

3) Análise das informações e conclusão

- Análise das informações: a partir do relatório preliminar elaborado, foi realizada uma análise detalhada das respostas obtidas.
- Elaboração das conclusões: registro das observações decorrentes da análise dos resultados.

2.3 A instituição

A instituição na qual foi conduzido este estudo é parte integrante da rede de Institutos Federais de Educação, Ciência e Tecnologia, vinculados diretamente ao Ministério da Educação. Esses órgãos 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 na realização de pesquisa aplicada e promoção do desenvolvimento tecnológico de novos processos, produtos e serviços. Especialmente de abrangência local e regional, oferecem mecanismos para a educação continuada, com estreita articulação com os setores produtivos e a sociedade (BRASIL, 2015b).

A estrutura *multicampi* e a clara definição do território de abrangência das ações dos Institutos Federais afirmam, na missão dessas instituições, o compromisso de intervenção em suas respectivas regiões, identificando problemas e criando soluções técnicas e tecnológicas para o desenvolvimento sustentável com inclusão social (BRASIL, 2016).

Fundada em 1909 como Escola de Aprendizes Artífices, durante sua história, recebeu, também, os nomes de Escola Técnica Federal de São Paulo e Centro Federal de Educação Tecnológica de São Paulo. Em dezembro de 2008, com sua transformação em Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), passou a ser uma autarquia federal de ensino e a ter relevância de universidade, destacando-se pela autonomia (BRASIL, 2015b).

O 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 à distância distribuídos pelo estado de São Paulo. Sua

organização geral compreende Órgãos Superiores, Órgãos Colegiados, Órgãos Descentralizados e Órgãos Executivos. Este último compreende, além de outras áreas, a Reitoria, os Órgãos de Apoio e as Pró-Reitorias de Ensino, de Extensão, de Pesquisa, Inovação e Pós-graduação, de Administração e a de Desenvolvimento Institucional (BRASIL, 2015b).

As Pró-Reitorias, dirigidas por Pró-Reitores nomeados pelo Reitor, são órgãos executivos que planejam, definem, acompanham e avaliam as atividades e as políticas relacionadas às seguintes dimensões:

À Pró-Reitoria de Ensino compete planejar, definir, acompanhar e avaliar o desenvolvimento das políticas e atividades acadêmicas, buscando o seu constante aprimoramento, em consonância com as diretrizes definidas pelo Ministério da Educação e com as disposições do Conselho Superior (BRASIL, 2015b).

À Pró-Reitoria de Extensão compete planejar, definir, acompanhar e avaliar as políticas e as atividades de extensão em suas relações com a sociedade e com as empresas, buscando articulá-las ao ensino e à pesquisa, em consonância com as diretrizes definidas pelo Ministério da Educação e com as disposições do Conselho Superior (BRASIL, 2015b).

À Pró-Reitoria de Pesquisa, Inovação e Pós-graduação compete planejar, definir, acompanhar e avaliar as políticas e o desenvolvimento das atividades a ela relacionadas, buscando seu fortalecimento em todos os níveis de ensino do IFSP, em consonância com as diretrizes definidas pelo Ministério da Educação e com as disposições do Conselho Superior (BRASIL, 2015b).

À Pró-Reitoria de Administração compete planejar, definir, acompanhar e avaliar as políticas e atividades de execução orçamentária, financeira e patrimonial, buscando o seu constante aprimoramento, em consonância com as diretrizes definidas pelo Ministério da Educação e com as disposições do Conselho Superior (BRASIL, 2015b).

Por fim, à Pró-Reitoria de Desenvolvimento Institucional compete planejar, definir, acompanhar e avaliar tanto o desenvolvimento das atividades de gestão de pessoal, quanto o desenvolvimento das políticas definidas pela Reitoria, levantando e analisando os resultados obtidos e buscando o aprimoramento do processo educacional e administrativo, em consonância com as diretrizes definidas pelo Ministério da Educação e disposições do Conselho Superior (BRASIL, 2015b).

Contemplando a área de Tecnologia da Informação do IFSP, sua estrutura conta, além de outras, com a Assessoria de Tecnologia da Informação, Diretoria de Infraestrutura e Redes, Diretoria de Sistemas de Informação e Diretoria Adjunta de Suporte à Tecnologia da

Informação. No portal da T.I. é possível, ainda, verificar as atribuições e responsabilidades de cada uma destas diretorias, por meio do endereço eletrônico <http://ti.ifsp.edu.br> (BRASIL, 2015b).

A governança de T.I. do IFSP trata, dentro da gestão de risco, da política de segurança da informação, trabalhando com diversos tipos de informações críticas diretamente relacionadas ao negócio, como informações acadêmicas dos alunos ou informações administrativas que influenciam na continuidade do negócio (BRASIL, 2016a).

Essas informações circulam e são armazenadas em grandes volumes, tanto no ambiente interno como no externo, em mídias físicas ou lógicas, utilizando, assim, um grande número de ativos, essenciais para o negócio da instituição. Dessa maneira, os recursos computacionais de rede, de comunicação, os documentos físicos gerados ou não por recursos computacionais e as informações desses recursos, como qualquer outro ativo da instituição, precisam ser protegidos (BRASIL, 2016b).

A política de segurança da informação da instituição se caracteriza pela tentativa de manter a confidencialidade, a integridade e a disponibilidade das informações, esteja ela residente em memória de máquinas e dispositivos, armazenada em disco, em trânsito ou impressas em documentos. Salvaguarda, assim, a exatidão e a completeza dessas informações por meio dos métodos de processamento, garantindo que a comunidade, sempre que necessário e de acordo com a permissão atribuída a cada um, tenha acesso a elas e aos ativos correspondentes (BRASIL, 2016b).

2.4 Estudo quantitativo

Para verificar o tratamento dado à segurança da informação, por meio da gestão de riscos dentro da governança de T.I. da instituição em estudo, foram analisados aspectos da gestão de risco que envolvem princípios como:

- Organização de segurança e infraestrutura;
- Políticas de segurança, normas e procedimentos;
- Programa de segurança;
- Treinamento e conscientização da cultura de segurança;
- Adequação.

Esses princípios podem ser vistos como dimensões da arquitetura de segurança da informação, abrangendo aspectos da mesma por meio da gestão de riscos dentro da governança de T.I., assim como proteção de informações confidenciais em conformidade com a legislação.

Os autores estudados nesta pesquisa e as áreas de foco da governança de T.I. apresentadas na Introdução (Figura 2) – que tratam do alinhamento estratégico, entrega de valor, gestão de recursos, mensuração de desempenho e, em especial, a gestão de riscos – permitem estabelecer as relações entre os seguintes planos de negócios: a T.I., a execução da proposta por meio do ciclo de entrega, a melhor utilização possível dos investimentos e recursos, a otimização do conhecimento, monitoramento de processos e gerenciamento do ambiente de risco nas atividades da organização, validando estes princípios chave.

Desse modo, em um primeiro momento, foi conduzido um estudo quantitativo. Nele, para definir constructos, os autores estudados no referencial teórico foram relacionados com a arquitetura de segurança da informação proposta por Tudor (2000) e adaptada por Da Veiga (2007,) abrangendo essas cinco dimensões.

1. Organização de segurança e infraestrutura

A própria definição do termo *corporação* inclui um corpo de pessoas unido e autorizado legalmente a agir, de forma organizada, como um único indivíduo, criado e regido por certos direitos e deveres. Por ser um processo metódico de avaliação moldada para os sistemas de decisão, a governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, podendo ser aplicada a diversas áreas da empresa, incluindo a de T.I. Com foco na eficiência e envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle, a governança corporativa exige dos gestores a competência de alinhar os investimentos à estratégia das organizações e assegurar que a infraestrutura seja adequada à crescente utilização de novas aplicações, possibilitando um trabalho eficiente e produtivo, com transparência e responsabilidade gerencial (OECD, 2015; IBGC, 2014; THOMPSON *et al.*, 2013; AKABANE, 2012; BRIS; BRISLEY; CABOLIS, 2008; ARTERO, 2007; HARDY, 2006; VAN GREMBERGEN; DE HAES; GULDENTOPS, 2004; ITGI, 2003; ALEXANDER, 2000).

Em diversos países, mais de 1/3 da economia consiste em organizações governamentais, incluindo educação, saúde e serviços que utilizam a infraestrutura de T.I. Esta, em sua forma ampla, inclui os sistemas de informação, o uso de *hardware* e *software*, telecomunicações, automação e recursos multimídia, utilizados para fornecer dados, informações e conhecimento. A informação e as tecnologias inseridas no ciclo de negócios se difundem como um ativo estratégico, de modo que sua governança envolve decisões no tocante a princípios, arquitetura, infraestrutura, aplicações e priorização de investimentos. (ISACA, 2012; RAMOS; NASCIMENTO, 2010; ARTERO, 2007; NOBRE; WEILL, 2004; LUFTMAN, 2003; WEILL; WOODHAM, 2002; LAURINDO *et al.*, 2001; CADBURY, 1992).

Desse modo, questionamentos podem ser levantados. Por exemplo:

No que tange à segurança da informação, os papéis desempenhados pelas pessoas são definidos?

As responsabilidades das pessoas são definidas?

