Pós-Graduação em Ciência da Computação

ANDRÉ MACEDO

PROPOSTA PARA IMPLEMENTAÇÃO DE MELHORES PRÁTICAS PARA MITIGAÇÃO DE RISCOS EM INCIDENTES DE TI NOS INSTITUTOS FEDERAIS DE EDUCAÇÃO

Recife
2017

ANDRÉ MACEDO

PROPOSTA PARA IMPLEMENTAÇÃO DE MELHORES PRÁTICAS PARA MITIGAÇÃO DE RISCOS EM INCIDENTES DE TI NOS INSTITUTOS FEDERAIS DE EDUCAÇÃO

Este trabalho foi apresentado à Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre Profissional em Ciência da Computação.

ORIENTADOR: Prof. Dr. Ruy José Guerra Barretto de Queiroz

Recife
2017

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

M141p Macedo, André
Proposta para implementação de melhores práticas para mitigação de riscos em incidentes de TI nos institutos federais de educação / André Macedo. – 2017.
128 f.: il., fig., tab.

Orientador: Ruy José Guerra Barretto de Queiroz.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2017.
Inclui referências.

1. Segurança da informação. 2. Gestão de riscos. I. Queiroz, Ruy José Guerra Barretto de (orientador). II. Título.

005.8 CDD (23. ed.) UFPE- MEI 2018-082

André Macedo

Proposta para Implementação de Melhores Práticas para Mitigação de Riscos em Incidentes de TI nos Institutos Federais de Educação

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre Profissional em 27 de junho de 2017.

Aprovado em: 27 / 06 / 2017.

BANCA EXAMINADORA

_____

Prof. Rafael Dueire Lins
Centro de Informática / UFPE

_____

Prof. José Carlos Silva Cavalcanti
Centro de Ciências Sociais Aplicadas / UFPE

_____

Prof. Ruy José Guerra Barretto de Queiroz
Centro de Informática / UFPE
(Orientador)

Dedico esse trabalho a minha esposa Andréia que sempre esteve presente ao meu lado nos momentos mais difíceis e que me motivou nesta caminhada árdua e aos meus filhos Gabriel e Lia, razões do meu viver.

Agradecimentos

Gostaria de agradecer, acima de tudo a Deus por me dar o sopro de vida e o intelecto para dedicação neste trabalho.

A toda a minha família em especial minha esposa Andréia que tornou minha referência de persistência nos estudos as minhas razões de minha vida: Gabriel e Lia.

Agradeço a oportunidade de capacitação ao IFSC que me auxiliou nos custos com a bolsa e demais despesas para o mestrado.

Agradeço aos meus colegas de trabalho do IFSC que motivaram meus estudos.

Agradeço a todos os professores do CIN da Universidade Federal de Pernambuco pela formação profissional em especial ao meu orientador professor Doutor Ruy José Guerra Barretto de Queiroz, pela oportunidade dada e pelos caminhos que foram indicados.

Aos meus amigos da turma de mestrado profissional, Hamilton, Bruno, Paula, Leonardo, Bernardes e David pelo apoio moral nos estudos em Recife.

Finalmente, gostaria de agradecer aos que contribuíram de forma direta ou indireta à realização desta etapa da minha vida.

Obrigado a todos !

“Para nós os grandes homens não são aqueles que resolveram os problemas, mas aqueles que os descobriram.”
- ALBERT SCHWEITZER

Resumo

Essa dissertação tem como objetivo identificar dentre as melhores práticas de gestão de riscos baseados na literatura científica uma proposta de guia em gestão de riscos. Para isso essa proposta foi concebida através de uma metodologia de pesquisa em que se utilizou a abordagem qualitativa e quantitativa, empregando procedimentos metodológicos com o uso da revisão sistemática da literatura, aplicando procedimentos bibliográficos e o levantamento de campo com aplicação de questionário de pesquisa. Com os dados obtidos através do questionário foi possível realizar o diagnóstico atual das instituições federais de educação na administração pública federal no que diz respeito à gestão de riscos com o intuito de que esse guia auxilie os gestores de TI. Por meio do Acórdão 3117/2014-TCU-Plenário, o quadro crítico em que se encontravam os órgãos da administração pública federal, em relação a uma política de gestão de riscos somente 23% das organizações declararam dispor de política corporativa formalmente instituída (11% parcialmente e 12% integralmente), ou seja, a grande maioria dos participantes não dispõe de um instrumento necessário para direcionar as ações corporativas para avaliação dos riscos associados ao alcance dos resultados organizacionais. Ao final da pesquisa percebeu-se que os gestores são responsáveis por viabilizar e garantir o adequado funcionamento da gestão de riscos, com o estabelecimento de diretrizes, criação de estruturas, se necessário, e a definição de papéis e responsabilidades. Cabe também aos gestores, estabelecer os níveis de riscos aceitáveis para subsidiar o processo de tomada de decisão, sobretudo as de nível estratégico nas instituições federais de educação.

Palavras-chave: Gestão de Segurança da Informação. Gestão de Riscos. Boas práticas.

Abstract

The present work aims to identify the best practices in risk management. Based on the risk management literature, a guide was proposed. This suggested guide was designed through a qualitative and quantitative research methodology. The present approach draws upon a systematic review of the literature, using bibliographic research procedures and two types of data collection, namely, field survey and questionnaire. Data derived from the field survey and the questionnaire enabled us to establish the current diagnosis of Federal Institutes of Education within the context of federal public administration regarding to risk management. From this perspective, we developed this guide, which will help the IT managers. The present guide was developed from the legal document, namely, 3117/2014-TCU- complementary law, and the guide has enabled the construction of the field research in which a questionnaire was applied. Subsequently, the critical framework was developed and applied to federal public administration institutions. Results indicate that only 23% of the organizations declared themselves to have a corporate policy of risk management (11% partially and 12% fully), that is, the vast majority of participants do not have the necessary tool to direct corporate actions to assess the risks associated with the achievement of organizational results. Our final considerations indicate that the top management is responsible for ensuring the proper functioning of risk management, establishing guidelines, creating structures, if necessary, and defining roles and responsibilities. It is also up to senior management to establish acceptable levels of risk to support the decision-making process, especially at the strategic level at federal institutions of education.

Keywords: Information security management. Risk management. Best practices.

Lista de ilustrações

Lista de quadros

Lista de abreviaturas e siglas

ABNT	Associação Brasileira de Normas Técnicas
AHP	Analytic Hierarchic Process
APF	Administração Pública Federal
ASCOM	Assessoria de Comunicação
BPMN	Business Process Modeling Notation
CGSI	Comitê Gestor de Segurança da Informação
COBIT	Control Objectives for Information and related Technology
COPPE/UFRJ	COPPE/UFRJ - Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia
DSIC	Departamento de Segurança da Informação e Comunicações
ESR	Escola Superior de Redes
EUA	United States of America
FCS	Ficha de Controle de Serviços
FMEA	Failure Mode and Effect Analysis
GSIPR	Gabinete de Segurança Institucional da Presidência da República
GT	Grupo de Trabalho
GTI	Governança de Tecnologia da Informação
IAS	International Accounting Standards
IBGC	Instituto Brasileiro de Governança Corporativa
IDS	Sistema de detecção de intrusão
IEC	International Engineering Consortium
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IFE	Instituto Federal de Educação
ISACA	Information Systems Audit and Control Association
ISECOM	Intitute for Security and Open Methodologies

ISO	International Organization for Standardization
ISSAF	Information Systems Security Assessment Framework
ITIL	Information Technology Infrastructure Library
MEC	Ministério da Educação
MIS	Management Information Systems
MPOG	Ministério do Planejamento, Orçamento e Gestão
NBR	Norma Brasileira
NIST	National Institude of Standards and Technology
NIST SP 800-30	National Institute of Standards and Technology Special Publication 800-30
OGC	Office of Gorvenment Commerce
OSSTMM	Open Source Security Testing Methodology Manual
PDCA	Planejamento, Desenvolvimento, Controle e Ação
PDI	Plano de Desenvolvimento Institucional
PDTI	Plano Diretor de Tecnologia de Informação
PENTEST	Penetration Test
POSIC	Política de Segurança da Informação e Comunicação
PPGA	Programa de Prevenção a Gestação de Auto Risco
PSI	Política de Segurança da Informação
RM	Ranking Médio
SEFTI	Secretaria de Fiscalização de Tecnologia da Informação
SEGINFO	Segurança da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SIC	Segurança da Informação e Comunicação
SISP	Sistema de Administração de Recursos de Tecnologia da Informação
SLTI	Secretaria de Logística e Tecnologia da Informação

SP	Serviço Público
TAM	Technology Acceptance Model
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

Sumário

1 INTRODUÇÃO

As organizações precisam proteger suas informações, sejam elas sigilosas ou não e para que elas estejam seguras, requerem procedimentos (TUYIKEZE e FLOWERDAY, 2014). Este avanço está relacionado às recomendações do Tribunal de Contas da União (TCU) referente à implantação de gestão de riscos em TI. GUERRA; ALVES (2004) destacam que “a gestão de TI que utiliza boas práticas começa por elementos fundamentais que irão ajudar neste processo difícil, por vezes complicado”. Ainda segundo Fernandes e Abreu (2008), o objetivo de qualquer ambiente que utiliza a TI é explorar a capacidade plena destes sem comprometer o desempenho da estrutura. Finalmente, CAVALCANTI FILHO et al. (2011, p. 1) afirma que “uma correta definição de uma estrutura específica de Gestão de TI para instituições, de maneira geral, é fator preponderante para o cumprimento das metas estabelecidas no seu planejamento estratégico”. Segundo Cavalcanti (2009) a governança de TI está relacionada a melhores práticas envolvendo serviços de TI como: serviços de suporte, infra-estrutura e operações de Data-Center. A adoção das práticas de Gestão de TI na Administração Pública Federal (APF) pode assegurar a correta aplicação de recursos, promover a proteção de informações críticas e contribuir para que as organizações públicas atinjam seus objetivos institucionais (MPOG, 2013).

Gerenciar os riscos é um dos pricipais processos de busca e identificação dos riscos de uma organização de forma a analisar e propor estratégias para o tratamento, mitigação ou aceitação destes riscos. Para a norma ABNT ISO/IEC 27005 o risco de segurança pode ser medido pela função da combinação entre a probabilidade de um impacto e a consequência do mesmo (ABNT, 2011).

O alcance de tais objetivos da norma (ABNT, 2011) não depende necessariamente da implantação de hardware e software, mas muitas vezes da realização de processo de Gerenciamento de Risco de TI eficiente, no qual todos os riscos estejam mapeados e as estratégias de mitigação contempladas.

O Governo Federal brasileiro promove ações de segurança da informação nos órgãos da APF no intuito de desenvolver o compromisso com a proteção das informações, na tentativa de manter sua disponibilidade, integridade, confiabilidade e autenticidade. Um dos documentos que promove a existência de ações de segurança nos órgãos da APF é a Norma Complementar 03/IN01/DSIC/GSIPR (BRASIL, 2009)

Algumas Instituições Federais de Educação ainda não disponibilizam um documento sobre Gestão de Riscos em caráter institucionalizado (BRASIL, 2016). Diante desse cenário, torna-se importante investigar as práticas de gestão de riscos que essas instituições utilizam para a implantação desse documento, bem como identificar as causas que torna inviável a sua implantação.

Na pesquisa realizada, buscou-se estudar práticas, metodologias e modelos que pudessem ser utilizados como base para o desenvolvimento da prática de gestão de riscos para as instituições federais de educação, além disso foi realizado uma pesquisa de campo como forma de diagnosticar a situação destas instituições na área de gestão de riscos.

Este capítulo apresenta a visão geral do trabalho, estruturado nas seguintes seções:

- Motivação e relevância: esta seção apresenta o contexto, a motivação e a justificativa para realização deste trabalho;
- Problema de Pesquisa: esta seção aponta o direcionamento para o problema de pesquisa a ser analisado e respondido;
- Objetivos: esta seção destaca o objetivo geral do trabalho e também os objetivos específicos que devem ser alcançados como desdobramentos do objetivo geral;
- Metodologia do Trabalho: esta seção apresenta os métodos, procedimentos e técnicas utilizados para atingir os objetivos deste trabalho, bem como coletar e apreciar os dados;
- Delimitações do Trabalho: esta seção especifica o campo de atuação e as etapas de implementação do objeto da proposta deste trabalho.
- Estrutura do Trabalho: esta seção expõe como estão organizados os capítulos do trabalho como um todo.

1.1 MOTIVAÇÃO E RELEVÂNCIA

O TCU entendendo que a constatação dessa fiscalização era preocupante na área de segurança da informação, recomendou ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

As informações devem estar protegidas de acesso não autorizado e acessível para quem possui permissão de acesso. Conhecer e tratar os riscos vem deixando de

ser apenas uma necessidade técnica ou operacional e vem se transformando em uma questão de necessidade estratégica para as instituições (DANTAS, 2011).

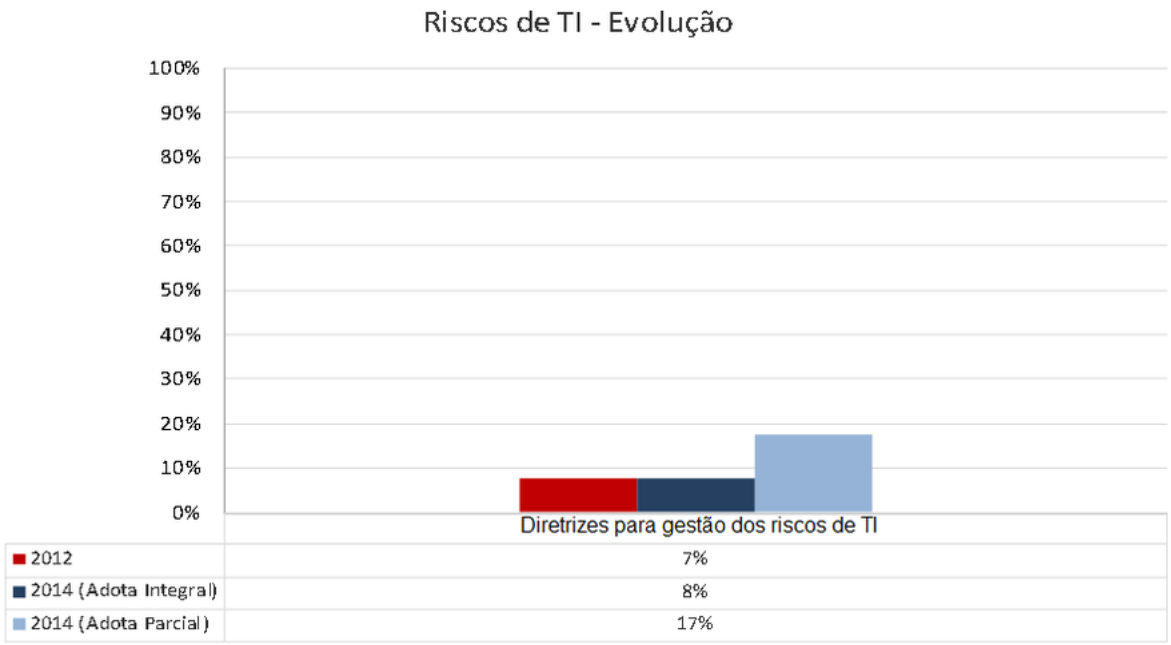
Conforme Brasil (2012) houve no ano de 2007 o primeiro levantamento de governança de TI nas instituições da Administração Pública Federal (APF). Este levantamento teve a participação de 255 instituições, que responderam um questionário com 39 perguntas e resultou o Acórdão2 1.603/2008-TCU-Plenário. O resultado dessa pesquisa foi preocupante e identificou-se a necessidade de realizar novos levantamentos visando o acompanhamento da situação de governança de tecnologia da informação (TI) nas instituições da Administração Pública Federal.

O relatório de 2014 demonstrou dados alarmantes e chamou atenção para um dado preocupante referente a situação da segurança da informação, em especial a análise e gestão de riscos. De acordo com relatório em 2010 apenas 17% das instituições públicas realizavam a análise de riscos, e em 2012 apesar do baixo índice apresentado, esse percentual ainda foi reduzido, obtendo-se apenas 10% das instituições realizando análise de riscos. O relatório evidencia o percentual de que 90% das instituições não realizam uma avaliação de riscos de segurança da informação.

No relatório realizado em 2014 somente 23% das organizações declararam dispor de política corporativa de gestão de riscos formalmente instituída (11% parcialmente e 12% integralmente), ou seja, a maioria dos participantes não dispõe de um instrumento necessário para direcionar as ações corporativas para avaliação dos riscos associados ao alcance dos resultados organizacionais. Isto é um indício de que as ações de segurança não são executadas de maneira sintonizada com a integridade das informações nas Instituições Federais. Isso porque, sem análise de riscos, não há como o gestor priorizar ações e investimentos com base em critérios claros e relacionados com os ativos (hardware e software) das instituições.

A figura 1.1 mostra os resultados obtidos em 2014:

Figura 1 – Evolução das práticas de governança relativas aos riscos de TI
Fonte: Acórdão 3.117/14 TCU/Plenário (Brasil, 2014)



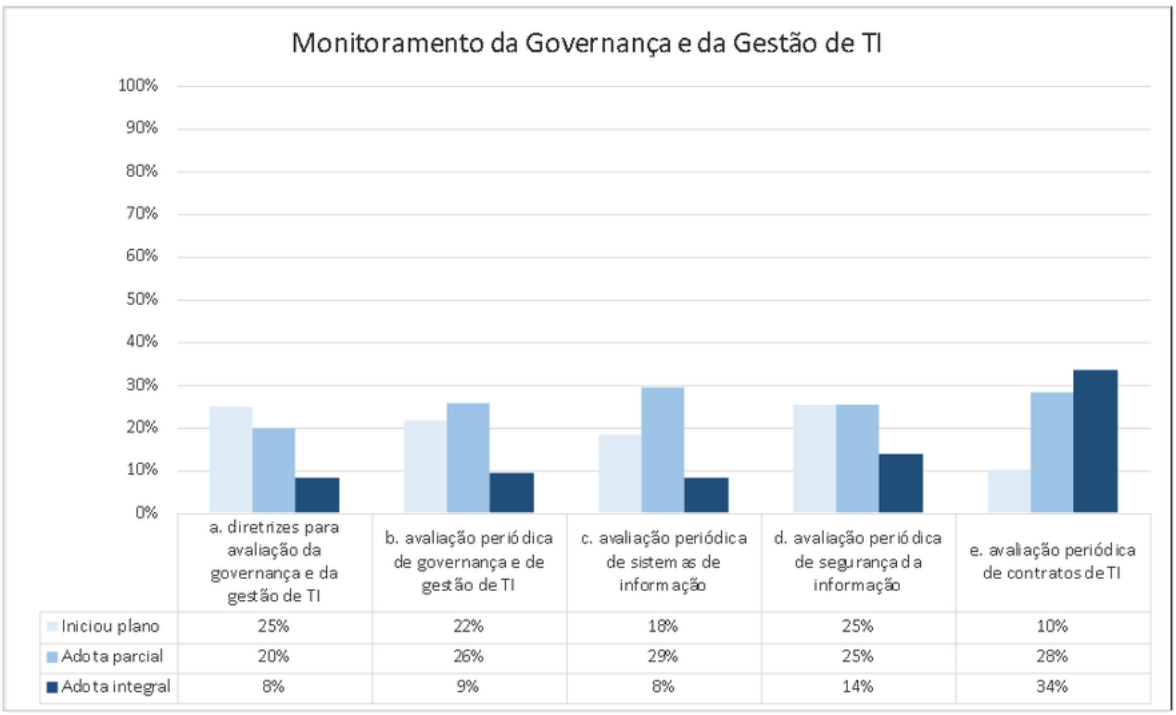
Observando a figura 1.2, verifica-se que 28% das organizações estabelecem diretrizes para o monitoramento da governança e da gestão de TI, mas apenas 8% adotam a prática de modo integral. Os 20% restantes, possivelmente, ainda não formalizaram a prática.

Importa ressaltar que a ausência de orientações claras da Alta administração sobre as ações e resultados esperados do processo de monitoramento da governança e da gestão de TI pode comprometer o acompanhamento do cumprimento dos planos e, por consequência, o alcance dos objetivos traçados.

No que se refere às avaliações periódicas de TI, que vão desde auditorias amplas sobre controles de governança e de gestão de TI até avaliações mais pontuais em contratos de serviços de TI, verifica-se que somente a prática de avaliar periodicamente contratos de TI conta com uma maioria de adoção. São 62% de organizações que declaram realizar esse tipo de avaliação, sendo 34% de modo integral e 28%, parcial. A adesão dos demais tipos de avaliação não chega a 40%, considerando a soma da adoção parcial com a integral: 35% para governança e gestão de TI, 37% para sistemas de informação e 39% para segurança da informação.

Além da inexistência de auditorias internas em muitas organizações do Poder Executivo, a falta de estrutura dessas unidades, especialmente a ausência de pessoal com conhecimento necessário para realizar esse tipo de trabalho, contribui significativamente para esse cenário de baixa adesão das práticas em tela.

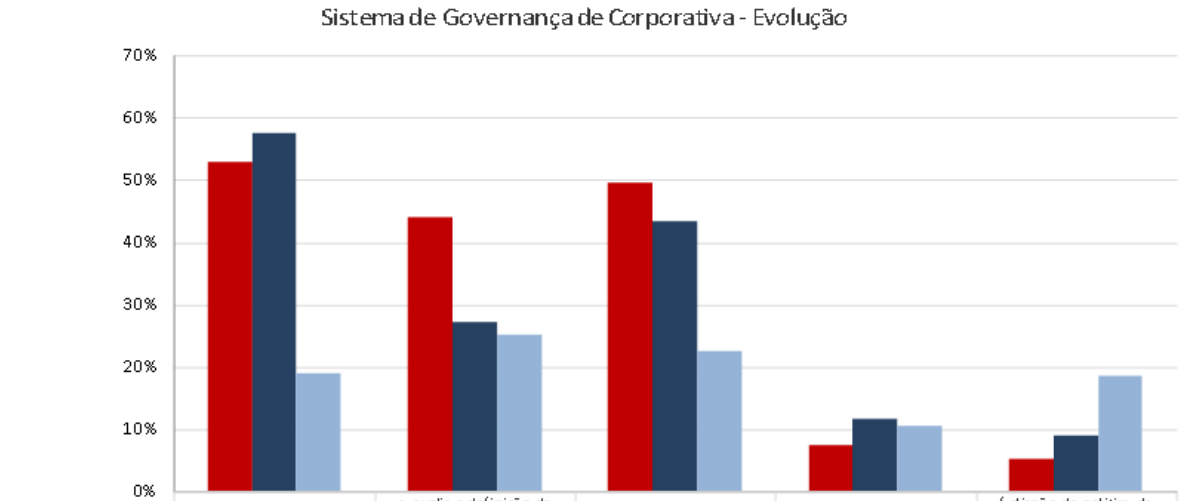
Figura 2 – Resultados apurados para as práticas sobre governança e gestão de TI
Fonte: Acórdão 3.117/14 TCU/Plenário (Brasil, 2014)



	a. diretrizes para avaliação da governança e da gestão de TI	b. avaliação periódica de governança e de gestão de TI	c. avaliação periódica de sistemas de informação	d. avaliação periódica de segurança da informação	e. avaliação periódica de contratos de TI
Iniciou plano	25%	22%	18%	25%	10%
Adota parcial	20%	26%	29%	25%	28%
Adota integral	8%	9%	8%	14%	34%

Observa-se, no item ‘e’ da figura 1.3, que somente 23% das organizações declararam dispor de política corporativa de gestão de riscos formalmente instituída (11% parcialmente e 12% integralmente), ou seja, a grande maioria dos participantes não dispõe de um instrumento necessário para direcionar as ações corporativas para avaliação dos riscos associados ao alcance dos resultados organizacionais.

Figura 3 – Práticas de sistema de governança
Fonte: Acórdão 3.117/14 TCU/Plenário (Brasil, 2014)



	b. dispõe de comitê de direção estratégica	c. avalia a definição de papéis e responsabilidades organizacionais	d. dispõe de código de ética	e. dispõe de política de gestão de riscos	f. dispõe de política de gestão de continuidade do negócio
2012	53%	44%	50%	7%	5%
2014 (Adota Integral)	58%	27%	43%	12%	9%
2014 (Adota Parcial)	19%	25%	23%	11%	19%

1.2 PROBLEMA DA PESQUISA

Conforme relatado pela pesquisa elaborada pelo TCU através dos últimos levantamentos de Governança de TI (BRASIL, 2010, 2012, 2014) onde se nota um baixo índice no tocante à Gestão de Riscos das Instituições Federais, surge o seguinte problema que norteia esta dissertação: Como mitigar o gerenciamento dos riscos de segurança da informação para atender os riscos que afetam os ativos de forma eficiente, a realidade das instituições federais de educação ?

1.3 OBJETIVOS

1.3.1 Geral

Definir um guia de melhores práticas para Mitigação de Riscos em Incidentes de TI nas Instituições Federais de Educação.

1.3.2 Específicos

Elaborar Revisão Sistemática sobre Gestão de Riscos em TI;

Verificar o cenário em que se encontra as IFE quanto à existência de Gestão de Riscos em TI;

Identificar as práticas de segurança da informação, utilizadas pelas IFE para implantação de Gestão de Riscos em Incidentes de TI;

Especificar melhores práticas em gestão de segurança da informação para implantação de Gestão de Riscos em Incidentes de TI;

Avaliar a proposta do guia de melhores práticas para Mitigação de Riscos em Incidentes em TI nas IFE.

1.4 METODOLOGIA

A respeito da técnica ou da metodologia que o pesquisador escolhe para o desenvolvimento de um trabalho, Oliveira Junior (2015), traz a seguinte ponderação:

Qualquer que seja a técnica ou o método escolhido pelo pesquisador, haverá limitações. Aliás, a própria escolha do objeto de estudo de pesquisa já requer um recorte da realidade a ser investigada. O importante é que tal escolha esteja cada vez mais respaldada em claras concepções do pesquisador sobre a natureza do objeto de estudo e o nível de análise e de descrição pretendido (OLIVEIRA JÚNIOR, 2015, p. 88).

A definição do instrumento metodológico em uma pesquisa está diretamente relacionada com o problema a ser estudado. Para Kauark et al. (2010, p. 53), “a metodologia é a explicação minuciosa, detalhada, rigorosa e exata de toda ação desenvolvida no método (caminho) do trabalho de pesquisa”. A figura 1.4 apresenta a metodologia utilizada na produção desse trabalho.

Figura 4 – Metodologia Aplicada
Fonte: Autor

Metodologia	Especificações
Método	Indutivo
Natureza	Aplicada
Abordagem	Quantitativa e Qualitativa
Objetivo	Descritiva e Exploratória
Procedimentos	Levantamento (através de questionário) Procedimentos bibliográficos (revisão sistemática) Documental
Área de concentração	Ciência da Computação – Segurança da Informação

1.4.1 Método

O método de pesquisa utilizado é do tipo indutivo que, partindo de dados particulares, suficientemente constatados, infere-se uma verdade geral ou universal. O conhecimento adquirido nesse tipo de pesquisa é fundamentado nas experiências vividas, não levando em conta princípios já preestabelecidos. Outro método utilizado para inferência dos dados será o procedimento estatístico (SILVIA e MENEZES, 2005).

1.4.2 Natureza

Do ponto de vista da natureza a pesquisa é do tipo pesquisa aplicada: pois busca gerar conhecimentos para aplicação prática e dirigidos a solução de problemas específicos envolvendo verdades e interesses locais (SILVIA e MENEZES, 2005)

1.4.3 Abordagem

Do ponto de vista da forma de abordagem do problema é do tipo pesquisa quantitativa: considera que tudo pode ser quantificável, o que significa traduzir em números as opiniões e informações para classificá-las e analisá-las. É usada quando se quer determinar o perfil de um grupo de pessoas, baseando-se em características que elas têm em comum. Requer o uso de recursos e de técnicas estatísticas (percentagem, média, moda, mediana, desvio-padrão, coeficiente de correlação, análise de regressão, etc.) (SILVIA e MENEZES, 2005). Neste trabalho procurou-se analisar e discutir os resultados dos questionários aplicados aos profissionais de TI das IFE.

1.4.4 Objetivo

Exploratória: A pesquisa exploratória encontra-se em fase preliminar, tendo como finalidade proporcionar mais informações sobre o assunto que se pretende investigar, possibilitando sua definição e seu delineamento. Foram utilizados os procedimentos da revisão sistemática e o levantamento da literatura em segurança da informação para proporcionar maior familiaridade com o assunto pesquisado.

Descritiva: Durante a pesquisa os fatos foram registrados, analisados, classificados, interpretados e comentados sem interferência do pesquisador. Segundo Gerhardt e Silveira (2009), para se desenvolver uma pesquisa, é indispensável selecionar o método e seus procedimentos a serem aplicados, podendo ser escolhido diferentes modalidades. Neste trabalho, foram utilizados três procedimentos: revisão bibliográfica (revisão sistemática da literatura), documental e levantamento de campo.

1.4.5 Procedimentos

Do ponto de vista dos procedimentos técnicos utilizados na pesquisa serão do tipo pesquisa bibliográfica, utilizando a revisão sistemática da literatura e levantamento de campo (SILVIA e MENEZES, 2005).

A revisão sistemática da literatura disponibiliza um resumo das evidências relacionadas a uma estratégia de intervenção específica, mediante a aplicação de métodos explícitos e sistematizados de busca, apreciação crítica e síntese da informação selecionada.

O levantamento de campo consistiu em questionários aplicados aos diretores de TI, ou especialistas na área de segurança da informação das IFE. Tal levantamento buscou a obtenção dos dados para diagnosticar a situação das IFE sobre a gestão de riscos.

1.4.6 Área de concentração

Para Santos (2002) a perspectiva da pesquisa representa qual o campo de interesse que foi focado na pesquisa. Este trabalho envolveu a áreas da concentração de Ciência da Computação e subárea de Segurança da Informação.

Ciência da Computação: neste caso, a pesquisa concentra-se nas bases tecnológicas para melhoria da segurança da informação com foco na gestão de riscos Isto compreende o valor da informação, do hardware, do software, das redes, dos dados e dos profissionais de TI para o negócio.

1.4.7 Delimitação

Uma vez estabelecida a questão-problema, é necessário estabelecer a seguinte delimitação:

O foco deste trabalho diz respeito a investigação das etapas de planejamento de práticas de gestão de riscos em TI. Como resultado um guia prático para sua implantação foi elaborado baseado nas melhores práticas apresentadas nos trabalhos relacionados. Não será considerada a criação das diretrizes, normas e procedimentos detalhados de uma gestão de riscos de TI, especificando o que este documento deve constituir e/ou como devem ser executadas nas IFEs.

1.5 ESTRUTURA DA DISSERTAÇÃO

O presente capítulo apresentou informações acerca da motivação e justificativa de pesquisa para esse trabalho bem como seus objetivos e procedimentos metodológicos adotados. O restante da dissertação está organizado da seguinte forma:

Capítulo 2: apresenta a revisão bibliográfica sobre Gestão de Riscos de TI de forma geral na APF e fundamenta o Gerenciamento de Riscos de TI e as melhores práticas de gestão de Riscos.

Capítulo 3: descreve o método de pesquisa, abordando as estratégias e procedimentos utilizados na condução desta pesquisa;

Capítulo 4: apresenta a proposta do Guia de melhores práticas para Mitigação de Riscos em Incidentes de TI, parte motivadora deste trabalho e avaliada por especialistas da área de TI.

Capítulo 5: são apresentadas as conclusões, principais contribuições e trabalhos futuros. Por fim, são apresentadas as seções que contêm a lista de referências utilizadas no desenvolvimento deste trabalho.

2 REVISÃO BIBLIOGRÁFICA

Este capítulo descreve todo o acervo que está envolvido no contexto da implantação de melhores práticas em órgão da APF, realizando uma revisão da literatura para obtenção do referencial teórico necessário, dando ênfase às principais áreas de estudo de segurança da informação. O capítulo está estruturado nas seguintes seções:

Segurança da informação: essa seção apresenta os conceitos iniciais e pilares que justificam a implantação de prática de gestão de riscos em TI;

Gerenciamento de Riscos em TI: essa sessão apresenta como é o procedimento do processo de gerenciamento de riscos em TI;

Melhores Práticas: essa seção apresenta as ferramentas de gestão de segurança da informação como orientação para implantação de práticas na implantação de gestão de riscos em TI;

Revisão Sistemática: descreve os passos utilizados para selecionar os principais trabalhos no “Estado da Arte”, identificados nas principais bases científicas;

Síntese do Capítulo: apresenta resumidamente a fundamentação delineada durante todo o capítulo.

2.1 SEGURANÇA DA INFORMAÇÃO

A informação é um recurso essencial para toda e qualquer organização, independente do seu porte e do segmento de atuação no mercado (FONTES, 2012, P.6). Para Castilho (2013), as organizações dependem incessantemente das informações para seus processos decisórios, crescimento corporativo e planejamento das atividades operacionais e estratégicas. Segundo Stoneburner (2002), a gestão de riscos é o processo de identificação dos riscos, avaliação de risco e tomada de medidas (tratamento do risco) para reduzir o risco a um nível aceitável. Para isso, alguns procedimentos são utilizados na tentativa de manter a disponibilidade, integridade, confiabilidade e autenticidade das informações, tais como: uma Política de Segurança da Informação, gestão de riscos e a própria gestão da segurança da informação.

O gerenciamento de riscos compreende as atividades coordenadas para dirigir e controlar a organização em relação aos riscos. O seu sistema de gerenciamento engloba o conjunto de elementos do sistema de gerenciamento da organização que incluem o planejamento estratégico, os tomadores de decisões e outros processos que lidam com riscos (ISO/IEC Guide 73:2002).

Dzazali e Hussein (2012) destacam que, organizações públicas enfrentam o desafio de proteger suas informações, considerando que são ambientes em que há

crescente complexidade, interconexões, incertezas e dependência da tecnologia, tendo ainda que realizar suas respectivas missões sem deixar de se submeter às normas e diretrizes provenientes dos órgãos centrais do governo. Entretanto, é necessário que medidas sejam tomadas para que tais informações sejam mantidas seguras e invioláveis.

Para este trabalho foi adotado o conceito de segurança da informação, o qual Castilho (2013, p.55) define como sendo, "o processo de proteger os ativos contra os diversos tipos de ameaças para garantir continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades do negócio". Para Quintella e Branco (2013, p. 2), segurança da informação diz respeito à "proteção da informação contra ameaças que possam valer-se das vulnerabilidades deste ativo, preservando suas propriedades fundamentais: disponibilidade, integridade, confidencialidade e autenticidade".

Conforme relatam Alves e Moreira (2012), a segurança da informação não se restringe apenas a dados, papéis, sistemas ou meio de armazenamento. É necessário que as organizações estabeleçam, internamente, normas e diretrizes que controlem a maneira de acessos às informações, bem como a forma de disseminá-las.

Segurança da informação, além de sua compreensão, é de fato a proteção da informação contra o uso, o acesso não autorizado e a negação de serviço a quem não é permitido acessá-la. Safa e Ismail (2013) dizem que, se as informações de uma organização forem violadas, não só geram custos adicionais para as organizações, como também afetam significativamente sua reputação. Por isso, as organizações necessitam de procedimentos, diretrizes e políticas que possibilitem nortear as ações do funcionalismo organizacional quanto em manter o mínimo de segurança ao acesso das suas informações armazenadas em sistemas, mídias ou impressas em papel.

A segurança da informação está, portanto, associada a leis, normas, regulamentos e padrões internacionais que prescrevem práticas tidas como necessárias (ALBUQUERQUE JÚNIOR e SANTOS, 2014). Essas ações podem ser determinantes na implantação, definição ou estabelecimento de papéis e responsabilidades, estratégias, estruturas organizacionais, tecnologias, políticas e outras medidas de segurança da informação. Castilho (2013, p. 55) comenta que "a segurança da informação é obtida a partir da implantação de um conjunto de políticas, processos, procedimentos e estruturas organizacionais de hardware e software". Esse mesmo conceito é fortalecido em práticas de gestão de segurança da informação, tais como a ISO/IEC 27001 e a ISO/IEC 27002.

Consentindo com tais informações, é importante que as instituições desenvolvam e estabeleçam um processo de segurança da informação, tendo por objetivo permitir e possibilitar o seu funcionamento adequado, identificando os ativos que se pretende

proteger, detectando assim os recursos e padrões necessários para formalizar o processo de segurança da informação.