2. Políticas de segurança, normas e procedimentos

Agregar valor envolve planejamento, sendo este afetado por pressões do negócio e obrigações legais. Não somente os requisitos regulamentares estão aumentando, mas também as responsabilidades de governança em supervisionar cada vez mais a segurança da informação. Nesse sentido, deve-se enfatizar o fato de que a legislação brasileira relacionada à Segurança da Informação e Comunicações (SIC) de caráter federal, estadual e municipal contempla uma grande quantidade de dispositivos legais, decretos, leis, instruções normativas e projetos de lei. Dentre estes, duas instruções normativas e 14 normas complementares devem ser obrigatoriamente observadas por todos os órgãos da gestão pública federal, conforme apresentado na Tabela 2 (Legislação relacionada à segurança da informação) e no Quadro 1 (Relação de instruções normativas e normas sobre segurança da informação). Além da obrigatoriedade em observar os dispositivos supracitados, as organizações públicas e arquivos públicos são também fortemente regulados e fiscalizados por órgãos de controle da Administração Pública, como Ministério do Planejamento, Orçamento e Gestão (MPOG), Controladoria Geral da União (CGU) e Tribunal de Contas da União (TCU) (ISO/IEC 38500, 2015; JUIZ; TOOMEY, 2015; VIEIRA; ALBUQUERQUE JR.; SANTOS, 2014; FRAGA, 2014; ISO/IEC 27001, 2013; ARAÚJO; 2012).

Públicas ou privadas, a maioria das instituições aplica uma série de contramedidas de segurança, políticas, procedimentos e diretrizes como medidas de proteção, tendo em vista que o sucesso da gestão de riscos busca, também, assegurar que o risco seja adequadamente identificado e reportado, podendo, assim, ser utilizado como base na tomada de decisões (JOURDAN *et al.*, 2010; ABNT, 2009a).

O processo de Gestão de Riscos de Segurança da Informação (GRSI) pode ser utilizado de forma iterativa na avaliação ou para atividades de tratamento de risco. Seu enfoque iterativo torna possível o detalhamento da avaliação a cada repetição, minimizando o tempo e o esforço necessários na identificação de controles, assegurando que riscos de alto impacto e probabilidade sejam adequadamente avaliados. Além disso, podem auxiliar na implementação de controles de segurança e contenção de ameaças aos ativos de informação (ABNT, 2011; ELOFF; ELOFF, 2005).

Desse modo, questionamentos podem ser levantados. Por exemplo:

São desenvolvidas políticas, normas ou procedimentos de segurança da informação?

3. Programa de segurança

A administração do risco nos guia por uma ampla gama de tomada de decisões, sendo necessária atenção às possíveis falhas ou erros, o que inclui a informação e a complexa tecnologia envolvida em seu processo (BERNSTEIN, 1997).

Os padrões de governança de risco tendem a ser de alto nível. Criar valor por meio da realização de benefícios e otimização dos riscos e recursos exige que a governança de T.I. seja eficiente, gerencie e avalie constantemente as atividades e os riscos relativos à T.I., de modo a mantê-los em um nível aceitável. Gerenciar o risco em diferentes empresas e situações oferece oportunidades para que as organizações observem problemas em seus processos internos (BROMILEY *et al*., 2015; OECD, 2014, ISACA, 2012; ITGI, 2007).

É crucial que haja o controle de risco, tanto pela ação direta dos gestores e funcionários como por delegações dos diretores, que podem se utilizar de qualquer oportunidade para formular diretivas estratégicas e de liderança. Ao investir na segurança de seus ativos de informação por meio de sua classificação, treinamentos e conscientizações, governos e organizações obtêm melhorias não somente na tomada de decisões. mas também na continuidade de suas operações (DA VEIGA; MARTINS, 2015; JOURDAN *et al.*, 2010; NIST, 2010; PURDY, 2010).

As organizações enfrentam influências de fatores incertos que afetam seus objetivos. Uma pequena brecha, roubo, erro, violação de sistema ou ataque de vírus na T.I. podem resultar em sérios danos ao orçamento e reputação da organização. De modo a reduzir incertezas, é necessário monitorar e identificar o risco para avaliar se este deve ser modificado ou tratado, uma vez que sua compreensão nos permite tomar decisões de modo racional e buscar meios de assegurar a proteção dos ativos de informação organizacional. (ABNT, 2011; ABNT, 2009a; HARDY, 2006).

Deste modo, questionamentos podem ser levantados. Por exemplo:

Um programa de segurança da informação é organizado tendo em conta a gestão de riscos?

4. Treinamento e conscientização da cultura de segurança

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, e se há conscientização quanto à aplicação desses princípios e demais contextos. Além disso, um bom planejamento e implementação de mecanismos formais de governança de T.I., aliados a uma cultura de segurança da informação, requer não somente cooperação de toda a organização, como também por parte dos gestores (DA VEIGA; MARTINS, 2015; MONTESDIOCA; MAÇADA, 2015; LUNARDI; BECKER; MAÇADA, 2012).

Abordagens de melhoria contínua, por meio de um processo de criação, implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação, auxiliam na especificação, realização e administração da segurança, representando uma visão abrangente da perspectiva da mesma e da privacidade da informação. Não obstante, é papel dos gestores alinhar as necessidades específicas com a estratégia da organização também por meio da conscientização, uma vez que as complexidades a serem mensuradas no ambiente público podem abordar performance, transparência, investimento em infraestrutura, liberdade de atuação, redução de custos e outros (THOMPSON *et al.*, 2013; ISO/IEC 27001, 2013; ISO/IEC 27002:2013; DA VEIGA; ELOFF, 2007; WEILL; ROSS, 2004; TUDOR, 2000).

Desse modo, questionamentos podem ser levantados. Por exemplo:

Os usuários são treinados e conscientizados quanto à importância da segurança da informação?

Há reflexo positivo dessa conscientização?

5. Adequação

A prevenção da perda, dano, destruição ou acesso não autorizado à informação processada por organizações é um processo contínuo, uma vez que a constante evolução dos riscos internos e externos pode resultar em violações e perdas para a organização como um todo. Administrar o risco nos guia por uma ampla gama de tomada de decisões, sendo necessária atenção às possíveis falhas ou erros, incluindo a informação e a complexa tecnologia envolvida em seu processo como apoio para alcançar os objetivos e metas de negócio (DA VEIGA; MARTINS, 2015; JUIZ; TOOMEY, 2015; LUFTMAN, 2003; BERNSTEIN, 1997).

O volume de informações eletrônicas utilizadas pelas empresas cresce gradativamente, tornando complexo seu gerenciamento produtivo, eficiência, responsabilidade gerencial e adequação da qualidade de acesso, confiabilidade e conformidade, com vistas a atender os objetivos organizacionais. Há também a preocupação com a exposição da empresa, cuja segurança pode ser comprometida por incidentes que representariam prejuízos financeiros ou para a imagem das organizações (AKABANE, 2012; ISACA, 2012; ALEXANDRIA, 2009; POSTHUMUS; VON SOLMS, 2004).

A segurança da informação é agenda estratégica no setor público brasileiro, existindo uma gama de dispositivos legais, decretos, leis, instruções normativas, projetos de lei e normas que tratam de sua aplicação nos órgãos vinculados ao Governo Federal e cuja observância é obrigatória. Além da obrigatoriedade em observar os dispositivos supracitados, as organizações públicas e arquivos públicos são também fortemente regulados e fiscalizados por órgãos de 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; VIEIRA; FRAGA, 2014; ARAÚJO, 2012).

Deste modo, questionamentos podem ser levantados.) Por exemplo:

Existe um controle interno da segurança da informação por meio de auditorias?

Existe um controle externo da segurança da informação por meio de auditorias?

O Quadro 2 apresenta o constructo da relação entre a arquitetura de segurança da informação e os autores estudados.

Quadro 2 – Constructo da relação entre a arquitetura de segurança da informação e autores

Dimensões		Autores
D1	**Organização de segurança e infraestrutura**	IBGC (2014), Thompson *et al*. (2013), Akabane (2012), ISACA (2012), Nobre, Ramos e Nascimento (2010), Bris, Brisley e Cabolis (2008), Artero (2007), Hardy (2006), OECD (2015), Van Grembergen, De Haes e Guldentops (2004), Weill (2004), Weill e Ross (2004), ITGI (2003), Weill e Woodham (2002), Laurindo *et al.* (2001), Alexander (2000), Tudor (2000), Cadbury (1992)
D2	**Políticas de segurança, normas e procedimentos**	Juiz e Toomey (2015); Vieira e Fraga (2014), Albuquerque Jr. e Santos (2014), ISO/IEC 27001:2013, ISO/IEC 27002:2013, Araújo (2012), ISO/IEC 27005:2011, Jourdan *et al*. (2010), ISO/IEC 38500:2009, ISO 31000:2009, Eloff e Eloff (2005), Tudor (2000), Schein (1985)
D3	**Programa de segurança**	Bromiley *et al*. (2015), OECD (2014), Da Veiga e Martins (2015), ISACA (2012), ISO/IEC 27005:2011, NIST (2010), Purdy (2010), Jourdan *et al*. (2010), ISO 31000:2009, ITGI (2007), Hardy (2006), Eloff e Eloff (2005), Tudor (2000), Bernstein (1997)
D4	**Treinamento e conscientização da cultura de segurança**	Da Veiga e Martins (2015), Montesdioca e Maçada (2015), Thompson *et al*. (2013), ISO/IEC 27001:2013, ISO/IEC 27002:2013, Lunardi, Becker e Maçada (2012), Da Veiga e Eloff (2007), Weill e Ross (2004), Tudor (2000)
D5	**Adequação**	Da Veiga e Martins (2015); Juiz e Toomey (2015), Albuquerque Jr. e Santos (2014), Araújo (2012), Akabane (2012), ISACA (2012), Alexandria (2009), Posthumus e Von Solms (2004), Luftman (2003), Tudor (2000), Bernstein (1997)

Fonte: Resultado da pesquisa

O Quadro 3, por sua vez, apresenta a relação entre os questionamentos levantados e os autores estudados, tendo como base os princípios que permitem a verificação do tratamento

dado à segurança da informação dentro da gestão de riscos na governança de T.I., e auxiliando na compreensão do ambiente de riscos na qual as organizações operam a fim de que estas possam avaliar e implantar controles.

Quadro 3 – Constructo da relação entre os questionamentos fechados e os autores

Dimensões	Questionamentos	Autores
D1 Organização de segurança e infraestrutura Questões: 01 e 02	No que tange à segurança da informação, os papéis desempenhados pelas pessoas são definidos?	IBGC (2014), Thompson *et al*. (2013), ISACA (2012), Nobre, Ramos e Nascimento (2010), Artero (2007), Weill (2004), Weill e Woodham (2002), Laurindo *et al.* (2001), Alexander (2000), Tudor (2000)
	No que tange à segurança da informação, as responsabilidades das pessoas são definidas?	OECD (2015), Akabane (2012), Bris, Brisley e Cabolis (2008), Hardy (2006), Weill e Ross (2004), Van Grembergen, De Haes e Guldentops (2004), ITGI (2003), Tudor (2000), Cadbury (1992)
D2 Políticas de segurança, normas e procedimentos Questões: 03, 04 e 05	São desenvolvidas políticas de segurança da informação?	Juiz e Toomey (2015), Jourdan *et al*. (2010), ISO/IEC 38500:2009, Eloff e Eloff (2005), Tudor (2000), Schein (1985)
	São desenvolvidas normas de segurança da informação?	Vieira e Fraga (2014), ISO/IEC 27002:2013, Araújo (2012), Tudor (2000)
	São desenvolvidos procedimentos de segurança da informação?	Albuquerque Jr. e Santos (2014), ISO/IEC 27001:2013, ISO/IEC 27005:2011, ISO 31000:2009, Tudor (2000)
D3 Programa de segurança Questão: 06	Um programa de segurança da informação é organizado tendo em conta a gestão de riscos?	Bromiley *et al*. (2015), OECD (2014), Da Veiga e Martins (2015), ISACA (2012), ISO/IEC 27005:2011, NIST (2010), Purdy (2010), Jourdan *et al*. (2010), ISO 31000:2009, ITGI (2007), Hardy (2006), Eloff e Eloff (2005), Tudor (2000), Bernstein (1997)
D4 Treinamento e conscientização da cultura de segurança Questão: 07	Os usuários são treinados e conscientizados quanto à importância da segurança da informação?	Da Veiga e Martins (2015), Montesdioca e Maçada (2015), ISO/IEC 27001:2013, ISO/IEC 27002:2013, Da Veiga e Eloff (2007)

Questão: 08	Há reflexo positivo dessa conscientização?	Thompson *et al*. (2013), Lunardi, Becker e Maçada (2012), Weill e Ross (2004), Tudor (2000)
D5 Adequação Questões: 09 e 10	Existe um controle interno da segurança da informação por meio de auditorias?	Da Veiga e Martins (2015); Juiz e Toomey (2015), Albuquerque Jr. e Santos (2014), Akabane (2012), Alexandria (2009), Posthumus e Von Solms (2004), Tudor (2000), Bernstein (1997)
	Existe um controle externo da segurança da informação por meio de auditorias?	Da Veiga e Martins (2015); Araújo (2012), Akabane (2012), ISACA (2012), Luftman (2003), Tudor (2000), Bernstein (1997)

Fonte: Resultado da pesquisa

O instrumento de coleta utilizado nesta etapa foi um questionário estruturado fechado, composto por 10 perguntas – elaboradas conforme a arquitetura de segurança da informação e autores descritos no Quadro 3 –, classificadas em uma escala do tipo *Likert* de 1 ("discordo completamente") a 6 ("concordo completamente") cujo gráfico encontra-se na Figura 8.

As análises quantitativas encontram-se no item 3.2, e os dados foram coletados por meio de um questionário digital, aplicado com auxílio da plataforma *Google Forms*.

2.5 Estudo qualitativo

Após a coleta e análise dos resultados do estudo quantitativo, verificou-se, especialmente no que se refere às dimensões de programa de segurança (D3), treinamento e conscientização da cultura de segurança (D4) e adequação (D5), que os dados obtidos apresentaram campo para melhor análise e compreensão e, consequentemente, para a necessidade da condução de uma nova pesquisa de profundidade.

Desse modo, em um segundo momento foi conduzido um estudo qualitativo seguindo de um roteiro e mediante prévia autorização da instituição em estudo.

O instrumento de coleta utilizado nesta etapa foi um questionário estruturado aberto, e assim como apresentado no estudo quantitativo, buscou verificar o tratamento dado à

segurança da informação dentro da gestão de riscos na governança de T.I. de uma instituição de ensino público federal.

As perguntas de número 6 a 10 aplicadas na primeira etapa da pesquisa foram aprofundadas em 14 (quatorze) questionamentos abertos, também elaborados conforme os constructos apresentados no estudo quantitativo. Foram abordadas, também, as áreas de foco na governança de T.I. (Figura 2 – ITGI, 2007, p.8) e as dimensões de programa de segurança (D3), treinamento e conscientização da cultura de segurança (D4) e adequação (D5). O Quadro 4 apresenta a relação entre essas dimensões e os questionamentos abertos.

A análise qualitativa dos dados coletados foi feita por meio da análise de conteúdo. Segundo Bardin (2011), essa abordagem é um conjunto de técnicas de análise das comunicações que, em sua função heurística, enriquece a tentativa exploratória, aumentando a propensão para a descoberta.

Quadro 4 – Constructo da relação entre as dimensões de segurança da informação e questionamentos abertos

Dimensões	Referência	Questionamentos
D3 **Programa de segurança** **Questões:** **11 a 13**	Um programa de segurança da informação é organizado tendo em conta a gestão de riscos?	Há algum método utilizado para classificar as informações? Há alguém responsável dentro do programa de segurança da informação para realizar avaliações de risco periódicas? Quando ocorrem incidências e violações de segurança, estes são monitorados e investigados visando melhorias?
D4 **Treinamento e conscientização da cultura de segurança** **Questões:** **14 a 16**	Os usuários são treinados e conscientizados quanto à importância da segurança da informação?	O treinamento dos funcionários quando a segurança da informação tem dados os resultados esperados? Os funcionários têm consciência de sua responsabilidade em proteger os ativos de informação da empresa? Os funcionários reconhecem potenciais violações de segurança e sabem quem contatar nestes casos?

D4 **Treinamento e conscientização da cultura de segurança** **Questões:** **17 a 19**	Há reflexo positivo dessa conscientização?	Os administradores de sistemas participam de treinamentos técnicos de segurança relativos aos sistemas operacionais, redes, bancos de dados ou aplicativos que eles gerenciam? Existem agentes de segurança responsáveis por integrar uma arquitetura de segurança da informação e de seus componentes a um programa de conscientização e treinamento? Os gerentes de departamento asseguram-se de que os funcionários que atuam sob sua responsabilidade são treinados, compreendem e aplicam as políticas de segurança?
D5 **Adequação** **Questões:** **20 a 24**	Existe um controle interno da segurança da informação por meio de auditorias?	São realizadas avaliações visando a identificação e análise de riscos associados à realização dos objetivos de negócio da organização? Existem procedimentos de controle para certificar que as diretrizes dos gestores são implementadas? São processadas e divulgadas informações e revisões relacionadas aos sistemas utilizados para a gestão eficaz e funções críticas do negócio?
	Existe um controle externo da segurança da informação por meio de auditorias?	Quem responde pela auditoria externa da organização quanto à segurança da informação? Em quais aspectos seria importante a mensuração da efetividade da arquitetura de segurança da informação adotada pela organização por meio de auditorias externas?

Fonte: Resultado da pesquisa

As análises qualitativas encontram-se no item 3.3 e os dados foram coletados por meio de um questionário digital, aplicado com auxílio da plataforma *Google Forms*.

3 ANÁLISE DE RESULTADOS

A apresentação de dados utilizada neste estudo de caso, assim como a dos resultados obtidos, deu-se pelo desenvolvimento de uma estrutura descritiva, objetivando melhor organização. Os resultados foram analisados conforme os dados obtidos dos questionamentos aplicados durante o primeiro semestre de 2016, contemplando os gestores das três áreas de T.I. da instituição – Sistemas; Infraestrutura e Redes; e a de Suporte.