A segurança da informação é de vital importância para que as instituições protejam seus ativos das vulnerabilidades e dos ataques inesperados, possibilitando que cumpram sua missão e seu planejamento estratégico (AL-HAMDANI e DIXIE, 2009). Para implantar e manter um processo de segurança da informação a Norma NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Código de prática para a gestão da segurança da informação, traz a seguinte orientação:

Convém que a direção estabeleça uma clara orientação, alinhada às diretrizes de gestão de riscos e que demonstre apoio e comprometimento com a instituição por meio da publicação e manutenção de uma política de segurança da informação para toda a organização (ABNT, 2013b, p.8).

2.1.1 Risco

De acordo com D'ANDREA (2011; p. 51) "o risco como oportunidade está centrado no investimento e tem base em iniciativas estratégicas. Quanto maior for o risco, maior o potencial de retorno, e, paralelamente, maior pode ser o potencial de perda." Nesta visão, onde o risco é compreendido como uma oportunidade, ações pró-ativas e ofensivas (não defensivas) são adotadas pelos gestores, com o propósito de que sejam obtidos resultados positivos.

O risco como ameaça, escopo deste trabalho, refere-se à abordagem mais tradicional, na qual a preocupação está atrelada à ocorrência de efeitos negativos como por exemplo perda financeira, fraude, roubo, comprometimento da imagem e reputação, infração legal, falhas tecnológicas, dentre outros. Nas situações em que o risco é visualizado como uma ameaça, os gestores atuam fortemente de maneira preventiva, a fim de minimizar o impacto causado para a organização caso o risco se materialize.

Segundo o levantamento de Governança de TI 2014 do TCU, constatou que o uso cada vez mais crescente da TI na execução dos processos organizacionais, em especial dos finalísticos, vem acompanhado do aumento do risco de segurança da informação, requerendo maior atenção da APF no estabelecimento dos processos e dos controles voltados à proteção das informações.

A ISO 31000 define o risco como sendo o efeito da incerteza nos objetivos e nesta definição conceitua a incerteza como estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

A IEC 27002 define risco como a possibilidade de um ativo estar sujeito a vulnerabilidades e incidentes (ameaças explorando essas vulnerabilidades), comprometendo a continuidade das atividades de uma organização (ABNT, 2013).

Risco é o impacto negativo da ação de uma vulnerabilidade, considerando tanto a probabilidade e o impacto da ocorrência, isto é, risco é a função que relaciona a probabilidade de uma determinada ameaça explorar uma vulnerabilidade em potencial e o impacto resultante desse evento adverso sobre a organização (STONEBURNER, 2002).

2.1.2 Ameaça

Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização (ISO/IEC, 2004). Agentes ou condições que causam incidentes que comprometem as informações e seus ativos, por meio de exploração de vulnerabilidades, o que provoca perdas de confiabilidade, integridade e disponibilidade, e, onsequentemente, causando impactos aos negócios de uma organização (SEMOLA, 2013).

Segundo GUIMARAES et al. (2009, p. 15) uma ameaça relacionada a um ataque de segurança pode ter a origem interna ou externa, comprometendo a integridade e privacidade das informaçoes estratégicas de uma empresa.

Ameaças são expectativas de acontecimento acidental ou proposital, causado por agente, o qual pode afetar um ambiente, sistema ou ativo de informação (BEAL, 2005). O conceito de ameaça pode ser definido como uma atividade deliberada, ou não intencional, com o potencial de causar danos aos ativos.

As ameaças podem ser classificadas em três grandes grupos: ameaças humanas, ameaças não humanas (ou ambientais) e desastres naturais. As ameaças humanas podem sofrer um segundo nível de segregação, intencional ou não intencional, e estão diretamente relacionadas às ações realizadas pelos indivíduos. Na categoria de ameaça humana intencional enquadram-se os “hackers”, “crackers” e funcionários descontentes. Em contrapartida os funcionários com poucos conhecimentos sobre aspectos tecnológicos podem ser classificados como ameaça humana não intencional.

Conforme o INFORMATION SECURITY FORUM (2001; p. 06), são consideradas ameaças “os meios pelos quais a confidencialidade, integridade e disponibilidade da informação podem ser comprometidas.” Nessa mesma abordagem, são consideradas categorias de ameaça: mau funcionamento de hardware e software; perda de serviço,

equipamento ou recursos; conseqüências não previstas durante um processo de gerenciamento de mudanças; erro humano e violação no acesso.

De acordo com WHITMAN (2003; p. 134), existem 9 categorias de ameaças, as quais estão relacionadas no quadro 2.1:

Quadro 1 – Exemplos de Ameaças
Fonte: WHITMAN (2003)

Ameaça	**Exemplo**
Erro humano ou falha	Acidentes, erros cometidos por funcionários
Comprometimento de propriedade intelectual	Pirataria, violação de "copyright"
Atos deliberados de espionagem	Acesso não autorizado a dados
Atos deliberados de sabotagem ou vandalismo	Destruição dos sistemas ou informação
Atos deliberados de roubo	Confisco ilegal de equipamentos ou informações
Ataques deliberados de software	Vírus, "worms", macros, negação de serviço
Falhas técnicas ou erros de hardware	Falha de equipamento
Falhas técnicas ou erros de software	"Bugs", problemas de codificação
Obsolescência tecnológica	Tecnologia antiquada ou em desuso

Em geral, as ameaças humanas sempre são materializadas a partir de uma motivação. No quadro 2.2 , STONEBURNER (2002; p. 13), exemplifica este conceito:

Quadro 2 – Motivação das ameaças
Fonte: STONEBURNER (2002)

Fonte de ameaça	**Motivação**	**Ações da ameaça**
"Hacker", "cracker"	Desafio Ego Rebeldia	Engenharia social Intrusão nos sistemas e interrupções Acesso não autorizado ao sistema
Terrorismo	Destruição Vingança	Penetração no sistema Negação de serviço
Espionagem industrial	Obtenção de vantagem competitiva Espionagem econômica	Roubo de informação Engenharia social

2.1.3 Vulnerabilidade

Fragilidade de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças (ABNT, 2013).

Fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque (BEAL, 2005).

Fragilidades presentes ou associadas a ativos de informação, que, ao serem exploradas, permitem a ocorrência de incidente na segurança da informação (SEMOLA, 2013).

As vulnerabilidades são definidas como circunstâncias que aumentam a probabilidade de materialização de uma ameaça, contribuindo para que ela ocorra com maior freqüência, maior impacto, ou ambos concomitantemente. As vulnerabilidades podem ser decorrentes de fraquezas existentes nos controles de segurança (sejam estes procedimentos, controles tecnológicos ou físicos), ou originadas por situações especiais. Muitas vezes o conceito de vulnerabilidade é interpretado como ausência de segurança. As vulnerabilidades contribuem para o risco do ambiente, pois colaboram para que a ameaça se concretize.

2.1.4 Impacto

O impacto refere-se ao dano causado no ambiente tecnológico ou ao negócio devido à exploração de uma vulnerabilidade por uma ameaça. Esse impacto deve ser analisado considerando o quanto as propriedades da informação como a confidencialidade, integridade e disponibilidade foram afetadas. Durante uma análise de risco, outros tipos de impacto também são considerados, dentre eles o financeiro e de imagem da organização. O impacto causado pela exploração de uma vulnerabilidade deve ser analisado quantitativamente e qualitativamente.

2.1.5 Ativos

Muitas metodologias de análise de risco iniciam o processo pela identificação e classificação dos ativos. O termo ativo possui um significado bastante amplo, e pode englobar recursos tangíveis e intangíveis. Dentre os recursos tangíveis encontramos hardware, documentos impressos, mídias magnéticas, etc. Em relação aos recursos intangíveis os principais são os dados e informações, embora o aspecto software e a imagem / reputação da organização também sejam considerados como ativos. Cabe destacar que alguns autores também classificam as pessoas como ativos. Os ativos

são os principais afetados por uma ameaça. Em função disso, os ativos críticos da organização precisam ser corretamente identificados, e as respectivas vulnerabilidades mapeadas, permitindo assim que contramedidas sejam adotadas evitando que as vulnerabilidades conhecidas sejam exploradas pelas ameaças.

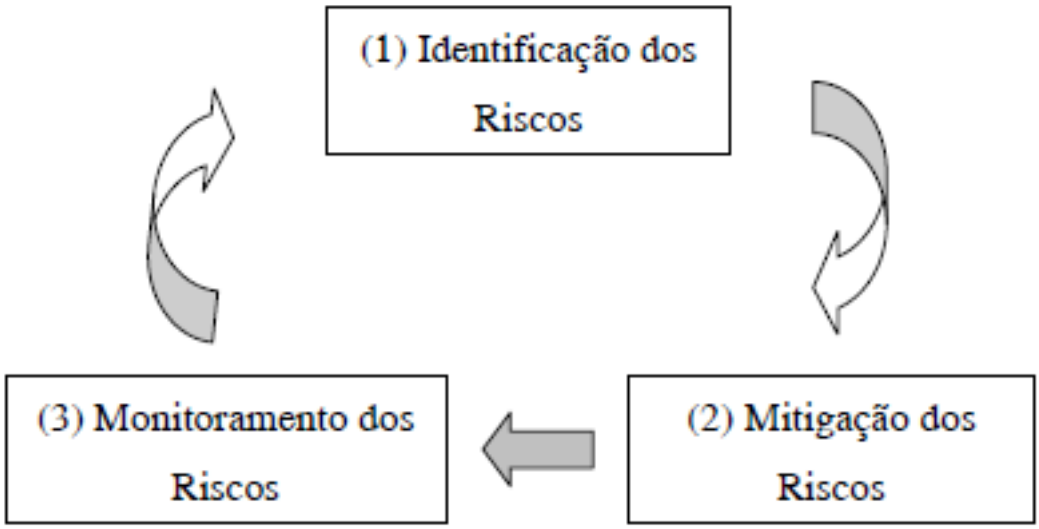
2.2 GERENCIAMENTO DE RISCOS EM TI

Um dos propósitos desta dissertação, além de apresentar uma análise comparativa de metodologias de Gerenciamento de Risco de TI comumente empregadas, é apresentar uma visão geral de quais etapas compõem o processo de Gerenciamento de Risco de TI, independente da metodologia.

Existem diferentes modelos e métodos para condução do processo de Gerenciamento de Risco de TI, e a extensão da análise e os recursos empregados podem variar dependendo do escopo do levantamento e da disponibilidade de dados e informações confiáveis. Adicionalmente, a disponibilidade de dados pode afetar a forma como o risco é mensurado, ou seja, a adoção de uma abordagem quantitativa ou qualitativa. Uma abordagem quantitativa geralmente estima o custo monetário do risco e das técnicas de minimização do mesmo baseado (1) na probabilidade que um evento prejudicial ocorra, (2) no custo de potenciais perdas, (3) no custo das ações de mitigação que podem ser adotadas. Quando dados confiáveis referentes à probabilidade de materialização da ameaça e custos não estão disponíveis, somente a abordagem qualitativa poderá ser adotada, e neste caso, os riscos são definidos de modo mais subjetivo, em geral utilizando escalas como alto, médio e baixo. Assim, o processo de avaliação de riscos dependerá fortemente da experiência prévia do profissional que está conduzindo o processo de análise de riscos.

Os riscos devem ser continuamente monitorados visto que as ameaças, vulnerabilidades e os próprios ativos alteram-se com o passar do tempo. Assim, novos riscos virão à tona e outros já mitigados podem se tornar uma preocupação. Dessa forma, o processo de Gerenciamento de Risco de TI é algo contínuo e evolutivo. A Figura 2.1 apresentada a continuidade desse ciclo.

Figura 5 – Ciclo de Gerenciamento de Risco de TI
Fonte: adaptado de WHITMAN (2003)



2.2.1 Identificação dos riscos

A identificação ou avaliação de riscos é a primeira etapa do processo de Gerenciamento de Risco de TI. Essa etapa visa mapear todas as potenciais ameaças aos quais os ativos estão suscetíveis, bem como as vulnerabilidades que esses possuem. As atividades como: avaliação da probabilidade de materialização das ameaças e estimativa dos impactos causados também são contempladas nessa etapa do processo. De acordo com ISO IEC 27005 (ABNT, 2011), os controles são empregados com uma das seguintes finalidades: detecção, proteção, prevenção, limitação, correção, recuperação, monitoramento e conscientização. A seleção adequada dos controles é essencial para assegurar que os ativos estejam adequadamente protegidos. Dentre os diversos tipos de controles existentes, podemos mencionar:

- firewalls de rede;
- criptografia;
- software antivírus;
- backups;
- mecanismos de controle de acesso;
- geradores de energia;
- assinatura digital; e procedimentos operacionais, etc.

2.2.2 Avaliação dos riscos

De acordo com COHEN (2003; p.10) a avaliação das ameaças deverá ocorrer conforme a periodicidade apresentada no quadro 2.3. Nesta tabela também são apresentados quais níveis hierárquicos dentro da organização deverão ser notificados quando da identificação de novas ameaças e com qual periodicidade.

Quadro 3 – Periodicidade para avaliação dos riscos
Fonte: COHEN(2003)

	Impacto		
Ameaça	**Baixo**	**Médio**	**Alto**
Baixa probabilidade	Anualmente. Gerência de nível médio.	Ciclo de revisão 6 meses. Alta administração atualizada anualmente.	Altas conseqüências em geral são originadas por altas ameaças. De qualquer modo a análise deve ser contínua. Alta administração atualizada mensalmente.
Média probabilidade	9 – 12 meses. Gerência de nível médio.	Ciclo de revisão 3-9 meses. Alta administração atualizada trimestralmente.	Contínuo. Alta administração atualizada mensalmente.
Alta probabilidade	6 meses. Gerência de nível médio.	Ciclo de revisão 3-6 meses. Alta administração Atualizada trimestralmente.	Contínuo. Alta administração atualizada mensalmente.

De acordo com WHITMAN (2003; p. 154), “risco é a probabilidade de ocorrência de uma vulnerabilidade, multiplicado pelo valor do ativo de informação, menos a porcentagem de risco mitigado pelos controles atuais, mais a incerteza do atual conhecimento da vulnerabilidade”.

2.2.3 Probabilidade de Risco

A probabilidade é o fator de incerteza envolvido no risco. É o índice que indica as chances de uma vulnerabilidade ser explorada, com sucesso, por uma ameaça. De acordo com STONEBURNER (2002;p.21), para derivar um índice que represente a probabilidade que uma potencial vulnerabilidade seja explorada por uma ameaça, os seguintes fatores devem ser considerados:

- origem e motivação da ameaça;

- natureza da vulnerabilidade; e existência e efetividade dos controles empregados.

A probabilidade de que uma potencial vulnerabilidade possa ser explorada por uma dada ameaça pode ser classificada em: alto, médio ou baixo. O quadro 2.4 descreve cada um dos critérios:

Quadro 4 – Classificação de níveis de probabilidade de concretização de ameaças
Fonte: STONEBURNER (2002)

Nível de probabilidade	**Descrição**
Alta	A origem da ameaça é altamente motivada e suficientemente capaz de ser exercida, e os controles empregados para evitar que a vulnerabilidade seja explorada são ineficientes. O evento é esperado e quase certo de que aconteça.
Médio	A origem da ameaça é motivada e capaz, mas os controles adotados podem impedir que a vulnerabilidade seja explorada. O evento poderá ocorrer alguma vez.
Baixo	A origem da ameaça é falha ou incapaz, ou os controles adotados para prevenir ou impedir sua ocorrência são eficazes. O evento poderá ocorrer em circunstâncias excepcionais.

A publicação especial do STONEBURNER (2002; p. 30) sugere que sejam atribuídos os seguintes valores para a probabilidade: 1.0 para Alto, 0.5 para Médio e 0.1 para Baixo.

Exemplificando, a probabilidade do recebimento de um e-mail contendo vírus deveria ser classificada com 1.0; enquanto que a probabilidade de um meteoro cair no setor de TI, tende a 0.1. Nessa classificação não existe a possibilidade de adotar

o valor 0, visto que uma vulnerabilidade com probabilidade zero de ocorrência não deve ser considerada durante o processo de análise de risco. Os pesos atribuídos às probabilidades são utilizados posteriormente no cálculo do nível de risco. Embora sejam sugeridos os valores acima, cabe ao responsável pela análise de risco definir os valores que reflitam o contexto de segurança da organização.

2.2.4 Tipos de Abordagens na probalidade de riscos

Há dois métodos fundamentalmente diferentes aplicados à mensuração do impacto: a análise qualitativa e a análise quantitativa.

Abordagem Qualitativa: na análise qualitativa todas as avaliações aplicadas são subjetivas por natureza, assim esta abordagem não provê unidades de medida que permitam quantificar a magnitude dos impactos, e conseqüentemente a análise de custo-benefício de qualquer controle é dificultada. Nesta abordagem, a análise final do risco é classificada em categorias definidas pelo responsável pela análise, as quais podem variar entre alto, médio e baixo de acordo com o quadro 2.5.

Quadro 5 – Magnitude de impacto
Fonte: WHITMAN (2003)

Magnitude do impacto	**Definição**
Alto	A exploração da vulnerabilidade pode resultar na (a) perda dos principais ativos / recursos da organização; (b) pode violar significativamente a reputação da organização, ou impedir que ela alcance seus objetivos; (c) acarretar em perdas humanas (morte) ou sérias lesões; (d) comprometer as operações de negócio com significantes conseqüências negativas aos clientes, processos ou sistemas.
Médio	A exploração da vulnerabilidade pode resultar em (a) perda de ativos ou recursos sofisticados; (b) prejudicar a reputação / interesses da organização, ou impedir que ela cumpra sua missão. É esperado que o evento acarrete em uma perda financeira intermediária, ou resulte em interrupções no negócio com conseqüências negativas.
Baixo	A exploração da vulnerabilidade pode resultar na (a) perda de ativos tangíveis ou pode (b) afetar visivelmente a missão, reputação ou interesse da organização. Não é esperado que o evento resulte em perdas financeiras significativas ou outros impactos duradouros ao negócio. Quaisquer problemas ocorridos serão facilmente contidos.