3.1 Perfil dos entrevistados

O Quadro 5 apresenta o perfil dos gestores entrevistados, selecionados conforme o critério de escolha por conveniência. Caracteriza-se, pela relativa variedade, com faixas etárias de 20 a 40 anos, tempo de gestão na área de T.I. oscilando entre aproximadamente 1 a 3 anos e níveis de escolaridade entre pós-graduação *lato-sensu* e *stricto-sensu*. Verifica-se, portanto, que todos possuem, no mínimo, especialização a nível de extensão.

Quadro 5 – Perfil dos entrevistados

Gestores	Tempo de gestão	Escolaridade	Faixa etária
A	até 2 anos	Pós-graduação (Extensão)	40
B	até 3 anos	Pós-graduação (Extensão)	20
C	até 3 anos	Mestrado	30
D	até 1 ano	Pós-graduação (Extensão)	20
E	até 3 anos	Pós-doutorado	40

Fonte: Resultado da pesquisa

3.2 Análise quantitativa de dados

A etapa quantitativa da coleta de dados foi aplicada em maio de 2016, e os dados foram extraídos do questionário digital aplicado por meio da plataforma *Google Forms*, em planilhas no formato Excel, que permitem a realização de cálculos estatísticos para apoiar a análise e verificação de tendências ou divergências.

Os dados obtidos estão representados no Quadro 6, e contêm um total de 10 questões enumeradas de Q01 a Q10, formuladas conforme os autores apresentados nos Quadros 2 e 3, classificadas de 1 (“concordo totalmente”) a 6 (“discordo totalmente”) e divididas em 5 dimensões: organização de segurança e infraestrutura (Q01 e Q02), políticas de segurança, normas e procedimentos (Q03, Q04 e Q05), programa de segurança (Q06), treinamento e conscientização da cultura de segurança (Q07 e Q08) e, por fim, adequação (Q09 e Q10).

Quadro 6 – Dados extraídos na primeira etapa da pesquisa

		Questões de pesquisa									
		D1		**D2**			**D3**	**D4**		**D5**	
		Q01	**Q02**	**Q03**	**Q04**	**Q05**	**Q06**	**Q07**	**Q08**	**Q09**	**Q10**
Gestores	**A**	3	3	4	4	3	4	3	2	1	1
	B	4	4	5	5	5	2	3	6	1	1
	C	4	5	6	6	3	3	3	6	2	1
	D	5	5	6	6	6	3	3	4	3	1
	E	4	3	4	4	4	4	2	2	1	1

Fonte: Resultado da pesquisa

As respostas referentes à dimensão D1 quanto à organização de segurança e infraestrutura (Q01 e Q02) apresentam poucas variações e, segundo os gestores, as pessoas entendem e desempenham seus papéis, no que diz respeito à segurança, de maneira satisfatória, assim como têm suas responsabilidades definidas, havendo, porém, margem para melhorias.

Organizações possuem foco na eficiência e envolvem relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle, sendo papel dos gestores alinhar os investimentos com a estratégia das organizações. Cabe aos mesmos, ainda, assegurar que a infraestrutura seja adequada à crescente utilização de novas aplicações, possibilitando um trabalho eficiente e produtivo, com transparência e responsabilidade gerencial (OECD, 2015; IBGC, 2014; THOMPSON *et al.*, 2013; AKABANE, 2012; BRIS; BRISLEY; CABOLIS, 2008; ARTERO, 2007; HARDY, 2006; VAN GREMBERGEN; DE HAES; GULDENTOPS, 2004; ITGI, 2003; ALEXANDER, 2000).

No que se refere à dimensão D2 de políticas de segurança, normas e procedimentos (Q03, Q04 e Q05), apesar da pequena variação apresentada quanto aos procedimentos de

segurança, as respostas indicam maior concordância de que estes são desenvolvidos, assim como concordam que há políticas e normas estabelecidas.

Uma das responsabilidades de governança reside em supervisionar cada vez mais a segurança da informação. Essa atenção é justificada, especialmente, pelo fato de que a legislação brasileira contempla uma grande quantidade de dispositivos legais, decretos, leis, instruções normativas e projetos de lei relativos ao tema, e que devem ser obrigatoriamente observados (ISO/IEC 38500, 2015; JUIZ; TOOMEY, 2015; VIEIRA; ALBUQUERQUE JR.; SANTOS, 2014; FRAGA, 2014; ISO/IEC 27001, 2013; ARAÚJO; 2012).

Não obstante, a correta aplicação de medidas de segurança, políticas, procedimentos e diretrizes auxiliam para que o risco seja adequadamente identificado e reportado, podendo, assim, ser utilizado como base na tomada de decisões (JOURDAN *et al.*, 2010; ABNT, 2009a).

O gráfico de linhas ilustrado pela Figura 8 contempla as respostas dos gestores e permite uma melhor visualização das mesmas.

Figura 8 – Gráfico de linhas contemplando as respostas dos gestores

Fonte: Resultado da pesquisa

Observa-se, por outro lado, que apesar da mesma variação, as respostas dos entrevistados, no que diz respeito às dimensões D3 (programa de segurança – Q06), D4 (treinamento e conscientização da cultura de segurança – Q07 e Q08) e D5 (adequação – Q09 e Q10), apresentam-se com maior intensidade na faixa de discordância. Ressalta-se, contudo,

a necessidade de um maior aprofundamento da pesquisa para verificar os motivos determinantes desse fato.

Não obstante, conforme apresentado nos Quadros 7 e 8, a análise das respostas por gestor e por questão de pesquisa que apresentam coeficiente de variação elevado podem ter relação com elementos não abordados na etapa quantitativa deste estudo ou até mesmo com o perfil dos entrevistados apresentado no Quadro 5.

Quadro 7 – Média (M), desvio padrão (D.P.) e coeficiente de variação (C.V.) por gestor

		M	D.P.	C.V.
Gestores	**A**	2,8	1,1	40,55%
	B	3,6	1,8	49,34%
	C	3,9	1,8	45,95%
	D	4,2	1,7	40,16%
	E	2,9	1,3	44,37%

Fonte: Resultado da pesquisa

O Quadro 8 contém, ainda, a média, desvios padrão e coeficiente de variação das respostas por questão de pesquisa e destaca questões relativas ao programa de segurança (D3), treinamento e conscientização da cultura de segurança (D4) e adequação (D5), que apresentaram média inferior a 4 ou coeficiente de variação muito elevado.

Quadro 8 – Média (M), desvio padrão (D.P.) e coeficiente de variação (C.V.) do questionário estruturado

	Questões de pesquisa									
	D1		**D2**			**D3**	**D4**		**D5**	
	01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
M	4,0	4,0	5,0	5,0	4,2	3,2	2,8	4,0	1,6	1,0
D.P.	0,7	1,0	1,0	1,0	1,3	0,8	0,4	2,0	0,9	0,0
C.V.	17,7%	25,0%	20,0%	20,0%	31,0%	26,1%	16,0%	50,0%	55,9%	0,0%

Fonte: Resultado da pesquisa

Analisando estes resultados, verifica-se que:

- **Dimensão 3** – Programa de segurança: as respostas da questão 6, apesar de convergentes, apresentam média de 3,2, indicando que os respondentes discordam de que haja organização do programa de segurança da informação que leve em conta a gestão de riscos.
- **Dimensão 4** – Treinamento e conscientização da cultura de segurança: as respostas da questão 07, apesar de convergentes, apresentam média de 2,8 e permitem verificar que os respondentes discordam de que haja uma aplicação eficaz de treinamentos e conscientização dos usuários quanto à segurança da informação. Já as respostas da questão 08 apresentam desvio padrão de 2,0 e coeficiente de variação 50%, valores que indicam divergências entre os respondentes de que haja reflexo positivo da conscientização dos usuários. Apesar disso, esses valores podem estar relacionados a elementos não abordados nesta etapa da pesquisa.
- **Dimensão 5** – Adequação: as respostas da questão 09, além de estarem divergentes, apresentam média de 1,6, indicando que os respondentes discordam fortemente de que haja um controle interno por meio de auditorias. Por fim, quanto à questão 10, todos os respondentes atribuíram o menor valor possível (1,0), indicando que discordam totalmente de que haja aplicação de um controle externo por meio de auditorias.

Os pontos supracitados não permitiram uma clara compreensão dos fatores que influenciaram as respostas obtidas quanto ao programa de segurança (D3), ao treinamento e conscientização da cultura de segurança (D4) e à adequação (D5). Assim, é motivada a aplicação de uma pesquisa qualitativa, com o objetivo de obter um embasamento científico adequado e uma melhor abordagem para endereçar a questão de pesquisa.

3.3 Análise qualitativa de dados

A etapa qualitativa da coleta de dados foi aplicada em junho de 2016, os dados foram extraídos do questionário digital baseado no Quadro 4 e aplicado por meio da plataforma *Google Forms*, em texto plano.

Para melhor compreensão dos dados coletados e aprofundamento no estudo, foi utilizada a análise de conteúdo. Segundo Bardin (2011), essa abordagem consiste em um conjunto de técnicas de análise das comunicações que, em sua função heurística, enriquece a tentativa exploratória, aumentando a propensão para a descoberta.

As diferentes fases da análise de conteúdo se organizam em torno de três polos cronológicos: pré-análise; exploração do material; tratamento dos resultados, inferência e interpretação. A fase de pré-análise trata da organização propriamente dita, tendo como objetivo sistematizar as ideias iniciais, de maneira a conduzir a um esquema preciso do desenvolvimento das operações sucessivas, num plano de análise; a exploração do material é essencialmente a codificação e decomposição em função de regras previamente formuladas e, por fim, o tratamento dos resultados obtidos e interpretação é o tratamento dos dados de maneira que estes sejam significativos.

Por meio de uma análise documental, é possível representar o conteúdo de um documento sob a forma diferente do original, a fim de facilitar, num estudo ulterior, a sua consulta e referenciação. Enquanto tratamento da informação contida nos documentos acumulados, a análise documental tem por objetivo dar forma conveniente e representar de outro modo essa informação por intermédio de procedimentos de transformação. Dessa maneira, buscou-se tanto um alcance descritivo como a inferência visual por meio de nuvem de palavras, dando maior destaque a características que se repetem dentro do conteúdo das respostas.

Destaca-se que, nesta etapa da pesquisa, devido a restrições de tempo, dois dos 5 cinco respondentes submeteram suas respostas de forma conjunta, resultando em um total de 4 (quatro) respostas por questão de pesquisa.

Nos Quadros 9, 10 e 11 estão descritas as respostas dos gestores (A, B, C e D) referentes aos questionamentos abertos (Q11 à Q24), e, para melhor visualização das características das mesmas, foram utilizadas nuvens de palavras, dando maior destaque às que mais se repetem.

Quadro 9 – Respostas do questionário aberto referentes à Dimensão 3 – Programa de segurança

Q11) Há algum método utilizado para classificar as informações?
A – Não. B – Não, o processo é empírico. Quando há necessidade de classificação se recorre a legislação, se não se encontra a definição são tomadas deliberações subjetivas geralmente baseadas em conhecimentos tácitos. C – Sim. D – Não.
Q12) Há alguém responsável dentro do programa de segurança da informação para realizar avaliações de risco periódicas?
A – Não. B – Não. C – Não. Não há um responsável definido e ocorre sob demanda. D – Não, pois há um responsável, porém, não foi definido a periodicidade.
Q13) Quando ocorrem incidências e violações de segurança, estes são monitorados e investigados visando melhorias?
A – Sim, de forma pontual. B – Sim. C – Sim. D – Sim, sendo que para cada incidente verificado, dependendo da ação realizada, abrangemos todo o data center para aplicar a melhoria.

Fonte: Resultado da pesquisa

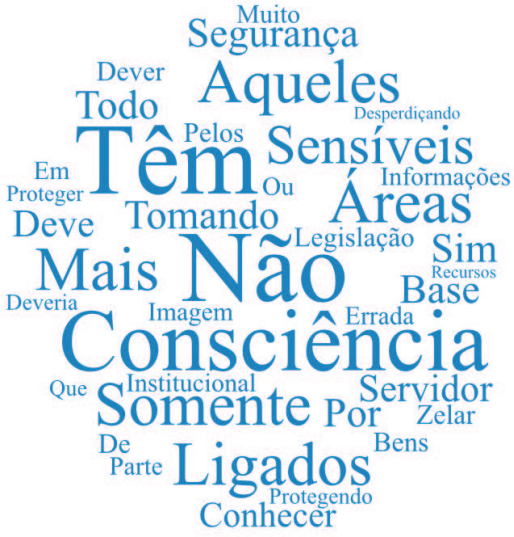
No que tange ao programa de segurança, a maioria dos respondentes discorda de que haja um método de classificação das informações, sendo ainda considerado algo baseado na legislação, conhecimentos tácitos, experiências e observações. Também não há um responsável dentro do programa de segurança definido para realizar avaliações de risco periódicas, ocorrendo estas sob demanda. Por outro lado, segundo os gestores, incidências e violações de segurança são monitorados e incidentes são investigados, ainda que de forma pontual, para que melhorias sejam aplicadas.

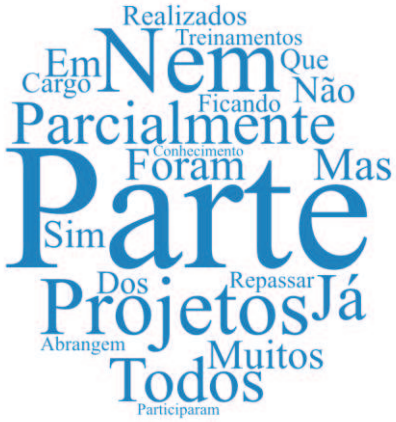
Mesmo monitorando, identificando e avaliando riscos, tomar decisões de modo racional envolve também a busca por meios de assegurar a proteção dos ativos de informação organizacional (ABNT, 2011; ABNT, 2009a; HARDY, 2006).

Ao investir na segurança de seus ativos de informação por meio de sua classificação, treinamentos e conscientizações, governos e organizações obtêm melhorias não somente na tomada de decisões, como também na continuidade de suas operações. A administração do risco demanda uma ampla gama de tomada de decisões, sendo necessária atenção às possíveis falhas ou erros, o que inclui a informação e a complexa tecnologia envolvida em seu processo. É crucial que haja o controle de risco, tanto pela ação direta dos gestores e funcionários como por delegações dos diretores, que podem se utilizar de qualquer oportunidade para formular

diretivas estratégicas e de liderança (DA VEIGA; MARTINS, 2015; JOURDAN *et al.*, 2010; NIST, 2010; PURDY, 2010; BERNSTEIN, 1997).

Quadro 10 – Respostas do questionário aberto referentes à Dimensão 4 – Treinamento e conscientização da cultura de segurança

Q14) O treinamento dos funcionários quando a segurança da informação tem dados os resultados esperados?	
A – Ainda não foi possível avaliar B – Sim. C – Em parte D – Até agora, foram feitos treinamentos focados em assuntos específicos e têm dado bons resultados.	
Q15) Os funcionários têm consciência de sua responsabilidade em proteger os ativos de informação da empresa?	
A – Somente aqueles ligados a áreas mais sensíveis à segurança B – Sim, tomando por base que todo servidor deve conhecer a legislação e o dever de zelar pelos, bens, informações e imagem institucional. C – Em parte D – Muito não têm consciência ou têm consciência errada, protegendo o que não deveria proteger desperdiçando recursos.	
Q16) Os funcionários reconhecem potenciais violações de segurança e sabem quem contatar nestes casos?	
A – Sim. B – Sim. C – Reconhecem eventualmente, mas sempre procuram o setor de Tecnologia da Informação. D – Em parte.	

Q17) Os administradores de sistemas participam de treinamentos técnicos de segurança relativos aos sistemas operacionais, redes, bancos de dados ou aplicativos que eles gerenciam?	
A – Sim. B – Parcialmente, em parte dos projetos. C – Em parte. D – Nem todos. Já foram realizados muitos treinamentos, mas não abrangem todos ficando a cargo dos que participaram em repassar o conhecimento.	
Q18) Existem agentes de segurança responsáveis por integrar uma arquitetura de segurança da informação e de seus componentes a um programa de conscientização e treinamento?	
A – Não. B – Não. C – Não. D – Hoje não há segregação dessa função. Tínhamos um setor com essa responsabilidade, mas essa parte do setor foi absorvido pelo outro e hoje não possui tal especialidade ficando de forma ad-hoc a responsabilização por essa função.	
Q19) Os gerentes de departamento asseguram-se de que os funcionários que atuam sob sua responsabilidade são treinados, compreendem e aplicam as políticas de segurança?	
A – Não. B – Não. C – Parcialmente, em parte dos projetos. D – Não há formalização dessa afirmação.	

Fonte: Resultado da pesquisa

Quanto ao treinamento e conscientização da cultura de segurança, os respondentes concordam em partes de que haja algum resultado positivo em relação ao treinamento de segurança da informação. Este, de acordo com as respostas, pode ser conduzido por assuntos específicos e, apesar de reconhecerem potenciais violações de segurança, a conscientização dos funcionários sobre suas responsabilidades em proteger ativos de informação se baseia em imposições legais e se apresenta de forma mais concreta em áreas mais sensíveis à segurança.