Abordagem Quantitativa: a maior vantagem da análise quantitativa do impacto é que ela provém medida da magnitude do mesmo, a qual pode ser utilizada nas análises de custo benefício dos controles. Uma desvantagem é que, dependendo da unidade de medida adotada para expressar esta análise, ela pode não ser tão clara, necessitando que o resultado seja interpretado de maneira qualitativa. Alguns indicadores utilizados para mensurar o impacto quantitativamente incluem:

- freqüência de exploração da vulnerabilidade por uma determinada ameaça, em um determinado período de tempo;

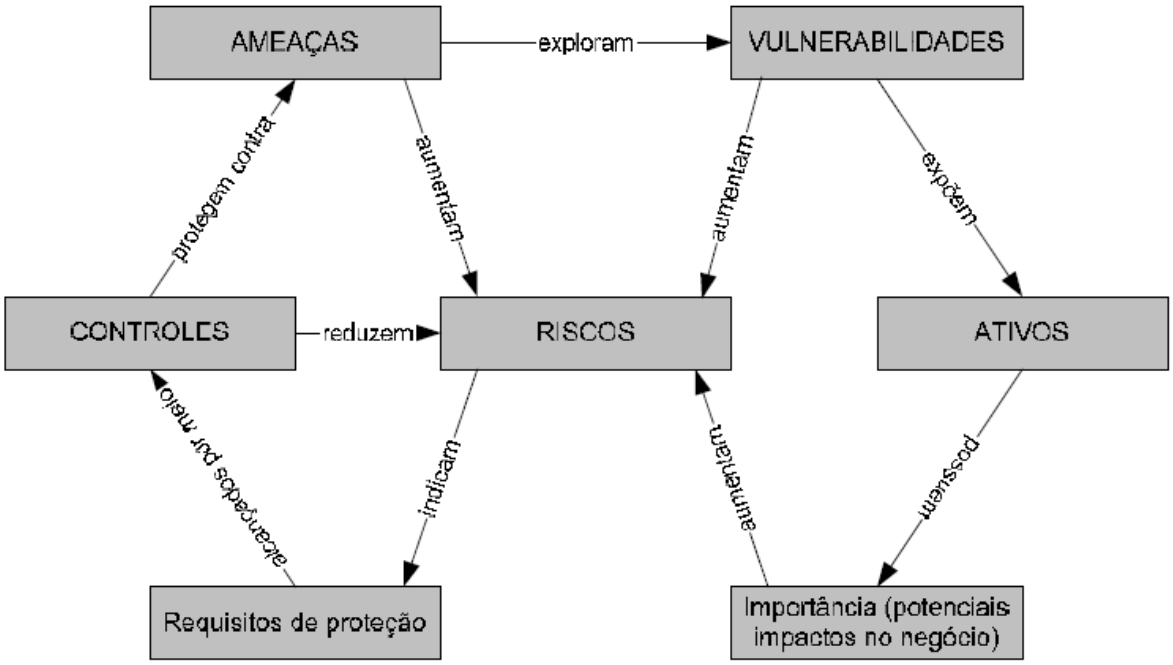
- custo decorrente da exploração da vulnerabilidade pela ameaça;

- valor do ativo;

2.2.5 Mitigação dos riscos

Uma vez identificados os riscos aos quais os ativos estão suscetíveis, inicia-se a etapa de mitigação dos riscos. A mitigação dos riscos consiste na seleção, priorização, avaliação e implementação de controles de segurança cuja finalidade é reduzir os riscos a um nível aceitável. A eliminação completa dos riscos geralmente é inviável, devido ao alto custo envolvido nesse processo. Assim, cabe à alta administração e gerências de nível médio decidir sobre qual etapa de mitigação consiste na seleção de estratégias a serem adotadas para eliminação ou minimização dos riscos, exemplificados na figura 2.2. Durante a etapa de mitigação aspectos financeiros são considerados, visto que os recursos empregados na mitigação dos riscos não podem ser superiores à possível perda financeira que o risco acarretaria, caso a ameaça se materializasse.

Figura 6 – Processo de Mitigação dos Riscos
Fonte: adaptado de WHITMAN (2003)



2.2.5.1 Controles para Mitigação de Riscos

Há somente três abordagens possíveis para mitigação dos riscos: evitar o risco, controlar, reduzir ou transferir o risco.Abaixo segue o detalhamento de cada uma das abordagens:

Evitar o risco: consiste em impedir a exploração de uma determinada vulnerabilidade. Em geral esta é uma das abordagens preferidas, visto que é mais fácil evitar o risco do que lidar com ele depois de materializado. A ação de evitar o risco é obtida através da contenção das ameaças, da remoção das vulnerabilidades nos ativos, e por meio da aplicação dos controles necessários, o que inclui implementação ou modificação de procedimentos ou tecnologia.

Controlar o impacto do risco: é uma das abordagens mais comuns no tratamento dos riscos. Neste caso ocorre o reconhecimento do risco e a adoção de mecanismos para monitorá-lo e gerenciá-lo. Neste contexto de redução do impacto causado pelo risco estão inseridos os Planos de Continuidade de Negócios, o Plano de Recuperação de Desastres, e o Plano de Resposta a Incidentes. A adoção de cada uma dessas estratégias depende da opercaionalidade da organização de detectar e responder ao ataque o mais rápido possível.

De acordo com WHITMAN (2003; p. 161) podemos definir, de modo sucinto:
- Plano de Resposta a Incidentes: ações que as organizações adotam durante os ataques. São aplicados no momento do incidente.

- Plano de Recuperação de Desastres: estratégias para limitar as perdas antes e durante os desastres, instruções passo a passo para retomar a normalidade. São medidas adotadas a curto prazo.
- Plano de Continuidade de Negócios: estratégia adotada para assegurar a continuidade dos negócios da organização, quando o desastre ocorrido tomou grandes proporções. Em geral requer re-alocação das operações.

Transferir o risco: é uma das opções adotadas pelas empresas quando a adoção de controles para minimizar o risco não é possível. Neste caso, a opção comumente adotada pelas empresas é a aquisição de seguros. Assim, caso o risco se materialize, as perdas ocorridas são recompensadas por um terceiro.

Aceitar o risco: consiste no reconhecimento da existência do risco e na decisão de aceitar as possíveis conseqüências caso o risco se materialize. A ação de aceitação do risco pode ser uma decisão de negócio consciente ou inconsciente.

2.2.5.2 Controles Preventivos, Corretivos e Detectivos

Os controles podem ser classificados de diferentes formas. Uma delas é classificá-los de acordo com sua natureza, por exemplo, controles gerenciais, operacionais e técnicos. Outro método é efetuar a categorização por área funcional: sistemas aplicativos, telecomunicações, redes, desenvolvimento de sistemas, operações, etc. Uma terceira abordagem é classificá-los de acordo com o objetivo ou propósito a que se destinam; neste caso a divisão seria: preventivos, detectivos ou corretivos.

Controles preventivos:

Compreendem todas as metodologias, práticas, ferramentas, tecnologias, para aprimorar a confiabilidade dos recursos. Tem por função impedir ou minimizar que eventos indesejáveis ocorram, evitando a incidência de erros, omissões ou ações maliciosas, e principalmente impedindo que os riscos se materializem. Em geral, a adoção de controles preventivos é melhor quando comparados aos detectivos ou corretivos. Cabe destacar que nem sempre é possível a implementação de controles preventivos; além disso, muitas vezes eles não são economicamente viáveis. São exemplos de controles preventivos: segregação de funções, mecanismos de controle de acesso físico ou lógico, software antivírus, conscientização, classificação das informações, firewall; dentre outros.

Controles corretivos:

Compreendem informações, procedimentos e instruções que tem por funções: minimizar o impacto causado pela ameaça; corrigir problemas identificados pelos controles detectivos; identificar a causa dos problemas; corrigir erros; e modificar procedimentos para evitar a ocorrência de problemas futuros. Exemplo de controle corretivo: plano de contingência.

Controles detectivos:

Controles que detectam que um erro, omissão ou ação maliciosa ocorreu. Os controles detectivos fornecem a avaliação de um resultado sobre a segurança do ambiente e se os controles preventivos atingiram seus objetivos. Controles detectivos incluem técnicas manuais e automatizadas e metodologias para medição da efetividade dos controles preventivos. São exemplos de controles detectivos: trilhas de auditoria, alarmes, IDS – “Intrusion Detection Systems”, câmeras de monitoramento, dentre outros.

2.3 MELHORES PRÁTICAS

Estudos e casos de sucesso em nível nacional e internacional, mostram que a implantação de boas práticas nas organizações pode reduzir os riscos, ameaças e vulnerabilidades nos sistemas de informação (SUSSY, 2015). Quintella e Branco (2013, p. 3) concordam que a "proteção adequada da informação pode ser mais facilmente gerida se forem usadas as 'melhores práticas'. Nascimento (2012, p. 69) corrobora o entendimento que: "todo o universo de segurança da informação é amparado por normas e melhores práticas vigentes no mercado". Tais normas são entendidas como regras de conduta que são utilizadas para dar suporte ao direcionamento de determinadas ações (ALVES e MOREIRA, 2012), descrevendo com detalhes quais passos devem ser seguidos na elaboração de uma política.

Segundo Al-Hamdani e Dixie (2009), muitas instituições de ensino têm adotado melhores práticas para implementar a segurança da informação em seus campi, outras têm adotado padrões internacionais como a ISO e outras instituições têm adotado padrões de órgãos nacionais.

Entretanto, organizações que procuram proteger a informação e os outros ativos associados, "dispõem de uma série de medidas de Segurança da Informação preconizadas por normas e modelos internacionais amplamente aceitos por profissionais e organizações de todo o mundo" (ALBUQUERQUE JÚNIOR e SANTOS, 2015, p. 2). Nesse sentido, é imprescindível considerar que a "Proteção adequada da informação pode ser mais facilmente gerida se forem usadas as "melhores práticas", que são um conjunto de procedimentos constituídos por padrões e recomendações de institutos de tecnologia (QUINTELLA e BRANCO, 2013, p. 3).

2.3.1 ISO/IEC 27002:2013

A família ISO/IEC 27000 é um conjunto de normas para regular os aspectos da segurança da informação, podendo ser aplicadas em qualquer organização. Dentre essa família, existe a NBR ISO/IEC 27002, a qual Castilho (2013) define como uma norma de sistemas de gestão da segurança da informação onde se define código de prática para gestão da segurança da informação e orienta quais os elementos são essenciais para promover uma adequada segurança da informação. Essa norma é, solidariamente, considerada e aceita por Huang, Zavarsky e Ruhl (2009), como a melhor prática para a gestão de segurança da informação.

A NBR ISO/IEC 27002 pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes e princípios gerais sobre metas geralmente aceitas

para a gestão da segurança da informação (MONTEIRO, 2009). Alves e Moreira (2012) relatam que a NBR ISO/IEC 27002 trata de diversas ações que ajudam na elaboração de uma Política de Segurança da Informação, conforme descreve quais passos seguir na elaboração da política de segurança da informação, descrevendo em detalhes quais os principais pontos a serem observados, quais riscos, ameaças e vulnerabilidades, como tratar cada evento ou incidente da informação.

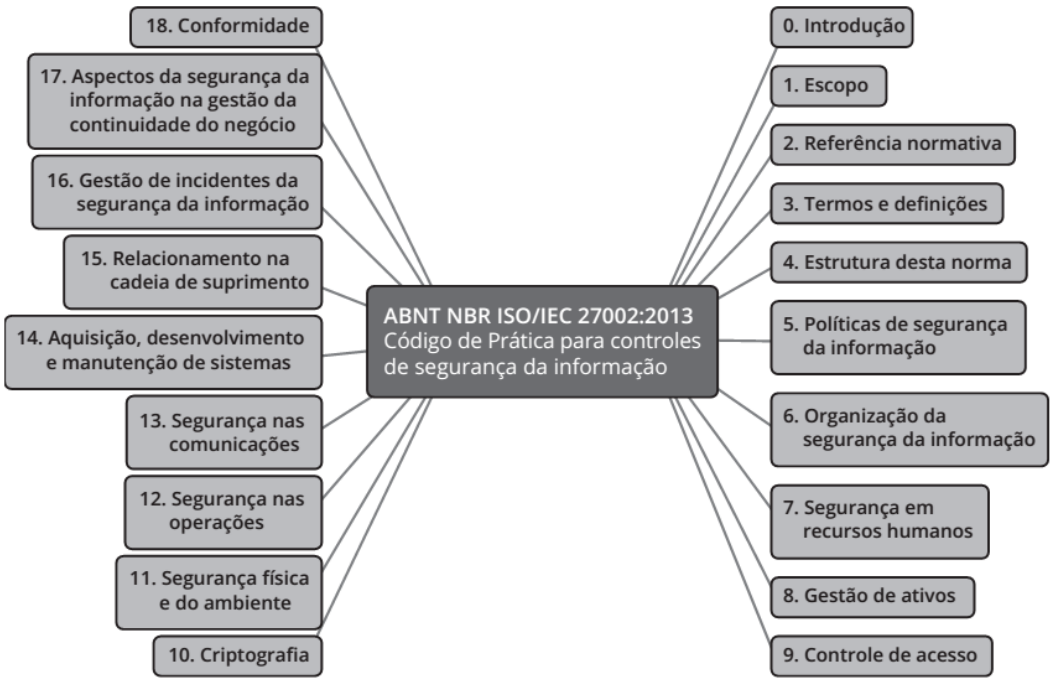
A NBR ISO/IEC 27002 tem como objetivo:

Fornecer diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implantação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização (ABNT, 2013a, p. 1).

Fontes (2011; 2012) e ISACA (2012c), ressaltam que o próprio *framework* COBIT, concernente ao assunto segurança da informação aconselha ao usuário obter informações mais detalhadas sobre as práticas e controles de segurança, consultando a NBR ISO/IEC 27002.

A norma está estruturada com 18 seções de controles de segurança da informação de conforme a figura 2.3. Cada seção, definindo os controles de segurança da informação, contém um ou mais objetivos de controle. “A ordem em que se encontram as seções não implica nem significa o seu grau de importância” (ABNT, 2013a, p. 1).

Figura 7 – Estrutura da NBR ISO/IEC 27002:2013
Fonte: Gestão da Segurança da Informação (COELHO et al., 2014).



2.3.2 Osstmm

É a metodologia que mantém um padrão internacional para testes de segurança, mantida pela ISECOM (Institute for Security and Open Methodologies) pois suas definições são consituídas a partir do escopo, que representa todo o ambiente de segurança operacional possível para qualquer interação com qualquer ativo. Este escopo é composto por três classes: COMSEC (Communications Security Channel), PHYSSEC (Physical Security Channel) e SPECSEC (Spectrum Security Channel). Essas classes são divididas em cinco canais :

1) Humano: trata todos os elementos humanos de comunicação onde a interação pode ser tanto física como psicológica.

2) Físico: relaciona todos os elementos tangíveis de segurança de natureza física ou não-eletrônica. Trata os elementos onde a interação requer esforços físicos ou uma energia de transmissão para manipular.

3) Wireless: trata todas as comunicações eletrônicas, sinais e frequências que tem um espectro eletromagnético conhecido.

4) Telecomunicações: compreende todas as redes de telecomunicações, digitais ou analógicas, onde as interações ocorrem através das linhas de rede telefônicas.

5) Redes de dados: representa todos sistemas eletrônicos e redes de dados onde as interações ocorrem através de cabos estabelecidos e linhas de rede com fio.

Dentro desses canais são descritos dezessete módulos para suas análises. Esses módulos, por sua vez, são divididos em quatro fases: fase Regulatória, fase de Definições, fase de Informações e fase de Teste de Controles Interativos. A fase Regulatória envolve os módulos de Revisão de Estado, Logística e Verificação de Detecção Ativa e representa a direção a ser tomada, o conhecimento que o auditor deve ter antes de realizar a auditoria, os requisitos de auditoria, o escopo e suas restrições. Já a fase de Definição é a principal em todo o processo, pois é responsável pela definição do escopo do teste. Na maioria das vezes, definir o escopo é uma tarefa complexa já que não é evidente o que o auditor precisa procurar, quais as consequências em encontrar erros e que tipo de testes ele deve executar (quais são obrigatórios e quais são opcionais). A composição desta fase é constituída pelos módulos Visibilidade de Auditoria, Verificação de Acesso, Verificação de Confiança e Verificação de Controles. A fase de Informação é a fase responsável por organizar o processo de coleta de informações, sendo composta pelos módulos de Verificação do Processo, Verificação de Configuração, Validação de Propriedade, Revisão da Segregação, Verificação da Exposição e Inteligência Competitiva. Por fim, a fase de Teste de Controles Interativos

descreve os testes práticos reais realizados sobre as informações coletadas. Essa fase é composta pelos módulos Verificação de Quarentena, Auditoria de Privilégios, Validação de Sobrevivência, Alerta e Revisão de Logs.

Para mensurar os resultados dos testes de segurança a metodologia OSSTMM utiliza a ideia de RAV (Risk Assessment Values). A função básica do RAV é analisar os resultados do teste e computar o valor atual da segurança baseado em três fatores: segurança operacional, controle de perda e limitações. O valor final de segurança é conhecido como RAV score. Usando o RAV score, um auditor pode facilmente extrair e definir marcos baseado no estado atual da segurança para realizar uma melhor proteção. De uma perspectiva de negócio, RAV pode otimizar a quantia de investimento requerido na segurança e pode ajudar a justificativa de investimentos em soluções mais efetivas.

2.3.3 Issaf

É uma biblioteca com várias funcionalidades que representam uma metodologia capaz de modelar os requisitos de controle internos para a segurança da informação, direcionado para avaliar a segurança de redes, sistemas e aplicações. Integrando esta metodologia como ciclo de vida de negócio, é possível fornecer acurácia, completude e eficácia requeridos para completar os requisitos de teste de segurança em uma organização tendo como foco: a área técnica, que estabelece o conjunto de regras e procedimentos para seguir e criar um processo adequado de avaliação de segurança, e a área gerencial, que realiza os compromissos com o gerenciamento e melhores práticas que devem ser seguidas ao longo do processo de auditoria.

A ISSAF também é estruturada em três grandes áreas de execução: planejamento e preparação, avaliação e relatório, limpeza e destruição de artefatos. A fase de Planejamento (organiza os passos necessários para definir o ambiente de teste) seja no planejamento e preparação das ferramentas de teste, contratos e aspectos legais, definição da equipe de trabalho, prazos, requisitos e estrutura dos relatórios finais. E a fase de avaliação que representa o centro da metodologia, onde o teste de penetração de segurança é realmente executado. A mesma é composta das seguintes atividades:

1. Coleta de informações: Consiste em coletar toda a informação possível sobre o alvo em questão a ser avaliado, auxiliando o avaliador a realizar a tarefa da maneira mais completa possível. Na maioria dos casos a principal e talvez única fonte de informação inicial é a Internet. Esta etapa é muito importante para o início do Pentest, no qual o processo de coleta interfere diretamente na completude do mesmo. Em geral, o objetivo desta atividade é explorar todas as vias possíveis de ataque dando uma

visão completa do alvo.