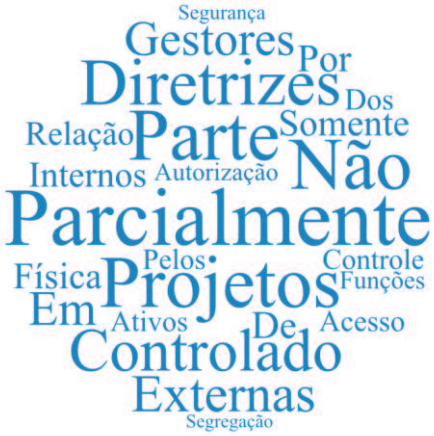
A privacidade da informação e sua segurança são dois conceitos inter-relacionados à proteção, e ambos devem ser considerados ao se tratar dos riscos da informação, verificando-se princípios que estão em consonância com preferências organizacionais e se há conscientização quanto à aplicação destes aos demais contextos organizacionais. Além disso, um bom planejamento e implementação de mecanismos formais de governança de T.I.,

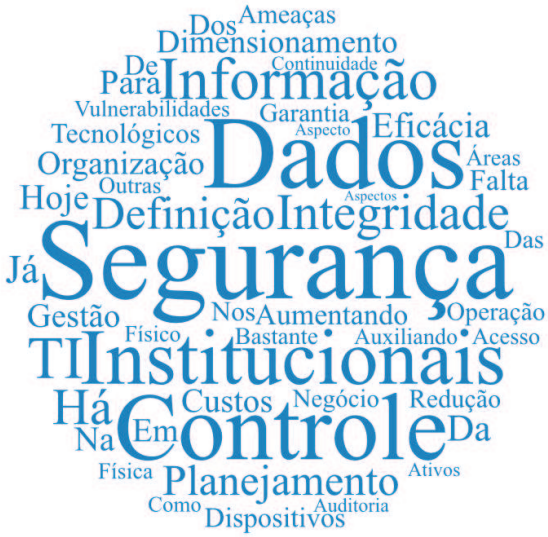
aliados a uma cultura de segurança da informação, requer não somente cooperação de toda a organização, mas também por parte dos gestores (DA VEIGA; MARTINS, 2015; MONTESDIOCA; MAÇADA, 2015; LUNARDI; BECKER; MAÇADA, 2012).

Ainda segundo os gestores, não há um treinamento referente à compreensão e aplicação de políticas de segurança. Mesmo que a participação de administradores de sistemas nos treinamentos técnicos relativos aos sistemas operacionais, redes, bancos de dados ou aplicativos que eles gerenciam ocorre de forma parcial em projetos, o repasse destas informações é feito pelos próprios participantes, não havendo agentes responsáveis por integrar uma arquitetura de segurança da informação e de seus componentes a um programa de conscientização e treinamento.

É papel dos gestores alinhar as necessidades específicas com a estratégia da organização também por meio da conscientização, uma vez que as complexidades a serem mensuradas no ambiente público podem abordar performance, transparência, investimento em infraestrutura, liberdade de atuação, redução de custos e outros (THOMPSON *et al.*, 2013; ISO/IEC 27001, 2013; ISO/IEC 27002:2013; DA VEIGA; ELOFF, 2007; WEILL; ROSS, 2004; TUDOR, 2000).

Quadro 11 – Respostas do questionário aberto referentes à Dimensão 5 – Adequação

<table>
<tr><th colspan="2">Q20) São realizadas avaliações visando a identificação e análise de riscos associados à realização dos objetivos de negócio da organização?</th></tr>
<tr><td colspan="2">A – Não.
B – Não.
C – Sim.
D – Formalmente em projetos de aquisição/contratação e informalmente em projetos de implantação.</td></tr>
<tr><th colspan="2">Q21) Existem procedimentos de controle para certificar que as diretrizes dos gestores são implementadas?</th></tr>
<tr><td>A – Somente em relação à autorização, controle de acesso, segurança física de ativos e segregação de funções
B – Parcialmente, em parte dos projetos.
C – Em parte.
D – Parcialmente controlado por diretrizes externas e não pelos gestores internos.</td><td> 
</td></tr>
</table>

Q22) São processadas e divulgadas informações e revisões relacionadas aos sistemas utilizados para a gestão eficaz e funções críticas do negócio?	
A – Não. B – Não. C – Em parte. D – Sim, no portal da TI.	
Q23) Quem responde pela auditoria externa da organização quanto à segurança da informação?	
A – O Assessor de Tecnologia da Informação. B – Desconheço. C – A Diretoria de Infraestrutura e redes. D – CGU e TCU.	
Q24) Em quais aspectos seria importante a mensuração da efetividade da arquitetura de segurança da informação adotada pela organização por meio de auditorias externas?	
A – No aspecto da segurança e integridade dos dados. B – Segurança dos dados institucionais e garantia da continuidade do negócio. C – Nos aspectos de planejamento (definição, dimensionamento e organização) dos dispositivos tecnológicos, aumentando a eficácia na gestão das ameaças e vulnerabilidades e auxiliando na redução de custos da operação. D – Hoje já há bastante controle para a segurança da informação em TI e falta auditoria da segurança da informação em outras áreas como controle de acesso físico e segurança física de ativos.	

Fonte: Resultado da pesquisa

No que se refere à adequação, segundo os gestores, os procedimentos de controle para certificar que diretrizes sejam implantadas existem apenas em partes ou relativos a projetos ou diretrizes externas, e, apesar de haver um portal de T.I., as informações e revisões relacionadas aos sistemas utilizados para a gestão eficaz e funções críticas do negócio não são amplamente divulgadas. Desse modo, as avaliações e análises de riscos associados à realização dos objetivos de negócios da organização são pouco presente ou ocorrem formalmente em projetos de aquisição e informalmente em projetos de implantação.

A prevenção da perda, dano, destruição ou acesso não autorizado à informação processada por organizações é um processo contínuo, uma vez que a constante evolução dos riscos internos e externos pode resultar em violações e perdas para a organização como um todo. Administrar o risco nos guia por uma ampla gama de tomada de decisões, sendo

necessária atenção às possíveis falhas ou erros, incluindo a informação e a complexa tecnologia envolvida em seu processo, como apoio para alcançar os objetivos e metas de negócio (DA VEIGA; MARTINS, 2015; JUIZ; TOOMEY, 2015; LUFTMAN, 2003; BERNSTEIN, 1997).

No tocante à mensuração dos aspectos de segurança da informação, segundo os respondentes a segurança de ativos, dispositivos tecnológicos, acesso físico e integridade dos dados são aplicáveis ao planejamento e continuidade do negócio, assim como auxiliam na redução de custos e eficácia na gestão de ameaças e vulnerabilidades. Entretanto, há grande divergência quanto ao responsável pela auditoria externa de segurança da informação.

Além da obrigatoriedade em observar os dispositivos legais, 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; VIEIRA; FRAGA, 2014; ARAÚJO, 2012).

3.4 Considerações finais

Conforme os resultados obtidos nas análises quantitativa e qualitativa, verifica-se que os aspectos analisados da gestão de riscos de segurança da informação, envolvendo princípios como organização de segurança e infraestrutura, políticas, programas de segurança, treinamento, conscientização e adequação, são convergentes e remetem à uma preocupação, por parte da instituição, com o ambiente de risco em que esta opera.

Os princípios podem ser vistos como dimensões da arquitetura de segurança da informação, abrangendo aspectos da gestão de risco, da governança corporativa, da criação de valor por parte da T.I e da segurança da informação, assim como proteção de informações confidenciais em conformidade com a legislação, o que permitiu a esta pesquisa atingir o seu objetivo. Além disso, os autores aqui estudados e as áreas de foco da governança de T.I. – apresentadas na Introdução (Figura 2) – que tratam do alinhamento estratégico, entrega de valor, gestão de recursos, mensuração de desempenho e, em especial, a gestão de riscos, permitem estabelecer as relações entre os planos de negócios, a T.I., a execução da proposta por meio do ciclo de entrega, a melhor utilização possível dos investimentos e recursos, a otimização do conhecimento, monitoramento de processos e gerenciamento do ambiente de risco nas atividades da organização, validando esses princípios-chave.

Segundo os gestores, no que diz respeito à segurança, as pessoas entendem e desempenham seus papéis de maneira satisfatória, assim como têm suas responsabilidades definidas. Há, porém, margem para melhorias, certificando-se de que a infraestrutura seja adequada à crescente utilização de novas aplicações, possibilitando um trabalho eficiente e produtivo, com transparência e responsabilidade gerencial.

A instituição desenvolve procedimentos de segurança, assim como estabelece políticas e normas internas, o que auxilia para que o risco seja adequadamente identificado e reportado, podendo, assim, ser utilizado como base na tomada de decisões.

Apesar das incidências e violações de segurança serem monitoradas e investigadas – mesmo que de forma pontual – para que melhorias sejam aplicadas, os gestores discordam de que haja um programa de segurança ou um método de classificação das informações que leva em conta a gestão de riscos, sendo o mesmo considerado como algo baseado na legislação, conhecimentos tácitos, experiências e observações. Não há também um responsável dentro do programa de segurança definido para realizar avaliações de risco periódicas, ocorrendo estas sob demanda.

Quanto ao treinamento e conscientização de usuários acerca da cultura de segurança da informação, os gestores discordam de que haja sua aplicação eficaz e um reflexo positivo dela, uma vez que esse processo é conduzido por assuntos específicos e, apesar de reconhecerem potenciais violações de segurança, a conscientização dos funcionários quanto às suas responsabilidades em proteger ativos de informação se baseia em imposições legais e se apresenta de forma mais concreta em áreas mais sensíveis à segurança.

No que se refere à adequação os gestores apontam que o controle interno por meio de auditorias ainda é pouco presente, assim como não há a aplicação de um controle externo por meio de auditorias. Os procedimentos de controle para certificar que diretrizes sejam implantadas existem apenas em partes ou relativos a projetos ou diretrizes externas. Apesar de haver um portal de T.I., as informações e revisões relacionadas aos sistemas utilizados para a gestão eficaz e funções críticas do negócio não são amplamente divulgadas, e as avaliações e análises de riscos associados à realização dos objetivos de negócios da organização são pouco presente ou ocorrendo formalmente em projetos de aquisição ou contratação e informalmente em projetos de implantação.

Verifica-se, também, que há margem para aplicação de melhorias, especialmente no que tange ao programa de segurança, conscientização de segurança da informação por meio de treinamentos, avaliação de riscos, controles técnicos e adequação abordados no Quadro 2 e

itens 2.4, estudo quantitativo e 2.5, estudo qualitativo, auxiliando a instituição a entender o ambiente de riscos no qual opera e as oportunidades que este oferece.

Portanto, mesmo considerando as limitações desta pesquisa pela amostragem não probabilística e por conveniência observa-se, a partir dos dados analisados, que os componentes verificados possuem aplicação na instituição, havendo também uma preocupação com o ambiente de risco em que opera (SAMPIERI; COLLADO; LUCIO, 2006; MALHOTRA, 2001; OLIVEIRA, 2001; KISH, 1965). Essa situação é caracterizada não somente pela obrigatoriedade em observar dispositivos os legais constantes na Tabela 2 e Quadro 1, mas também por envolver componentes da governança corporativa e a criação de valor por meio dos ativos de tecnologia da informação (DA VEIGA; MARTINS, 2015; VIEIRA; FRAGA, 2014; ARAÚJO 2012; DA VEIGA; ELOFF, 2007; BERNSTEIN, 1997).

CONCLUSÃO

Este estudo buscou analisar os aspectos da segurança da informação dentro da gestão de risco dentro na governança de T.I. de uma instituição de ensino público federal e sua principal contribuição, tanto na perspectiva prática quanto teórica, reside na análise de aspectos da segurança da informação dentro da gestão de risco na governança de T.I., que envolvem princípios como organização de segurança e infraestrutura, políticas de segurança, normas e procedimentos, programa de segurança, treinamento e conscientização da cultura de segurança e adequação.

Não obstante, as limitações desta pesquisa, além de restrições de recursos financeiros, referem-se à aplicação da técnica para a coleta de dados baseada em uma amostragem não probabilística, cujo critério de seleção de cada elemento foi por conveniência e se restringiu à reitoria do Instituto Federal de Educação, Ciência e Tecnologia, não tendo sido ampliada aos demais *campi* pertencentes à rede, sendo, portanto, não aleatória e não permitindo generalizações do resultado.

Sugere-se, dessa forma, a ampliação deste estudo, contemplando maiores amostras, com tratamentos mais específicos em relação às normas e vinculação às leis, assim como a utilização de outras técnicas que contemplem este contexto em novas pesquisas.

REFERÊNCIAS

AAKER, D.; KUMAR, V.; DAY, G. **Marketing research.** New York: John Wiley & Sons, 1995.

ABNT. **NBR ISO 31000**: Gestão de riscos – Princípios e diretrizes. Rio de Janeiro**:** Associação brasileira de normas técnicas, 2009a, p. 24.

_____. **NBR ISO/IEC 38500**: Governança corporativa de tecnologia da informação. .Rio de Janeiro: Associação brasileira de normas técnicas, 2009b, p. 15.

_____. **NBR ISO/IEC 27005**: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação. Rio de Janeiro: Associação brasileira de normas técnicas, 2011, p. 87.

AKABANE, G. 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.

ALEXANDER, L. Corporate governance and cross-border mergers. **Conference Board Research Report**, Nova York, jun. 2000.

ALEXANDRIA, J. C. S. **Gestão de segurança da informação** – uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. 2009. 192f. Tese (doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

ARAÚJO, W. 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.

ARTERO, J. P. **Corporate Governance: The revival of an academic, professional and policy field.** New YorK: JP Morgan Chase, 2007, p.1-25.

BARDIN, L. **Análise de conteúdo**. (Tradução de: Luís Antero Reto e Augusto Pinheiro). São Paulo: Edições 70, 2011.

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

CERT.BR. **Incidentes Reportados ao CERT.br –** Janeiro a Dezembro de 2015. Brasília: Comitê Gestor da Internet no Brasil. Disponível em: <http://www.cert.br/stats/>. Acesso em 10 de nov. 2015.

_____. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 1988.

_____. Ministério da Educação. **Estatuto do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo.** Brasília, DF: Senado Federal. Disponível em: <http://www.ifsp.edu.br/index.php/documentos-institucionais/estatuto.html>. Acesso em: 10 nov. 2015b.

_____. Ministério da Educação. **Portal da Tecnologia da Informação do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo**. Brasília, DF: Senado Federal. Disponível em: <http://ti.ifsp.edu.br/>. Acesso em: 10 nov. 2016a.

_____. Ministério da Educação. **Política de Segurança da Informação**. Brasília, DF: Senado Federal. Disponível em:<https://nuvem.ifsp.edu.br/public.php?service=files&t=ab70b662b5a94953a3a53df38ccaf308>. Acesso em: 10 nov. 2016b.

_____. Eliezer Pacheco. Secretaria de Educação Profissional e Tecnológica do Ministério da Educação. **Os Institutos Federais:** uma Revolução na Educação Profissional e Tecnológica. Brasília, DF: Senado Federal. Disponível em: <http://portal.mec.gov.br/setec/arquivos/pdf/insti_evolucao.pdf>. Acesso em: 10 nov. 2016.

BRIS, A.; BRISLEY, N.; CABOLIS, C. Adopting better corporate governance: Evidence from cross-border mergers. **Journal of Corporate Finance**, Grécia, v. 3, n. 14, p. 224-240, fev. 2008.

BROMILEY, P.; MCSHANE, M.; NAIR, A.; RUSTAMBEKOV, E. Enterprise Risk Management: Review, Critique, and Research Directions. **Long Range Planning**, [s.l.], v. 48, n. 1, p. 265-276, jan. 2015.

CADBURY, A. **The Financial Aspects of Corporate Governance**. Londres*:* Committee on the Financial Aspects of Corporate Governance, 1992, p. 90.

CHAU, S. L. **An Anatomy of Corporate Governance**. Hong Kong: Hang Seng Management College, p.1-16, dez. 2011.

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

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

_____. A framework and assessment instrument for information security culture. **Computers & Security**, v. 29, n. 2, p.196-207, mar. 2010.

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

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

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

FOWLER JR., F. **Survey research methods**. 8 ed. Thousand Oaks: Sage, 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, G. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. **Information Security Technical Report**, 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.

IBGC. **Guia das melhores práticas de governança para fundações e institutos empresariais**. 2.ed. São Paulo: IBGC e GIFE, 2014. Disponível em< http://www.ibgc.org.br/userfiles/files/GUIA%20GIFE%20_%202014%281%29.pdf>. Acesso em: 12 jun. 2015.

ISACA. **COBIT 5: Modelo Corporativo para Governança e Gestão de T.I.** Rolling Meadows: Information Systems Audit and Control Association, 2012, p. 98.

ISO 31000:2009. **Risk Management**: Principles and guidelines. International Organization for Standardization, ISO. 2009.

ISO/IEC 27001:2013. **Information technology** – Security techniques – Information security management systems – Requirements. International Organization for Standardization, ISO. 2013.

ISO/IEC 27002:2013. **Information technology** – Security techniques – Code of practice for information security management. International Organization for Standardization, ISO. 2013.

ISO/IEC 38500:2015. **Information technology** – Governance of IT for the organization. International Organization for Standardization, ISO. 2015.

ITGI. **Board Briefing on IT Governance**. 2ª Ed. Rolling Meadows: It Governance Institute, 2003, p. 7.

_____. **COBIT 4.1**: Objetivos de Controle para Informações e Tecnologias Correspondentes. Rolling Meadows: IT Governance Institute, 2007, p. 212.

_____. **Enterprise Value Governance of IT Investments** – The Val IT Framework 2.0 Extract. Rolling Meadows: IT Governance Institute, 2008, p. 45.

JOURDAN, Z.; RAINER, R.K.; MARSHALL, T.E.; FORD, F.N. An investigation of organizational information security risk analysis. **Journal of Service Science**, vol. 3 Alabama, 2010, p. 9.

JUIZ, C.; TOOMEY, M. To govern IT, or not to govern IT? **Communications of the ACM,** v. 58, n. 2, p. 58-64, fev. 2015.

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

KISH, L. **Survey sampling.** New York: John Wiley & Sons, 1965.

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 (TI) 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.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G. Um estudo empírico do impacto da governança de T.I. no desempenho organizacional. **Produção**, v. 22, n. 3, p. 612-624, maio/ago 2012.

LUNARDI, G. L.; BECKER, J. L.; MAÇADA, A. C. G.; DOLCI, P. C. The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. **International Journal of Accounting Information Systems**, v. 15, n. 1, p.66-81, mar. 2014.

MALHOTRA, N. K. **Pesquisa de marketing** – Uma orientação aplicada. 3ª 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.** São Paulo: Atlas. 1996.

MIGUEL, P. A. C. Estudo de caso na engenharia de produção: estruturação e recomendações para sua condução. **Produção**, São Paulo, v. 17, n. 1, p. 216-229, jan. 2007.

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

NIST. **Guide for Applying the Risk Management Framework to Federal Information Systems:** A Security Life Cycle Approach. Gaithersburg: National Institute of Standards and Technology, 2010, p. 93.