2. Mapeamento da rede: Informações específicas da rede, baseado também na atividade de coleta, são mapeadas para produzir a topologia de rede do alvo. Existem diversas ferramentas que podem ser utilizadas para auxiliar a descoberta e o mapeamento da rede e dos computadores envolvidos no teste. Esta atividade, resumidamente, foca seus esforços nos aspectos técnicos de descoberta de informações. Durante a enumeração e o mapeamento de rede o auditor busca identificar os sistemas operacionais envolvidos, firewalls, sistemas de detecção de intrusão, servidores e serviços, dispositivos de perímetro, roteamento e topologia geral rede (layout físico).

3. Identificação de vulnerabilidades: Esta atividade, de posse dos dados enumerados e da topologia de rede, busca encontrar falhas dentro da rede, servidores, serviços e outros recursos. A partir da enumeração e mapeamento de rede o auditor busca verificar fatores como a precisão na identificação de serviços e sistemas operacionais e listar os computadores e servidores vulneráveis. O objetivo desta etapa é usar as informações coletadas para fazer uma avaliação técnica atualizada sobre a existência de vulnerabilidades. Esta atividade é realizada combinando versões de serviços vulneráveis com sequência de comandos elaborados por *hackers* conhecidos, percorrendo a rede em diversas direções, testando webservices, localizando senhas fracas e contas e escalando privilégios.

4. Penetração: Prova as vulnerabilidades e códigos elaborados por hackers que o auditor identificou anteriormente.

5. Acesso e Escalada de Privilégio: Esta atividade é um advento de quando o testador ganhou algum acesso no alvo através da execução das atividades anteriores e assim pode realizar a escalada de privilégio.

6. Enumeração: Uma vez que o auditor ganhou o acesso e os privilégios, são executados, por exemplo: ataques a senhas, monitoramento e análise de tráfego, coleta de cookies, coleta de endereços de e-mail, identificação de rotas na rede e mapeamento de redes internas.

7. Comprometer usuários remotos: O invasor deve tentar comprometer os usuários remotos, tele-comutadores e sites remotos.

8. Manutenção de acesso: O auditor precisa reter os links de comunicação com a rede alvo. Essa comunicação, por sua vez, é interessante que seja através de um canal secreto (covert channel) para diminuir as chances de detecção.

9. Cobrindo rastros: O principal objetivo desta atividade é esconder ferramentas ou códigos elaborados por hackers usados durante o comprometimento do alvo.

Por fim, a fase de Relatório, Limpeza e Destruição de Artefatos é responsável

pelo processo de pós-invasão do teste. O auditor escreve um relatório completo e destrói os artefatos construídos durante a fase de Avaliação.

A metodologia ISSAF possui ampla documentação sobre a sua estrutura, e apresenta como uma das principais vantagens a criação de uma conexão clara entre as tarefas do Pentest e as ferramentas utilizadas. Da mesma forma, a ordem na qual a metodologia descreve o processo do Pentest é otimizada para ajudar o testador na execução completa e correta do teste, evitando erros comumente associados com estratégias de ataques selecionados aleatoriamente. Pelo viés de limitações, ressalta-se a falta de melhores orientações na elaboração de relatórios, que não é bem definida e possui pontos que deveriam ser atualizados. Juntamente a isso, o fato do fluxo de controle ser one-way desconsidera hipóteses que podem melhorar o procedimento do teste uma vez que o testador já descobriu algumas vulnerabilidades, assim como o que acontece na metodologia OSSTMM.

2.3.4 Ptes

A metodologia PTES (Penetration Testing Execution Standard) detalha instruções de como executar as tarefas que são requeridas para testar precisamente o estado da segurança em um ambiente. A intenção do modelo é não estabelecer padrões engessados para um teste de penetração, e a comunidade de analistas e profissionais de segurança responsável por sua criação trata a ideia de que as diretrizes para o processo de avaliação da segurança de um ambiente devem ser de fácil compreensão para as organizações. Por essa razão, as diretrizes técnicas ajudam a definir procedimentos a serem seguidos durante um Pentest, fazendo com que a metodologia forneça um estrutura base para iniciar e conduzir um teste de segurança, além de possuir gráficos bem organizados e uma série de métodos incluídos. A estrutura da metodologia é composta por sete fases:

1) Interação: apresenta o planejamento de ferramentas e técnicas que serão utilizadas no Pentest.
2) Coleta de informações: fornece um padrão destinado ao processo de reconhecimento do alvo em questão.
3) Modelagem de ameaças: define a modelagem de ameaças para que o Pentest tenha seu direcionamento realizado de maneira correta.
4) Análise de vulnerabilidades: trata o processo de descoberta de falhas e vulnerabilidades de um sistema ou ambiente.
5) Exploração: foca em estabelecer o acesso a um sistema ou recurso passando pelas restrições de segurança.

6) Pós - exploração: determina o valor de uma máquina compromissada e mantém o controle da mesma para uma futura utilização.

7) Relatório: define os critérios basilares para o relatório do teste.

PTES é um modelo de gestão projetado para fornecer às empresas/organizações e aos prestadores de serviços de segurança uma linguagem e escopo comuns para a realização de Pentest. Tal tarefa está relacionada principalmente a realização de padrões concisos para medir testes de penetração e oferecer orientações de como o teste precisa ser realizado aos clientes. A forma como são fornecidas as diretrizes de execução do processo representa a principal vantagem do modelo em relação aos demais, aliado ao fato de que o mesmo considera o conhecimento do testador como aspecto primordial ao longo das fases. Dessa forma, a construção da metodologia por parte da comunidade de especialistas na área de segurança fornece uma abordagem diferenciada e diretamente ligada aos critérios técnicos de um teste de segurança. Em contraponto, isso impacta vagamente nos aspectos de negócio, tornando-se uma fator limitante para a completude de um Pentest. Em relação a documentação da metodologia, a citação do uso de ferramentas e técnicas para cada uma das fases é descrita de maneira extremamente robusta, ao passo que orientações em relação à medidas de eficiência, elaboração dos relatórios e tratamento de caminhos alternativos na descoberta de vulnerabilidades, por exemplo, poderiam ser melhor definidas.

2.3.5 Nist 800-30

A metodologia NIST foi inicialmente introduzida inicialmente como um GUIA pela GNST (Guideline on Network Security Testing), reproduzida na publicação especial 800-42, e a sua última versão continuada é apresentada na publicação especial 800-15 como Technical Guide to Information Security Testing and Assessment. A elaboração deste modelo é considerada a primeira que introduz um processo detalhado e formal para a escrita de relatórios, e da mesma forma em relação a trabalho e processo que lida com hipóteses induzidas. A sua estrutura segue quatro etapas principais: Planejamento (o sistema é analisado para encontrar os alvos de teste mais interessantes) ; Descoberta, (o testador procura as vulnerabilidades no sistema); Ataque (onde o testador verifica se as vulnerabilidades encontradas podem ser exploradas); e Relatório (onde cada resultado proveniente das ações realizadas na etapa anterior é reportado).

Uma vez que tem um foco em componentes de concreto como sistemas, ele pode ser facilmente utilizado para as organizações que são novas para a avaliação de risco (LIANG, 2013).

Adicionalmente, cada passo executado possui um vetor de entrada, que representa o conjunto de dados a serem analisados, e um vetor de saída, que representa

o conjunto completo de resultados derivados das ações executadas. Em seu fluxo, a seta orientada entre ataque e descoberta é a primeira tentativa de representação de hipóteses induzidas. A ideia principal de hipóteses induzidas se baseia nos artefatos: Vetor Alvo (TV), Vetor de Vulnerabilidade (VV) e Vetor de Ataque (AV), que representam respectivamente: o conjunto de alvo com investigação em andamento, conjunto de vulnerabilidade conhecidas e o conjunto de ataque relevantes.

Além do fato de considerar hipóteses induzidas, outra característica positiva da metodologia é a forma como a mesma orienta o auditor na elaboração dos relatórios. De acordo com as melhores práticas, a metodologia sugere escrever um relatório passo-a-passo, onde o auditor relata suas descobertas depois da fase de planejamento e depois de cada ataque (realizado com sucesso ou não), descrevendo as vulnerabilidades que puderam ou não ser exploradas. Em compensação a isso, a metodologia não provê modelos e orientações para a escrita dos relatórios finais. Da mesma forma, cabe ressaltar a maneira como é construído o vetor de vulnerabilidade, onde apenas uma parte dos problemas encontrados durante a primeira fase originam vulnerabilidades em potencial. Em paralelo a isso, não fazem parte do relatório aqueles problemas que não listam falhas, e tal prática deve ser reconsiderada: todos os problemas encontrados devem ser levados em conta como descobertas interessantes e então, devem ser documentados pois posteriormente podem vir a serem riscos relevantes. Por fim, a forma utilizada pela norma para explicitar as suas definições e conceitos pode ser considerada uma limitação no que diz respeito ao entendimento da mesma, uma vez que sua compreensão sobre o que, onde, porque e como o processo de teste será realizado não é completamente claro.

2.3.6 Relação entre normas e modelos

O quadro 2.6 apresenta algumas das práticas recomendadas pela ISO/IEC 27002:2013, OSTMM, ISSAF, PTES E NIST 800-30 para a implantação das Melhores Práticas para mitigação de riscos em incidentes de TI. Tais práticas foram identificadas durante o estudo para a produção de de melhores práticas para implantação desse guia.

Quadro 6 – Comparativo entre normas e metodologias

Item	Prática:	ISO 27002	OSSTMM	ISSAF	PTES	NIST 800-30
1	PDCA (Processo de Gerenciamento de Risco de TI)	Atende	Parcialme nte	Parcialmente	Não Atende	Atende
2	Estrutura do Documento	Atende	Atende	Atende	Parcialmente	Parcialmente
3	Escopo da metodologia	Atende	Atende	Atende	Parcialmente	Atende
4	Envolvimento Alta Administração	Parcialmente	Não Atende	Parcialmente	Não Atende	Não Atende
5	Identificação dos ativos críticos	Atende	Não Atende	Parcialmente	Parcialmente	Parcialmente
6	Mapeamento de Vulnerabilidades	Parcialmente	Não Atende	Não Atende	Parcialmente	Atende
7	Identificação de Ameaças	Não Atende	Não Atende	Não Atende	Parcialmente	Parcialmente
8	Controle para mitigação dos Riscos	Atende	Não Atende	Não Atende	Parcialmente	Atende

2.4 REVISÃO SISTEMÁTICA

O estudo de Revisão Sistemática teve como objetivo levantar informações a cerca da segurança da informação, na tentativa de identificar as melhores práticas para mitigação de riscos em TI. O método utilizado nessa pesquisa seguiu critérios de seleção, pré-estabelecidos, sobre um determinado assunto ou tema que consistiu em: definir uma pergunta; buscar fontes primárias de informação relacionadas com a pergunta a ser respondida (artigos, livros, etc.); definir critérios de inclusão e exclusão das fontes primárias encontradas; analisar a qualidade das fontes primárias com base nos critérios de inclusão estabelecidos e apresentar os resultados do estudo (KITCHENHAN et al., 2008).

Uma das razões para se utilizar o método de revisão sistemática foi a identificação de uma boa fundamentação teórica, obtendo, com isso, agregação de conteúdos que pudessem trazer resolução de um problema proposto ou a busca de uma resposta a questões de pesquisa (MELO et al., 2014), bem como identificar temas que necessitam ser comprovadas, auxiliando na orientação para investigações futuras (SAMPAIO e MANCINI, 2007).

Segundo Biolchini et al. (2005), são estabelecidos três fases no processo que conduzirá a revisão de literatura: planejamento, execução/desenvolvimento e análise e

divulgação dos resultados. Cada etapa descreve os passos e as ações ou atividades necessárias para identificação dos estudos que tiveram relevância com essa pesquisa.

- Fase de Planejamento: foi elaborado o protocolo de revisão, antes do início da pesquisa, incluindo os seguintes itens: palavras chaves de pesquisa, onde os estudos foram encontrados, critérios de inclusão e exclusão dos artigos, definição dos desfechos de interesse, verificação dos resultados, determinação da qualidade dos estudos e análise da estatística utilizada.

- Fase de Execução: foi realizada toda a condução criteriosa dos estudos primários, conforme estabelecido no protocolo criado na etapa de planejamento. Para o desenvolvimento e execução da revisão sistemática, todas as atividades de seleção e leitura foram realizadas entre o período de 01/01/2016 à 30/03/2016. Todos os estudos foram identificados, coletados e organizados em uma lista estruturada, passando por revisões, a cada etapa, para ter certeza que os estudos relevantes não foram eliminados ou passados despercebidos pelo pesquisador. Concluindo essa fase, as informações foram extraídas somente dos estudos selecionados.

A necessidade da existência de políticas para a existência do processo de segurança da informação é descrita na NBR ISO/IEC 27002:2013: “A segurança da informação é alcançada pela implantação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e função de software e hardware”, (ABNT, 2012).

Pensando nesse questionamento, este estudo de Revisão Sistemática teve como objetivo levantar informações acerca da segurança da informação, na tentativa de identificar as melhores práticas para a mitigação de riscos em incidentes de TI. O método de revisão sistemática consiste na revisão da literatura seguindo critérios de seleção, pré-estabelecidos, sobre um determinado assunto ou tema e consiste em:

1) definir uma pergunta;

2) buscar fontes primárias de informação relacionadas com a pergunta a ser respondida (artigos, livros, etc.);

3) definir critérios de inclusão e exclusão das fontes primárias encontradas;

4) analisar a qualidade das fontes primárias com base nos critérios de inclusão estabelecidos e

5) apresentar os resultados do estudo (KITCHENHAN et al., 2008).

Conforme apresentado na figura 6, esta fase passou por 5 etapas que possibilitaram fazer uma filtragem de todos os estudos identificados nas seguintes bases científicas: ACM, IEEE Explore, Science Direct, Google Scholar e Scopus.

Na etapa 1, por meio dessa filtragem de busca de estudos nas bases científicas

conforme definição de strings, foram identificados 542 estudos que poderiam apresentar relação com a pesquisa. Na Etapa 2, foram selecionados 27 estudos identificas como relevantes por meio da leitura dos títulos. Na etapa 3, a seleção de cada estudo foi aprimorada por meio de filtragem, utilizando-se dos critérios de inclusão e exclusão, a partir da leitura do resumo (abstract). Sendo assim, foram selecionados 11 estudos. Na etapa 4, foram lidas a introdução e a conclusão dos estudos da etapa anterior, sendo selecionados apenas os estudos que tivessem relação com as questões de pesquisa.

Dessa forma, foram selecionados 11 estudos dos 27 estudos selecionados na etapa anterior. A etapa 5 serviu para realizar a leitura de todos os estudos selecionados na etapa anterior, destacando pontos relevantes de acordo com os propósitos estabelecidos pela pesquisa.

As figuras 2.4 e 2.5 lista os 27 trabalhos selecionados.

Figura 8 – Trabalhos relacionados

Ano	Trabalho	Tipo	Autor	Base
2014	Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool Demo)	Artigo	Mayer, Nicolas and Aubert, Jocelyn	ACM
2013	Risk Mitigation Decisions for IT Security	Artigo	Yeo, M. Lisa and Rolland, Erik and Ulmer,	
2015	Using stakeholders knowledge for data quality of information system, information system security documentation quality, information systems security risk management	Artigo	Sillaber, Christian and Breu, Ruth	
2014	Is Privacy Supportive for Adaptive ICT Systems?	Artigo	Wohlgemuth, Sven	
2015	Complexity Reduction in Information Security Risk Assessment	Artigo	Haya, Glourise M.	
2015	Information Security Risk Management in Computer Networks Based on Fuzzy Logic and Cost/Benefit Ratio Estimation	Artigo	Anikin, Igor and Emaletdinova, Lilia Yu.	
2013	The State of the Art of Risk Assessment and Management for Information Systems	Artigo	Lulu Liang and Wang Ren and Jing Song and Huaming Hu and Qiang He and Shuo Fang	IEEE
2013	The research and application of the risk evaluation and management of information security based on AHP method and PDCA method	Artigo	Meng Meng	
2014	Information security Risk Management in Critical informative Systems	Artigo	Kiran, K.V.D. and Reddy, L.S.S. and Kumar, VP.	
2015	Security Risk Management in complex organization	Artigo	Sedinic, I. and Perusic, T.	
2013	Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems	Artigo	Moyo, M. and Abdullah, H. and Nienaber, R.C.	
2015	A Risk Analysis Model for PACS Environments in the Cloud	Artigo	Da Silva Cordeiro, S. and SantAna, F.S. and Suzuki, K.M.F. and Mazzoncini Azevedo-Marques, P.	
2013	Risk Assessment Methodology Based on the NISTIR 7628 Guidelines	Artigo	Abercrombie, Robert K. and Sheldon, Frederick T. and	
2014	Information security risk management planning: A case study at application module of state asset directorate general of state asset ministry of finance	Artigo	Prasetyo, S. and Sucahyo, Y.G.	
2015	Experimentation tool for critical infrastructures risk management	Artigo	Bialas, A.	

Figura 9 – Trabalhos relacionados

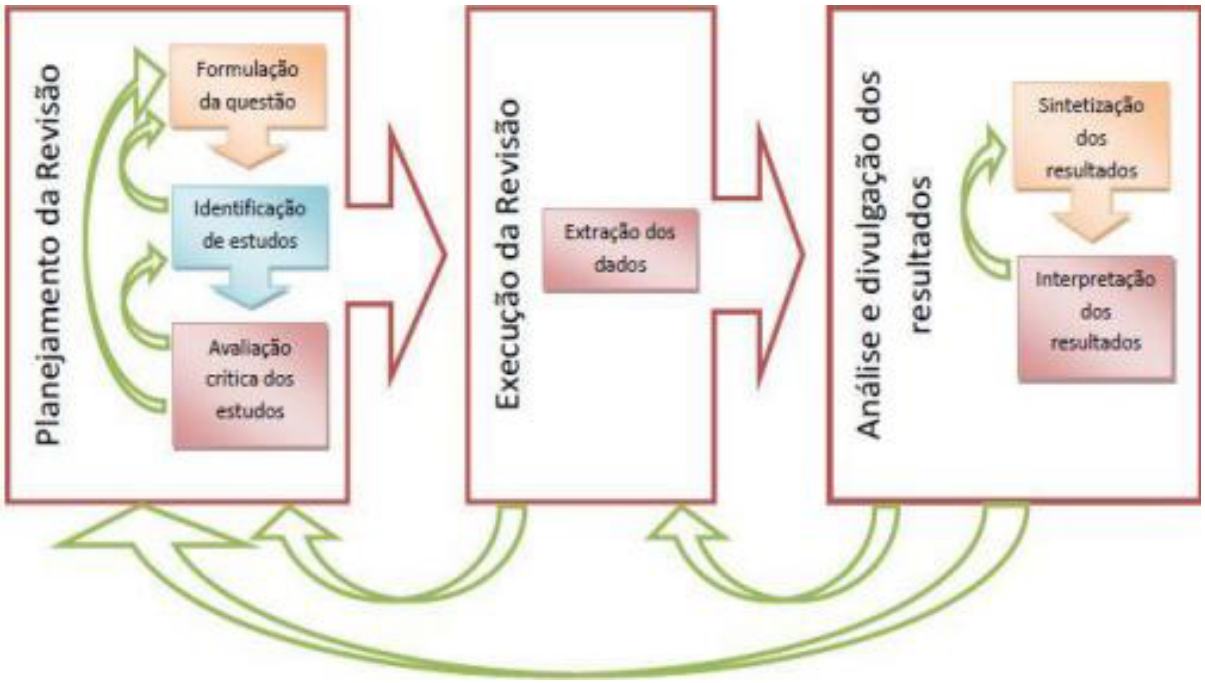
2013	Information security risk assessment in SCM	Artigo	Roy, A. and Gupta, A.D. and Deshmukh, S.G.	
2014	Development of risk factor management method for federation of clouds	Artigo	Alguliyev, R. and Abdullayeva, F.	
2014	A multidimensional approach to information security risk management using (FMEA) and fuzzy theory	Artigo	Maisa MendonÃ§a Silva and Ana Paula Henriques de Gusmãoo	
2014	A Quantitative Approach to Risk Management in Critical Infrastructures	Artigo	E. Sapori and M. Sciutto and G. Sciutto	
2013	Monitoring information security risks within health care	Artigo	Nicole van Deursen and William J. Buchanan and Alistair Duff	Science Direct
2013	Chapter 1 - Information Security Risk Assessments Chapter 2 - Information Security Risk Assessment: A Practical Approach Chapter 6 - Risk Management	Artigo	Mark Talabis and Jason Martin	
2013	Accounting Information Security: Procedures for the Preparation of a Security Policy Based on ISO 27001 and ISO 27002	Artigo	MATTES e PETRI	Google Scholar
2013	Politica de segurança da informação aplicada em uma instituição de ensino mediante análise de risco	Dissertação	*Sérgio Duque Castilho, Miguel Feitoza da Fonte*	
2014	Fatores criticos de sucesso em segurança da informação em um órgão da Administração Pública Federal	Monografia	Quintella, Heitor Luiz Murat de Meirelles; Branco, Marcelo Pereira de Oliveira	
2012	Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal	Artigo	DE ARAUJO, Wagner Junqueira.	

Fase de Análise e Divulgação de Resultados: é a etapa final do processo de elaboração de uma revisão sistemática. Consiste em mostrar os dados em um formato que possa ser analisado e estudado. Geralmente, nessa fase da revisão, os resultados são exibidos em forma de tabelas ou gráficos, tendo como base as fontes de informações primárias selecionadas (SAMPAIO e MANCINI, 2007).

O desenvolvimento da metodologia de revisão sistemática inclui a caracterização de cada estudo selecionado, avalia a qualidade de cada um destes estudos, identifica seus conceitos importantes, compara análises apresentadas e conclui sobre o que a literatura afirma sobre determinada área, apontando ainda setores que carecem de novos estudos.

A Figura 2.6 apresenta o processo de condução da revisão sistemática e suas atividades relacionadas para este trabalho.

Figura 10 – Revisão Sistemática
Fonte: Arruda (2014)



Para contemplação de todas as etapas descritas anteriormente, a revisão sistemática teve início com a elaboração de um protocolo de revisão especificado com o objetivo de realizar um levantamento bibliográfico e científico na área de Gestão de Segurança da Informação.

Após finalizar todas as atividades das etapas de execução da revisão, foram selecionados 11 estudos que estavam em conformidade com os critérios de inclusão, estando esses em total relevância com a questão de pesquisa elaborada para atender o objetivo proposto para revisão.

Segundo Sampaio e Mancini (2007), “a realização de uma revisão sistemática envolve o trabalho de pelo menos dois pesquisadores, que avaliarão, de forma independente, a qualidade metodológica de cada artigo selecionado”.

Figura 11 – Parte 1- Protocolo de revisão

Protocolo de Revisão Sistemática

Realizar um levantamento bibliográfico, literário e científico em Gestão de segurança da informação com temas relacionados a Gestão de Risco, Política de Segurança e Modelo de Maturidade.

Questão de pesquisa

Q1 – Quais as melhores práticas em gestão de TI para o desenvolvimento e implantação de políticas de segurança da informação?
Q2 – Como realizar o gerenciamento dos riscos de incidentes de TI para atender os negócios de forma eficiente, apropriada e condizente com a realidade das instituições federais de educação?

Palavras-chaves relacionadas às questões de pesquisa
A pesquisa abrange a área de gestão da segurança da informação, porém será delimitado nas sub áreas de política de segurança da informação, gestão de riscos e modelo de maturidade.
Os idiomas pesquisados serão o inglês e português, pois a literatura científica também são encontrados no idioma de aplicação da pesquisa.

Português:	Inglês:
- Segurança da informação, modelo de maturidade de segurança da informação, nível de maturidade de segurança da informação, maturidade organizacional de segurança da informação; - Política de segurança da informação, Gerenciamento de política de segurança da informação, ISO/IEC 27002, OSSTMM, NIST, PTES, ISSAF, boas práticas; - Gestão de Riscos de Segurança, Modelos de Gestão de Riscos de Segurança da Informação, Metodologia de Gestão de Riscos de Segurança da Informação, Framework de Gestão de Riscos de Segurança da Informação	- Information security, information security maturity model, level of information security maturity, organizational maturity of information security; - Information security policy, information security policy management, ISO / IEC 27002; ISO / IEC 27002, OSSTMM, NIST, PTES, ISSAF, best practices, - Security Risk Management, Models Security Risk Management of Information, Security Risk Management Methodology of Information, Security Risk Framework for the Management of Information.

Intervenção
Pretende-se, por meio de busca na literatura científica, intervenções na área de segurança da informação em Gestão de Risco, Política de Segurança da Informação e Modelo de Maturidade em segurança da Informação.

Efeito
Com a referida pesquisa pretende-se alcançar as seguintes ações:
- assegurar que as políticas de segurança sejam implementadas e orientadas a partir de práticas de gestão de TI, reconhecidas internacionalmente, tais como: ISO/IEC 27002, OSSTMM, NIST, PTES, ISSAF.

- propor que a maturidade da gestão de segurança da informação possam ser formulados e direcionados de maneira mais condizente com as melhores práticas mundiais e necessidades do negócio.

População
A população aplicável a esta pesquisa pode ser resumida em estudos e trabalhos (artigos, dissertações, teses, livros, normas, decretos e normativas aplicadas na Administração Pública Federal) encontrados na literatura em segurança da informação.

Aplicação
O resultado dessa pesquisa é a aplicação de propostas para modelos de implementação e melhorias de política de segurança da informação, com base nas melhores práticas de gestão de TI, elaboração/revisão e melhoria da maturidade da gestão de segurança da informação nas instituições federais de educação; elaboração de um modelo a ser utilizado nas Instituições federais de educação para a Gestão de Riscos de TI.

Figura 12 – Parte 2- Protocolo de revisão

Critérios de seleção de fontes para a pesquisa dos trabalhos: devem selecionar estudos de nível primário; os estudos selecionados devem sem ser revisado por pares; devem estar na web, com exceção apenas de livros que podem ser impressos; devem disponibilizar os trabalhos na integra e gratuitamente para fins de pesquisa; devem possuir mecanismos avançados de busca que permitam a combinação de palavras-chave com os termos de relação "AND" e "OR"; devem ser de renome científico acadêmico mundial, com exceção de sites web de universidades, caso seja necessário, que contenham os mecanismos de busca exigidos.

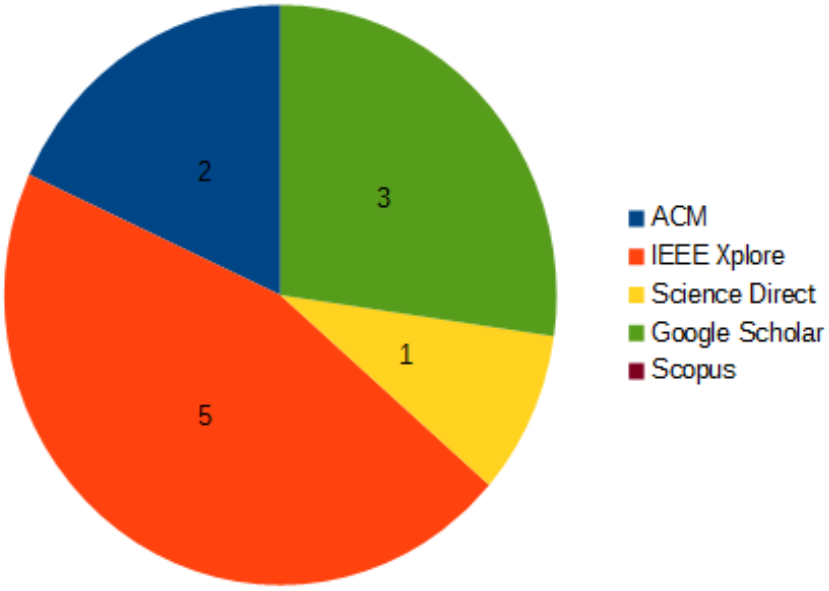
Figura 13 – Parte 3 - Protocolo de revisão

Procedimentos para seleção das fontes: As fontes serão selecionadas por meio de testes com as palavras-chave já citados. Caso retornem resultados satisfatórios ao teste, elas serão incluídas, ao contrário serão excluídas (descartadas).	
Método de pesquisa: A busca por trabalhos será realizada de forma eletrônica, através de mecanismos de busca de sites web especializada e de renome científico acadêmico, podendo ser utilizados também sites de universidades que contenham esses mecanismos disponíveis;	
Strings de busca: as strings ou frases de busca são baseadas nas palavras-chave já citadas. Esses strings serão aplicadas de acordo com a disponibilidade técnica de estratégia de busca do mecanismo a ser utilizado, podendo sofrer pequenas adaptações para que o mecanismo consiga executá-las. As strings são as seguintes: **Português:** 1. - gestão de segurança da Informação OR política de segurança da informação OR gestão de riscos da segurança da informação; 2. - "Gestão de Segurança da Informação" OR nível de maturidade" OR "modelo de maturidade" - política de segurança da informação OR COBIT OR ITIL OR "ISO/IEC 27002" OR "melhores práticas" OR "Gestão de risco "AND (Modelos OR framework OR metodologia OR "ISO/IEC 27002") 3. - OSSTM OR NIST OR PTES OR ISSAF	**Inglês:** 4. - Information Security Management OR information security policy OR management risk security information 5. - "Information Security Management" OR "maturity level" OR "maturity model" - "information security polity" OR COBIT OR ITIL OR "ISO/IEC 27002" OR "best practices" - "management risk" AND (Models OR framework OR methodology OR "ISO/IEC 27002") 6. - OSSTM OR NIST OR PTES OR ISSAF **Lista de fontes de busca:** ACM Portal, IEEE Xplore, ScienceDirect, Google Scholar e Scopus.
Definição dos trabalhos Os seguintes critérios devem nortear a inclusão e exclusão dos trabalhos. Inclusão: - Estudos primários; - Estudos revisados por pares; - Os estudos devem apresentar relevância no título; - Os trabalhos devem estar disponibilizados por completo; - Os trabalhos devem demonstrar algum embasamento científico que comprove os seus resultados; - Estudos que discutem as questões de pesquisa já citados; - Estudos publicados entre janeiro de 2010 a dezembro de 2015. - Exclusão: - Estudos secundários; - Estudos não revisados por pares; - Estudos duplicados; - Estudos que não apresentam relevância no título; - Estudos que não relatem as questões pesquisadas;	

A figura 2.10 apresenta o quantitativo de estudos primários selecionados em cada base científica. Dos 11 estudos selecionados pela revisão sistemática, em 5 bases,

observou-se que a base IEEE Xplore apresentou maior número de estudos relevantes enquanto a base Scopus não apresentou nenhum estudo relevante para a pesquisa.

Figura 14 – Estudos relevantes por base científica



2.5 TRABALHOS RELACIONADOS À REVISÃO SISTEMÁTICA

Esta seção é dedicada aos três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. São itens essencias no que diz respeito a segurança da informação pois estão relacionados a gestão de riscos em TI, tema de grande relevância e importância, devido a essas caracteristicas e para que se tenha o embasamento científico para o desenvolvimento deste trabalho foi realizado o procedimento de revisão sistemática da literatura.

Diversos artigos foram relacionados ao tema gestão de riscos através desse procedimento, utilizando-se os recursos de filtros com base em critérios pré-definidos, selecionando 11 artigos, publicados no período de 2013 a 2015. Esses artigos foram essenciais para o desenvolvimento do trabalho de acordo com a seção 2.5, p 51 e resumo de cada trabalho.

2.5.1 Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool Demo)

Artigo publicado em 2014 no SIN '14: Proceedings of the 7th International Conference on Security of Information and Network. O artigo trata sobre o uso de uma ferramenta específica para Gestão de Riscos de Segurança da Informação no contexto da regulação dos provedores de serviços de telecomunicações europeias. O objetivo do trabalho é apresentar as características e abordagem para a abordagem TISRIM (Tudor Information Security Risk Management tool) fine-tuning, da ferramenta de gestão de riscos. Tal ferramenta utilizou diferentes métodos e normas baseadas na ISO/IEC 27005 seguindo as etapas de: estabelecimento de contexto, identificação dos riscos, análise de riscos, avaliação de riscos, aceitação do risco, comunicação e consulta dos riscos e o monitoramento do risco e revisão. Após a definição das etapas estabelecidas é definido o método de pesquisa (MAYER e AUBERT, 2014).
Para que o objetivo do trabalho fosse alcançado, definiu-se um método de pesquisa em quatro etapas:

Etapa 01 - Modelagem dos serviços de telecomunicações mediante processos de negócios,

Etapa 02 - Modelagem dos serviços de Telecomunicações mediante arquitetura de um sistema de informação,

Etapa 03 - Definição da base de conhecimentos relacionados com o serviço de riscos e

Etapa 04 - A integração dos resultados de uma ferramenta de software e de experimentação.

Foi desenvolvido o software TISRIM e adaptado ao setor de telecomunicações. A ferramenta foi desenvolvida e apoiada em colaboração com os Provedores de Serviços de Telecomunicações e as agências reguladoras o que proporcionou flexibilidade a ferramenta. Tal abordagem permitiu integrar conhecimentos específicos do setor, incluindo bases de conhecimento e um primeiro nível de identificação de riscos (serviços típicos e ativos, ameaças principais), que ajudam a facilitar o processo de gestão de riscos de segurança da informação. A ferramenta ajudou as agências reguladoras na obtenção e processamento dos dados e na utilização de relatórios e estatísticas. A grande contribuição do trabalho foi a rapidez no processo de gestão de riscos, dando celeridade na identificação e no tratamento dos riscos, além de prover o mapeamento dos riscos de forma padronizada e sistemática

2.5.2 Risk Mitigation Decisions for IT Security

Este artigo define o problema do fluxo de redução do risco e apresenta um modelo formal usando uma estrutura de workflow. Três métodos de fixação de controles diferentes são introduzidos para resolver o problema e uma análise comparativa é apresentada através de um conjunto de testes. Um ano de ataques simulados foi utilizado para validar a qualidade das soluções. No artigo observamos que o método de fixação de controle de programação matemática produz melhorias substanciais em termos de redução de riscos, quando comparado com heurísticas que normalmente seriam usadas pelos gestores para resolver o problema. A contribuição desta pesquisa é fornecer aos gestores métodos para reduzir substancialmente os riscos de segurança da informação, enquanto obtém significativamente melhores retornos sobre seus investimentos em segurança. Para isso utiliza-se de uma abordagem simulada para controlar o posicionamento, que orienta o gerente a examinar toda a sua infraestrutura de uma forma integral, para isso faz-se necessário o comprometimento dos gestores em suas atividades e conhecimento a respeito da GR (YEO, 2014).

2.5.3 The state of the art of risk assessment and management for information systems (LIANG, 2013)

Artigo publicado em 2014 no 9th International Conference Information Assurance and Security (IAS), 2013. O artigo destaca a importância da avaliação e gestão de riscos para a garantia da segurança do sistema, explicando que apenas o cuidado não é o suficiente, mas também uma análise sistemática das vulnerabilidades e ameaças e com esse resultado de análise poderá determinar a extensão em que os eventos possam afetar de forma adversa a organização.

Pela análise da ameaça e informações sobre as vulnerabilidades, pode-se identificar e determinar até que ponto as mesmas podem afetar negativamente uma organização. Além disso, com base no tipo de ameaça e no valor de impacto, a probabilidade da ocorrência de tal evento será dado. No artigo é feito uma introdução a gestão de riscos, em seguida é apresentado um modelo de gestão de riscos em 3 (três) níveis e por fim os seis passos pra um modelo de gestão de riscos é analisado.

A avaliação de Risco é uma parte da estrutura hierárquica de gerenciamento de risco sendo composto por 4 etapas: preparação, realização, comunicação e manutenção. O primeiro passo no processo de avaliação de risco é preparar a avaliação. O propósito deste passo é estabelecer um contexto para a realização de avaliação de risco na etapa seguinte.

Realizar a avaliação é a segunda etapa, também é o passo mais importante no processo de avaliação de riscos. A lista de riscos de segurança da informação é obtida

para informar as decisões de resposta a riscos nesta etapa. Para alcançar esta função, as organizações analisam as ameaças, vulnerabilidades e seus impactos, e calculam a probabilidade de ocorrência do evento, e reúnem a informação essencial de acordo com o contexto de avaliação estabelecido no primeiro passo.

A terceira etapa do processo de avaliação de risco é comunicar os resultados da avaliação e compartilhá-los. Assim, os tomadores de decisão poderão ter a informação adequada para tomar decisões de risco mais precisas.

Manter a avaliação é o último passo no processo de avaliação de riscos. Para garantir a eficácia da resposta ao risco, faz-se necessário a revisão das decisões de gestão de risco. Através do monitoramento de risco de forma contínua, as organizações mantem as avaliações de risco para incorporar as alterações atualizadas. O artigo demonstrou os principais conceitos da avaliação e gestão de riscos, conceitos esses fundamentais para a interpretação do processo de gestão de riscos (GUANGFU, 2010).