NOBRE, A. C. S.; RAMOS, A. S. M.; NASCIMENTO, T. C. Fatores que influenciam a aceitação de práticas avançadas de gestão de segurança da informação: um estudo com gestores públicos estaduais no Brasil. **Anais do encontro da associação nacional de pós-graduação e pesquisa em administração**, Rio de Janeiro: Editora 34, 2010.

OECD. Principles of Corporate Governance. Organisation for Economic Co-operation and Development. OECD Publishing. 2015. Disponível em: < https://www.oecd.org/corporate/principles-corporate-governance.htm>. Acesso em: 10 jun. 2015.

_____. Risk Management and Corporate Governance. Organisation for Economic Co-operation and Development. OECD Publishing. 2014. Disponível em: < http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf>. Acesso em: 09 jun. 2015.

O GLOBO. CPI investiga vazamento de informações sigilosas. **O Globo**, Rio de Janeiro, 26 de jun. de 2012. Disponível em <http://glo.bo/LLkl1D>. Acesso em 15 de nov. 2016.

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**, 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), p. 638-646, 2004.

PURDY, G. ISO 31000: 200 – Setting a New Standard for Risk Management. **Risk Analysis**, v. 30, n. 6, p. 881-886, abr. 2010.

RAGHUPATHI, W. Corporate governance of IT: A framework for development. **Communications of the ACM**, v. 8, n. 1, p. 94-99, ago. 2007.

RIBEIRO, S. Polícia prende quadrilha que vendia dados sigilosos da Receita Federal em SP. **G1**, São Paulo, 24 de abr. 2007. Disponível em <g1.globo.com/Noticias/SaoPaulo/0,,MRP26487-5605,00.html>. Acesso em 15 de nov. 2016.

SAMPIERI, R. H.; COLLADO, C. F.; LUCIO, M. P. B.. **Metodología de la Investigación**. 4ª ed. Cidade do México: Mac Graw Hill, 2006, p.736.

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

SCHIFFMAN, L.; KANUK, L. **Comportamento do consumidor.** 6ª ed. São Paulo: LTC Editora, 2000.

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

SINGH, S. **O livro dos códigos:** a ciência do sigilo o do antigo Egito à criptografia quântica. Rio de Janeiro: Record, 2001.

THOMPSON, S.; EKMAN, P.; SELBY, D.; WHITAKER J. A model to support IT infrastructure planning and the allocation of IT governance authority. **Decision Support Systems**, v. 59, n. 1, p. 108-118, nov. 2013.

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

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

VIEIRA, T. M.; FRAGA, J. A. 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.

WEILL, P. Don't just lead, govern: How top-performing firms govern IT. **Center For Information Systems Research,** Massachusetts, v. 3, n. 1, p. 17, mar. 2004.

WEILL, P.; ROSS, J. W. **IT governance: how top performers manage IT decisions rights for superior results**. Boston: HBS Press, 2004.

WEILL, P.; WOODHAM, R. Don't Just Lead, Govern: Implementing Effective IT Governance. **Center For Information Systems Research,** Massachusetts, v. 326, n. 1, 20 p, abr. 2002.

YIN, R. K. **Estudo de caso: planejamento e métodos.** 2ª ed. Porto Alegre: Bookman, 2001.

APÊNDICE A – CARTA DE AUTORIZAÇÃO

São Paulo, 10 de fevereiro de 2016.

Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP.

Prezado Sr.,

Como parte da pesquisa realizada pelo Sr. Jackson Gomes Soares Souza sobre gestão de riscos de segurança da informação e sua apresentação na governança de tecnologia da informação da administração pública federal do programa de Pós-Graduação Stricto Sensu do Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS), alguns estudos de caso serão realizados.

Este estudo, sob a orientação do Prof. Dr. Carlos Hideo Arima, necessita de levantamento de dados mediante aplicação de questionário aos gestores responsáveis pela governança de tecnologia da informação do IFSP.

Desta forma, solicitamos a colaboração do Sr. e do IFSP em autorizar a realização desta pesquisa e asseguramos a confidencialidade dos dados e informações obtidos e a utilização deles unicamente para atender a finalidade desta pesquisa. Qualquer tipo de divulgação adicional será realizado mediante autorização prévia do IFSP.

Ao término da pesquisa, os resultados estarão disponíveis para a sua apreciação e consulta.

Atenciosamente,

Carlos Hideo Arima	Jackson Gomes Soares Souza
Prof. Dr. do Programa de Pós-Graduação do CEETEPS	Aluno do Programa de Pós-Graduação do CEETEPS

Assinatura do gestor

APÊNDICE B – ROTEIRO PARA QUESTIONÁRIO ESTRUTURADO FECHADO

ANTES DA APLICAÇÃO DO QUESTIONÁRIO

O questionário pretende verificar como a gestão de riscos de segurança da informação se apresenta na instituição conforme a percepção dos gestores de T.I..

Caso o respondente se abstenha de responder alguma alternativa, o pesquisador entenderá e respeitará tal decisão.

O objetivo da pesquisa não é julgar o trabalho realizado, mas analisar e compreender os resultados foram obtidos.

O pesquisador está interessado em analisar as respostas e resultados colocados à sua disposição.

DIMENSÃO 1 – ORGANIZAÇÃO DE SEGURANÇA E INFRAESTRUTURA

01) No que tange à segurança da informação, os papéis desempenhados pelas pessoas são definidos?

02) No que tange à segurança da informação, as responsabilidades das pessoas são definidas?

DIMENSÃO 2 – POLÍTICAS DE SEGURANÇA, NORMAS E PROCEDIMENTOS

03) São desenvolvidas políticas de segurança da informação?

04) São desenvolvidas normas de segurança da informação?

05) São desenvolvidos procedimentos de segurança da informação?

DIMENSÃO 3 – PROGRAMA DE SEGURANÇA

06) Um programa de segurança da informação é organizado tendo em conta a gestão de riscos?

DIMENSÃO 4 – TREINAMENTO E CONSCIENTIZAÇÃO DA CULTURA DE SEGURANÇA

07) Os usuários são treinados e conscientizados quanto à importância da segurança da informação?

08) Há reflexo positivo dessa conscientização?

DIMENSÃO 5 – ADEQUAÇÃO

09) Existe um controle interno da segurança da informação por meio de auditorias?

10) Existe um controle externo da segurança da informação por meio de auditorias?

APÊNDICE C – ROTEIRO PARA QUESTIONÁRIO ESTRUTURADO ABERTO

ANTES DA APLICAÇÃO DO QUESTIONÁRIO

O questionário aberto pretende aprofundar o estudo relativo às dimensões abordadas anteriormente e verificar como a gestão de riscos de segurança da informação se apresenta na instituição conforme a percepção dos gestores de T.I..

Caso o respondente se abstenha de responder alguma pergunta, o pesquisador entenderá e respeitará tal decisão.

O objetivo da pesquisa não é julgar o trabalho realizado, mas analisar e compreender os resultados foram obtidos.

O pesquisador está interessado em analisar as respostas e resultados colocados à sua disposição.

DIMENSÃO 3 – PROGRAMA DE SEGURANÇA

Referência: Programa de segurança da informação organizado tendo em conta a gestão de riscos

11) Há algum método utilizado para classificar as informações?

12) Há alguém responsável dentro do programa de segurança da informação para realizar avaliações de risco periódicas?

13) Quando ocorrem incidências e violações de segurança, estes são monitorados e investigados visando melhorias?

DIMENSÃO 4 – TREINAMENTO E CONSCIENTIZAÇÃO DA CULTURA DE SEGURANÇA

Referência: Treinamento e conscientização dos usuários quanto à importância da segurança da informação

14) O treinamento dos funcionários quando a segurança da informação tem dados os resultados esperados?

15) Os funcionários têm consciência de sua responsabilidade em proteger os ativos de informação da empresa?

16) Os funcionários reconhecem potenciais violações de segurança e sabem quem contatar nestes casos?

Referência: Reflexo da conscientização dos usuários

17) Os administradores de sistemas participam de treinamentos técnicos de segurança relativos aos sistemas operacionais, redes, bancos de dados ou aplicativos que eles gerenciam?

18) Existem agentes de segurança responsáveis por integrar uma arquitetura de segurança da informação e de seus componentes a um programa de conscientização e treinamento?

19) Os gerentes de departamento asseguram-se de que os funcionários que atuam sob sua responsabilidade são treinados, compreendem e aplicam as políticas de segurança?

DIMENSÃO 5 – ADEQUAÇÃO

Referência: Controle interno da segurança da informação por meio de auditorias

20) São realizadas avaliações visando a identificação e análise de riscos associados à realização dos objetivos de negócio da organização?

21) Existem procedimentos de controle para certificar que as diretrizes dos gestores são implementadas?

22) São processadas e divulgadas informações e revisões relacionadas aos sistemas utilizados para a gestão eficaz e funções críticas do negócio?

Referência: Controle externo da segurança da informação por meio de auditorias

23) Quem responde pela auditoria externa da organização quanto à segurança da informação?

24) Em quais aspectos seria importante a mensuração da efetividade da arquitetura de segurança da informação adotada pela organização por meio de auditorias externas?