2.5.4 The research and application of the risk evaluation and management of information security based on AHP method and PDCA method

Artigo publicado na conferência Information Management, Innovation Management and Industrial Engineering (ICIII), 2013 6th International Conference on. O Artigo apresenta um modelo para realizar a transformação de uma análise riscos qualitativa para quantitativa para que se possa alcançar uma gestão de riscos de segurança informação dinâmico O modelo utiliza o método AHP com o uso de pesos para avaliação de riscos de segurança da informação, obtendo com isso os fatores de riscos. Posteriormente foi utilizado o método PDCA (Plan-Do-Check-Action). A contribuição do artigo para este trabalho é como material teórico a respeito dos conceitos e dos cálculos utilizados que serviram de base nesta dissertação (MENG, 2013).

2.5.5 Information security Risk Management in Critical informative Systems

O artigo foca em sistemas críticos e examina o domínio de engenharia de segurança da informação, processos de análise e gestão de riscos de segurança da informação no que se refere à garantia da informação e de sistemas críticos. Propõe uma forma de medição formulada pela definição de uma função de risco continuo, dependente do tempo com base em análise multivariada e teoria da distribuição de probabilidade. A análise de risco vem encontrando relutância em sua abordagem devido a percepção de sua complexidade e inexatidão. Análise de Riscos de Segurança é uma técnica utilizada na Gestão de Riscos como método de identificação de ameaças, vulnerabilidades e possíveis impactos para controles de segurança de sistemas de

informação críticos. Existem dois tipos de Análise de Riscos: análise e avaliação qualitativa e análise e avaliação quantitativa, cada uma apresentando suas vantagens e desvantagens. Este trabalho busca reconhecer e identificar todas as incertezas associadas com Análise de Riscos para sistemas de informações críticos e é dividido em quatro partes. A primeira parte especifica os problemas e as opções de avaliação de riscos de abordagens analíticas. A segunda parte especifica uma revisão abrangente sobre o assunto. A terceira parte identifica os elementos e componentes do risco, permitindo a implementação da metodologia formal para definir a expressão de risco que compõe toda análise de riscos para sistemas de informações críticos. A quarta parte proveu a metodologia que foi usada para analisar e validar tais expressões, concluindo sobre a importância de seu uso (KIRAN, 2014).

2.5.6 Security Risk Management in Complex Organization

O objetivo do artigo é descrever a maneira de alinhar diferentes metodologias de Gerenciamento de Riscos de Segurança da Informação causadas por diferentes requisitos de negócios. Tais metodologias descrevem a maneira de alinhar diferentes metodologias de gerenciamento de riscos causadas por diferentes requisitos de negócios. Essas metodologias apoiam os processos de decisões operacionais e apoiam os relatórios de riscos. O artigo explana alguns modelos de Gestão de Riscos de TI como o OCTAVE, NIST, COBIT e a ISO 27005 (SEDINIC e PERUSIC, 2015). A abordagem utilizada no artigo e implementada na empresa mostrou inúmeros benefícios que são:

- maneira prática para integrar metodologias de riscos diferentes;realizar a avaliação de riscos no curto período;
- realizar avaliação de risco em nível muito profundo e detalhes para riscos específicos tecnologicamente;
- unificação dos resultados para a área diferente em que as ferramentas de gerenciamento de risco são utilizados;
- otimização do tempo gasto no gerenciamento de riscos.

2.5.7 Information security risk management in small-scale organizations: A case study of secondary schools computerized information systems

O artigo trata da implementação da metodologia de gestão de risco OCTAVE-SMALL em duas escolas sul-africanas. Tal metodologia foi projetada para ser utilizada em pequenas organizações, apesar de haver variações da metodologia para serem

usadas em médias e grandes organizações, o que torna viável sua implementação nessas escolas consideradas pequenas (MOYO, 2013).

O autor descreve o processo de implantação da metodologia e seus passos de execução. Os dados foram coletados por meio de observação, listas de controles e planilhas OCTAVE-SMALL personalizadas e posteriormente processadas e interpretadas de forma qualitativa.

A metodologia adaptada é composta por quatro processos: 1- Identificar os ativos da CIS críticos e seus requisitos de proteção, 2 - Identificar ameaças aos ativos críticos, 3 - Identificação de vulnerabilidades em instalações de computação, 4 - Avaliação de riscos, desenvolvimento e implementação de estratégias de tratamento.

Os benefícios decorrentes da implantação da metodologia são proporcionar aos participantes uma oportunidade de desenvolver uma apreciação da segurança da informação em geral e como gerenciar os riscos associados. Também irá desenvolver e fomentar um sentimento de responsabilidade e prestação de contas em naqueles usuários que anteriormente foram deliberadamente envolvidas em atividades que levaram a violações de segurança.

2.5.8 A multidimensional approach to information security risk management using (FMEA) and fuzzy theory

O artigo apresenta uma abordagem para a gestão de riscos de segurança da informação, abrangendo Análise dos Modos de Falha e seus Efeitos (FMEA) e da lógica fuzzy. Esta abordagem analisa cinco dimensões de segurança da informação: o acesso à informação e sistemas, segurança de comunicação, infraestrutura, gerenciamento de segurança e desenvolvimento de sistemas de informação segura (SILVA, 2014). O autor explana sobre a gestão de riscos de segurança em uma organização e diz que a mesma envolve a identificação e análise de riscos para a organização, identificando e avaliando os danos que podem ser causados por um ataque bem sucedido nos negócios, e decidir em mitigar ou reduzir o risco. O autor desenvolveu uma metodologia para analisar as cinco dimensões da gestão de riscos com base no FMEA e teoria linguística difusa. A metodologia é comporta por 5 fases ou etapas: 1 – Identificação especialista, 2 - Determinação e avaliação de potenciais modos de falha, 3 - Determinação número fuzzy RP, 4 – Avaliação Dimensão, 5 – Ordenação Dimensão.

2.5.9 Accounting Information Security: Procedures for the Preparation of a Security Policy Based on ISO 27001 and ISO 27002 (MATTES e PETRI, 2013).

Artigo apresentado na International Conference on Information Systems and Technology Management , 2013. Apresenta como objetivo reunir e compilar informações necessárias para a elaboração de uma Política de Segurança da Informação com o intuito de especificar um padrão mínimo para implantação de políticas e normas de segurança em escritórios de contabilidade. A aplicação das ISO 27001 e ISO 27002 implica maior segurança e padronização dos serviços e da gestão da informação contábil. O objeto para justificativa foi a entrevista feita pelo autor em escritórios contábeis e as pesquisas feitas pelas empresas PricewaterhouseCoopers e Módulo Security Solutions. O artigo auxilia a estruturar um Sistema de Gestão da Segurança da Informação (SGSI) com base nas respectivas ISO, seguindo os requisitos apresentados e técnicas padrões indicadas. A metodologia de pesquisa utilizada nesse trabalho caracterizou-se como descritiva, abordagem quantitativa, procedimentos técnicos bibliográficos e documentais. As pesquisas indicam grande crescimento mundial com a questão da Segurança da Informação e principais problemas encontrados em escritórios contábeis. Como resultados, foram levantados os itens mínimos do padrão ISO 27002 relacionados com os riscos pertinentes à contabilidade.

2.5.10 Politica de segurança da informação aplicada em uma instituição de ensino mediante análise de risco (CASTILHO, 2013).

O estudo é uma publicação da Revista Tecnológica da Faculdade de Tecnologias de Ourinhos, 2012. Esse traz como objetivo geral elaborar uma política de segurança seguindo a NBR ISO/IEC 27002:2005 para o laboratório de informática e a rede sem fio de uma Instituição de Ensino Superior. O estudo inicia alertando para a importância de executar a análise de risco em qualquer instituição antes de se elaborar a política de segurança. O autor ressalta que para o desenvolvimento de uma política de segurança é imprescindível o conhecimento das melhores práticas em segurança da informação utilizado no mercado, os padrões para discussão com a alta administração, a necessidade de metas organizacionais e a formalização dos procedimentos para interligá-los às políticas corporativas. Como metodologia foi utilizada uma entrevista com usuários de uma universidade para verificar o grau de satisfação com o uso da rede acadêmica (laboratórios de informática e rede sem fio). Após a coleta de dados e análise dos resultados, foi apresentada uma proposta de uma política de segurança com o objetivo de diminuir as vulnerabilidades presentes e os incidentes constatados na pesquisa. Como proposta inicial, a elaboração de uma política de segurança em consonância com normas, padrões e procedimentos que pudessem inibir a utilização dos recursos não acadêmicos, trouxe benefício ao departamento de

TI da instituição, diminuindo os incidentes de segurança e permitindo que ameaças e vulnerabilidades tivessem menor incidência de ocorrência.

2.5.11 Fatores críticos de sucesso em segurança da informação em um órgão da Administração Pública Federal (QUINTELLA e BRANCO, 2013).

Apresentado nos Anais do II Simpósio Internacional de Gestão de Projetos e I Simpósio Internacional de Inovação e Sustentabilidade, 2013. Apresenta como objetivo disponibilizar informações a um órgão da Administração Pública Federal que possam subsidiar o projeto de implantação de uma Política de Segurança da Informação e sua sustentabilidade. O artigo buscou identificar os Fatores Críticos de Sucesso (FCS) para a implantação de uma Politica de Segurança da Informação (PSI) em um órgão da Administração Pública Federal. Apesar de as “melhores práticas” em segurança da informação encontrarem-se normatizadas através da família de normas ISO/IEC 27000 (2005), os FCS variam de uma instituição para outra. O objetivo foi disponibilizar informações a um órgão da APF que possam subsidiar o projeto de implantação de uma política de segurança e sua sustentabilidade. A pesquisa está baseada nos estudos de Rockart (1979) sobre as dimensões dos FCS. A elaboração dos FCS foi baseada nos prognósticos de Porter (1986), deduzidos dos estágios do ciclo de vida dos produtos, os quais foram parcialmente validados por um questionário estruturado aplicado aos gestores e demais servidores do órgão da APF. A metodologia utilizada foi baseada no método hipotético-dedutivo de Popper e os resultados encontrados apontaram os FCS para a implantação da política de segurança.

2.6 SÍNTESE DO CAPÍTULO

Em síntese este capítulo abordou os principais conceitos pertinentes as boas práticas de segurança da informação, gerenciamento de Riscos os conceitos de risco, ameaça, vulnerabilidade, impacto e ativos. Além disso, apresentou os modelos sobre gestão de riscos utilizados na comunidade internacional como: ISO 27002 o OSSTMM, ISSAF, PTES E NIST 800-30. Esse é essencial para que se possa aprimorar os conhecimentos sobre gestão de riscos e demonstrar a importância do tema para as organizações que buscam uma segurança da informação eficaz e eficiente.

Este capítulo também abordou o levantamento de suas auditorias pelo TCU relevantes a incidentes de segurança relacionados a gestão de TI. Também abordou

os procedimentos da revisão sistemática da literatura, desde as fases iniciais de planejamento, passando pela execução até a análise e divulgação dos dados. Ao final do capítulo foi apresentado o resumo dos 11 artigos considerados relevantes para este trabalho. Tais artigos foram obtidos das bases ACM, IEEE Xplore, Science Direct, Google Academic e Scopus. Os artigos selecionados através da revisão sistemática apontam as diversas metodologias, normas e modelos de gestão de riscos, pois foram importantes para a conslidação do guia de mitigação de riscos em TI. Através da leitura crítica dos 11 (onze) artigos selecionados através da revisão sistemática, definiu-se que a gestão de riscos é um fator de suma importância para as organizações que pretendem alcançar a segurança da informação e uma governança de TI efetiva e eficaz.

3 ESTUDO DE CAMPO

Este capítulo apresenta os dados estatísticos e a discussão acerca das informações coletadas através da realização do estudo de campo, aplicado com gestores dos Institutos Federais de Educação, Ciência e Tecnologia, tendo como objetivo identificar o estado atual da gestão de riscos de TI.

3.1 CARACTERIZAÇÃO DOS IFE

Os Institutos Federais de Educação, Ciência e Tecnologia foram propostos pelo MEC em 2007 (Decreto Nº.095/2007), pela lei nº 11.892, de 29 de dezembro de 2008, foi instituída a Rede Federal de Educação Profissional, Científica e Tecnológica, criando os Institutos Federais de Educação, Ciência e Tecnologia, e deu outras providências. Tal Decreto, em seu Art. 2º, define os IFEs como: instituições de educação superior, básica e profissional, pluricurriculares e multicampi, especializados na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas, nos termos desta Lei.

O próprio MEC admite que tais instituições não são propriamente “novas”, pois foram organizadas a partir da integração de duas ou mais instituições federais de educação profissional de um mesmo estado, ou da transformação de Centros Federais de Educação Tecnológica, de Escolas Técnicas Federais e de Escolas Técnicas vinculadas a Universidades Federais (AMORIM, 2013).

Atualmente, existem 605 campi em funcionamento em todo o Brasil, que integram 38 Institutos Federais, 02 Centros Federais de Educação Tecnológica (CEFETs) e o Colégio Pedro II (MEC, 2016). Maiores detalhes sobre as instituições e seus campi, podem ser consultados em: http://redefederal.mec.gov.br.

Os Institutos Federais são instituições que atuam na oferta da educação profissional e tecnológica, em todos os seus níveis e modalidades, formando e qualificando cidadãos com vistas à atuação nos diversos setores da economia, com ênfase no desenvolvimento socioeconômico local, regional e nacional. Representam centros de excelência ao atuarem desde o ensino técnico de nível médio até a pós-graduação, no desenvolvimento de programas de extensão, divulgação científica e tecnológica, além de realizar e estimular a pesquisa aplicada, a produção cultural, o empreendedorismo e o cooperativismo (MEC, 2016). A elaboração e atualização regular do Plano Diretor de Tecnologia da Informação PDTI pelos órgãos federais é uma orientação estabelecida no âmbito do SISP, também é recomendado que se faça e atualize periodicamente o

Plano de Desenvolvimento Institucional (PDI) e institua o Comitê Gestor de Tecnologia da Informação (CGTI), buscando alinhamento estratégico com a Alta Administração. Vale ressaltar que os IFE são similares, mas não iguais em sua organização.

3.2 INSTRUMENTO DE PESQUISA

A técnica utilizada para a coleta de dados dessa pesquisa foi o questionário em formato eletrônico. Segundo GIL (2010), essa técnica constitui o meio mais rápido e barato de obtenção de informações, além de não exigir treinamento de pessoal e garantir o anonimato. Considerando o universo da pesquisa e sua localização geográfica (estendendo-se a todos os estados brasileiros), o questionário foi disponibilizado por meio eletrônico, através do Google Formulários destinado aos gestores de TI dos Institutos Federais de Educação, possibilitando que esta pesquisa estivesse em conformidade com o escopo deste trabalho.

Com estas seções adotadas, conseguiu-se separar o escopo que representa cada pergunta, proporcionando uma pesquisa bem alinhada com os aspectos envolvidos em uma proposta de implantação do processo de Gerenciamento de riscos de TI.

Para confecção do formulário, adotou-se uma escala que facilitou o colaborador a responder de acordo com o nível de concordância. Para isso, foi adotada a escala Likert, que é considerada um tipo de escala de resposta psicométrica, usada habitualmente em questionários, sendo a mais usada em pesquisas de opinião. Ao responderem a um questionário baseado nesta escala, os respondentes especificam seu nível de concordância com uma afirmação. O formato típico da escala adotada é o seguinte (MATTAR, 2013):

1 - Discordo Totalmente;

2 - Discordo Parcialmente;

3 - Nem Concordo nem Discordo;

4 - Concordo Parcialmente;

5 - Concordo Plenamente.

Após o questionário ter sido respondido, cada item pôde ser analisado separadamente ou, em alguns casos, as respostas dadas puderam ser somadas para criar um resultado por grupo de itens (BACKER, 1995) e (OLIVEIRA, 2005).

3.2.1 Aplicação da Pesquisa e Coleta

Para aplicação da pesquisa, foi necessário que o questionário fosse avaliado por profissionais da área de segurança da informação na fase de pré-teste. Gil (2010) relata que o pré-teste não pode trazer nenhum resultado referente aos objetivos da pesquisa, porém está centrado na avaliação do instrumento que se aplica, visando que afira exatamente o que pretende alcançar.

A primeira etapa da pesquisa para aplicação do questionário, na fase de avaliação, se deu pela seleção de indivíduos pertencentes ao grupo de profissionais em Ciência da Computação das IFE que se pretendia estudar. Para isso, foi enviado uma mensagem eletrônica para Analistas e Técnicos em TI com experiência em Segurança da Informação, com o intuito de responder ao questionário inicial, avaliando aspectos quanto a:

Clareza e precisão dos termos: os termos técnicos utilizados necessitam de explicações adicionais?

- Quantidade de perguntas: o número de perguntas é excessivo, traz cansaço ou torna o entrevistado impaciente ?

- Formas e sequência de perguntas: as perguntas seguem um roteiro e sequência lógica sobre o problema apresentado e os objetivos a serem alcançados ?

- Percepção do entrevistado: o questionário pode apresentar outras perguntas ao conteúdo apresentado que não fazem parte do grupo de perguntas ?

Assim, foram solicitadas aos entrevistados informações a respeito do conteúdo do questionário inicial quanto às dificuldades encontradas para respondê-las, como também sugestões para melhorias no conteúdo apresentado.

O questionário de avaliação ficou disponível entre o período de 17/02/2017 a 27/02/2017. Nessa fase, foram recebidas oito respostas de profissionais de Tecnologia da Informação das IFE em que a amostra selecionada contribuiu para avaliar e fazer os ajustes para o questionário final.

A aplicação da segunda etapa do questionário aconteceu por meio do preenchimento de um formulário web, em que cada participante respondeu a um total de 24 perguntas. Cada participante da pesquisa foi contatado, inicialmente, através de um e-mail, sendo que este contato foi refeito por meio de telefonemas, no intuito de reforçar o convite a responder ao questionário. No e-mail, constavam orientações com os procedimentos a serem seguidos para preenchimento do questionário. O questionário ficou disponível para preenchimento entre 01/03/2017 a 31/03/2017, período em que a amostra selecionada contribuiu para alcançar o objetivo da pesquisa. A relação das perguntas do questionário podem ser vistas no Quadro 3.1. No quadro 3 segue a

relação do questionário aplicado após a reformulação das perguntas e ajustes na fase pré-teste.

Quadro 7 – Questionário pré-teste reformulado
Fonte: autor

N.	Pergunta
Q1	Informe a sigla da sua instituição.
Q2	Selecione o seu cargo/função na sua instituição.
Q3	Há quanto tempo você trabalha no cargo/ função?
Q4	A minha instituição investe e apoia implantação de Gestão de TI ?
Q5	Na minha instituição existe um Plano Diretor de Tecnologia da Informação (PDTI) ?
Q6	Na minha instituição existe um Comitê Gestor de Tecnologia da Informação (CGTI) ou similar ?
Q7	Na minha instituição existe uma coordenação ou núcleo de segurança em infraestrutura de TI ?
Q8	A minha instituição dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização ?
Q9	O instituto define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto ?
Q10	O instituto define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI ?
Q11	Meu instituto toma decisões estratégicas considerando os níveis de risco de TI definidos ?
Q12	Há quanto tempo o ativo (ex: hardware, software...) de informação está em operação ?
Q13	Considerando o tempo de existência do ativo de informação, é possível classificá-lo como um alvo:
Q14	O ativo de informação está localizado em área:
Q15	O ativo de informação está sob uma plataforma tecnológica com característica:
Q16	Caso exista histórico, que incidentes já comprometeram o ativo de informação no passado ?
Q17	A minha instituição faz uso ou tem implantado algum tipo de serviço de gerenciamento de Risco em TI (Nmap, Nessus, OpenVAS...) ?
Q18	Em caso afirmativo, esse gerenciamento de Risco em TI está baseada em uma das normas/metodologias (ABNT NBR ISO/IEC 31000:2009, ABNT NBR ISO/IEC 27002:2013, NIST SP800-30, OSSTMM, ISSAF...) ?
Q19	A minha instituição executa processo de monitoramento do uso dos recursos de TI com objetivo de detectar atividades não autorizadas ?
Q20	A minha instituição executa o processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos ?
Q21	Todos os incidentes são registrados e classificados quanto ao risco (alta, média, baixa probabilidade de um evento ocorrer.) ?
Q22	Minha instituição realiza periodicamente a auditoria em TI ?
Q23	Na minha instituição a equipe técnica possui treinamento periódico em auditoria de TI ?
Q24	A minha instituição possui um contrato de terceiros com auditoria em TI ?

3.3 DEFINIÇÃO DA POPULAÇÃO E AMOSTRA

Para a definição da população escolhida na pesquisa foram os Gestores de TI (reitores e diretores de TI) dos IFE. E para a caracterização do perfil das instituições referente ao Gerenciamento de Incidentes de TI, foi necessário utilizar o método de amostragem com uma pequena parte dos elementos que compõe o universo. ”Quando essa amostra é rigorosamente selecionada, os resultados obtidos na pesquisa tendem a aproximar-se bastante dos que seriam obtidos caso fosse possível pesquisar todos os elementos do universo” (GIL, 2010), p.109.

Para esse estudo foi utilizado o tipo de amostra Probabilística Casual Simples, na qua “cada elemento da população tem oportunidade igual de ser incluído na amostra” KAUARK; MANHÃES; MEDEIROS (2010), p. 62. Com o auxílio de procedimentos

estatísticos, tornou-se possível calcular a margem de segurança dos resultados obtidos. O estudo considerou o cálculo da Amostra Finita com uma população de pesquisa inferior a 100 IFE, considerando que no MEC existem 38 Institutos Federais de Educação, 02 Centros de Educação Federal de Ensino Tecnológica e 01 Colégio Pedro II, totalizando assim 41 IFE (MEC, 2016). Para o cálculo da Amostra Finita, utilizou-se a seguinte fórmula de acordo com a figura 3.1.

Figura 15 – Fórmula para cálculo de amostra finita
Fonte: adaptado de GIL (2010)

$$n = \frac{\sigma^2.p.q.N}{e^2(N-1) + \sigma^2.p.q}$$

Essa fórmula, é composta por:

^2 = nível de confiança escolhido, expresso em número de desvios-padrão;

p = percentual com o qual o fenômeno se verifica;

q = percentual complementar (100 – p);

N = tamanho da população;

e^2 = erro máximo permitido;

n = tamanho da amostra.

Substituindo os valores na fórmula apresentada na Figura 3.1 , foi estabelecido que o percentual com o qual o fenômeno se verifica seja por volta de 3,0%, portanto, p é igual a 100 – 3, ou seja, 97. Em seguida, tamanho da população de 41, adotou-se um nível de confiança de 95,5% (o correspondente a dois desvios-padrão) e um erro máximo de 3,0%. Substituindo os valores do cálculo da amostra finita, obtêm-se o resultado apresentado na Figura 4.2. Tendo como base a fórmula apresentada, observou-se a necessidade de aproximadamente 31 respondentes, representando uma população de 41 Institutos Federais de Educação. Essa amostra foi necessária para que a pesquisa tivesse um nível de confiança aceitável. Obteve-se um número superior ao esperado de 48 IFE respondentes de acordo com a figura 3.2:

Figura 16 – Cálculo da amostra finita
Fonte: Autor, adaptado de Gil (2009)

$$x = \frac{2^2 . 3 . 97 . 41}{3^2 . (41 - 1) + 2^2 . 3 . 97} = \frac{47724}{1541} = 31{,}31$$

3.4 SELEÇÃO E ORGANIZAÇÃO DOS DADOS

No período de recebimento das respostas (01/03 a 31/03/2017), por meio do questionário eletrônico, foi possível perceber algumas informações duplicadas e/ou incompletas. Após o encerramento do questionário, iniciou-se o processo de seleção das respostas recebidas, o que diminuiu o número de respostas válidas (completas) a serem analisadas. GIL (2010) p. 113, diz que ”é necessário também, à medida que os dados sejam agrupados, examiná-los para verificar se estão completos, claros, coerente e precisos”. Quanto à participação dos Institutos tivemos 48 respondentes. Entretanto, após finalizar o período de preenchimento do questionário, 10 dessas respostas foram desconsideradas ao analisar inconsistências nas mesmas (inconsistências ou duplicidades), sendo selecionadas 38 respostas válidas (completas), permitindo o não comprometimento da etapa posterior de análise dos dados.conforme a Figura 3.3.

Figura 17 – Respostas da pesquisa de campo
Fonte: Autor

Institutos Respondentes			
Respostas			
Completas	**Inconsistentes**	**Duplicadas**	**Total**
38	3	7	48

3.5 ANÁLISE E INTERPRETAÇÃO DOS DADOS

Para realizar a análise e a interpretação dos dados utilizou-se a técnica de estatística descritiva, cuja essência consiste no recolhimento, na análise e na interpretação dos dados através da criação de instrumentos adequados, tais como gráficos, quadros

e tabelas com indicadores numéricos LAKATOS; MARCONI (2009). Visando analisar os resultados, por meio de uma abordagem quantitativa para estabelecer o Ranking Médio (RM) das respostas do questionário, que utilizou a escala tipo Likert de 5 pontos, com vistas a mensurar o grau de concordância ou discordância dos respondentes do questionário. O RM se baseia nas propostas de (MALHOTRA, 2012),(TRESCA; DE ROSE JÚNIOR, 2000), (CASSIANO, 2005) e (OLIVEIRA, 2005).

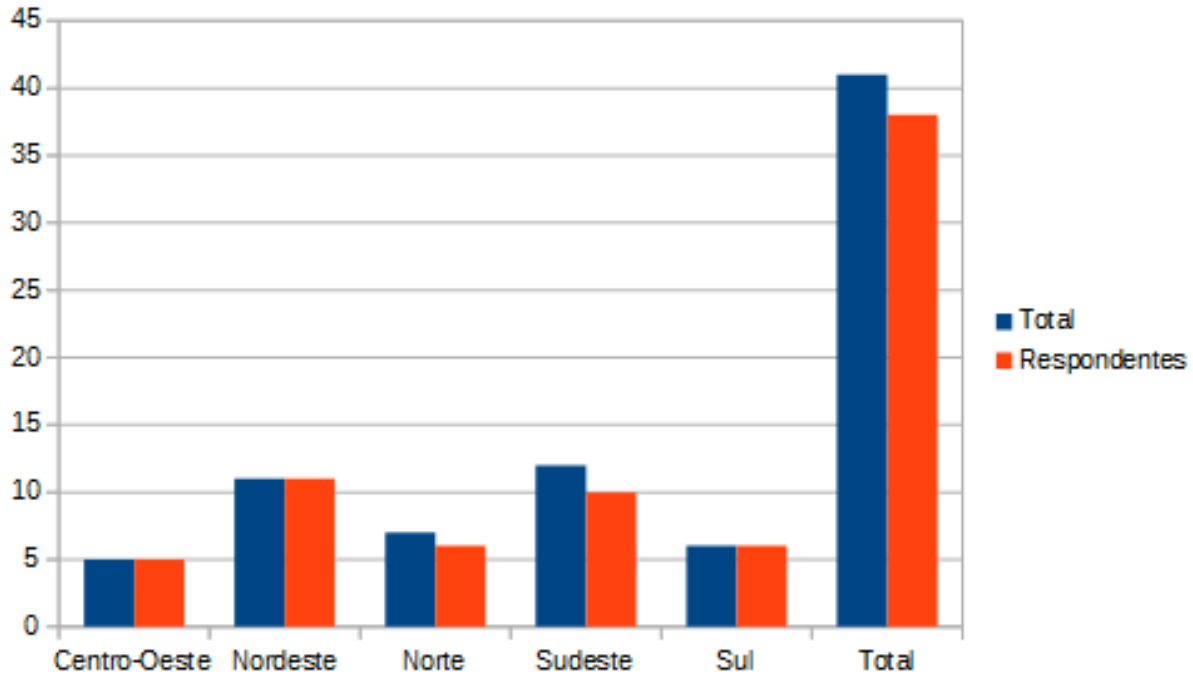
Através da obtenção do RM, a pontuação atribuída às respostas, relacionando a frequência das respostas dos respondentes à quantidade de vezes em aparecem nos questionários, os valores menores que 3 são considerados como discordantes e, os maiores que 3, como concordantes, considerando uma escala de 5 pontos. O valor exatamente 3 foi considerado “indiferente” ou “sem opinião“, sendo o ”ponto neutro“, equivalente aos casos em que os respondentes deixaram em branco ou responderam (OLIVEIRA, 2005).

A análise foi realizada com base nas respostas do questionário, cujo objetivo foi identificar o estado atual do nível de adoção do Gerenciamento de Incidentes de TI, nos Institutos Federais de Educação, Ciência e Tecnologia. Os resultados dessa pesquisa de campo buscou justificar a elaboração do Guia de Gestão de Riscos em Incidentes de TI, baseado nas boas práticas da ISO 27002/20013, OSSTMM, ISSAF, PTES E NIST. Para melhor compreensão da análise exploratória, as 24 perguntas abordadas no questionário da pesquisa de campo foram identificadas durante a análise como pergunta (Q1) à pergunta (Q24).

3.5.1 Identificação dos Institutos

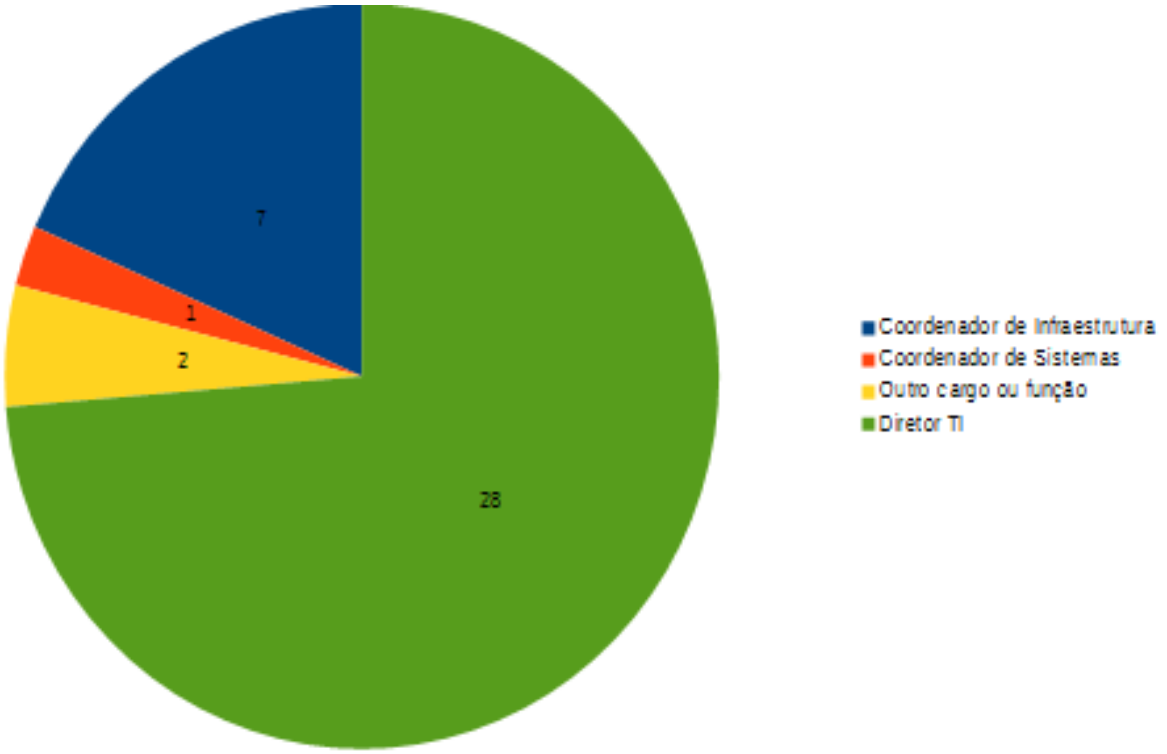
O estudo contemplou o total de 41 Institutos Federais de Educação do Brasil. Conforme se pode observar no gráfico da figura 3.4, a questão 1 foi solicitada a identificação da instituição do respondente da pesquisa. Do universo da pesquisa, tivemos resposta no questionário de 92,68% dos institutos, de um total de 38 Institutos Federais de Educação.

Figura 18 – Respondentes por região



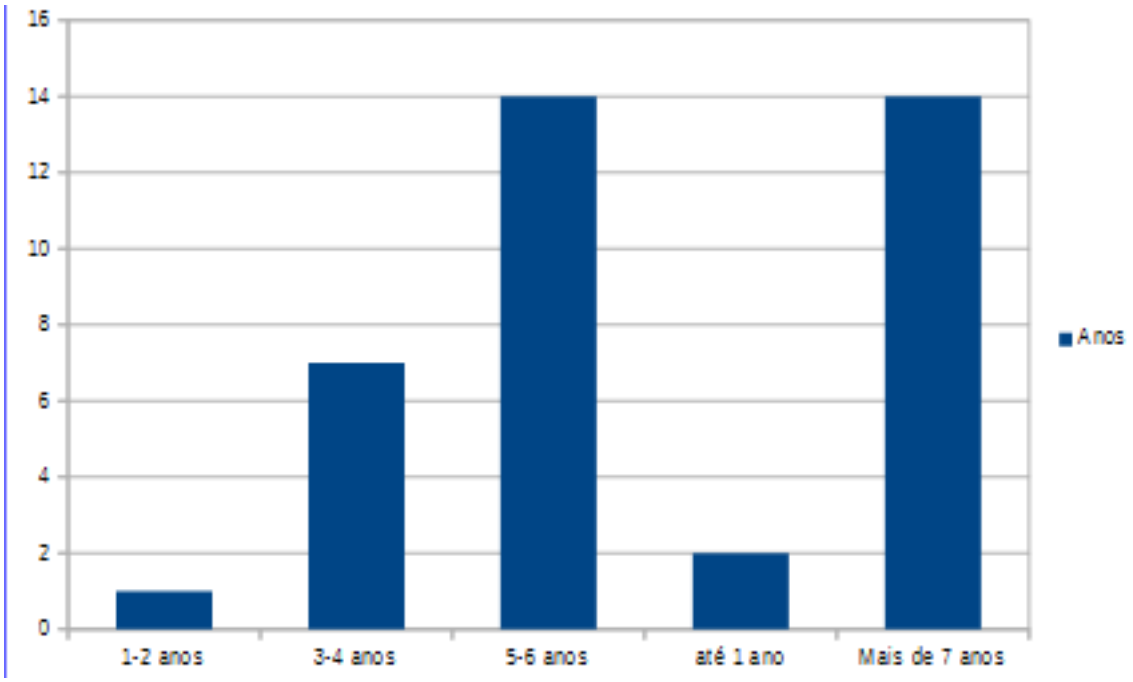
Na Pergunta 2 do questionário foi solicitada a identificação do respondente quanto ao cargo ou à função que exerce na instituição. Por meio de um questionário, 73,68% (28 respostas) e 5,26% (2 respondentes) representados por outro cargo ou função.

Figura 19 – Identificação dos cargos



Na Pergunta 3, trata-se do tempo no cargo ou na função, 73,68% dos respondentes informaram ter mais de 5 anos em relação ao tempo no cargo ou função, reforçando que a maior parte destes gestores de TI, atuam há mais de cinco anos na gestão de seus órgãos na APF, demonstrando que já possuem experiência e conhecimento relacionado às principais atribuições e competências exigidas neste cargo de gestão ocupada na APF.

Figura 20 – Tempo no cargo



3.5.2 Liderança da Alta Administração e Gerenciamento de Riscos em TI

Quando questionados a questão 4, sobre investimento e apoio da implantação de gestão de TI na instituição, conforme Figura 3.7 , 21 dos respondentes disseram que concordam parcialmente ou totalmente, o ranking médio calculado é de 3,49, média de 55%. Na Pergunta 7, questiona-se se na instituição existe uma coordenação ou núcleo de segurança de TI, o resultado demonstra que 70% dos respondentes discordam e/ou ficam neutros em relação à pergunta, equivalente a RM 2,68. Em relação à Pergunta 11 se a instituição realiza ações que visam promover a implantação de processos para a continuidade das atividades, para a qualidade dos serviços e tomada de decisões, tem-se RM de 2,5, sendo que 13 dos respondentes ficaram neutros, mas 16% deles concordaram. Quanto à Pergunta 23: Se a instituição investe em treinamento e consultoria, visando implementar o gerenciamento de auditoria de TI, o resultado RM foi de 1.79, sendo 16% do respondentes neutro e 0% concordantes, conforme RM apresentado na Figura 3.7 .

Figura 21 – Apoio da alta administração

Questões	Respostas						
	1	2	3	4	5	MP	RM
4. A minha instituição investe e apoia implantação de Gestão de TI.	1	4	12	16	5	129	3,49
7. Na minha instituição existe uma coordenação ou núcleo de segurança em infraestrutura de TI.	9	8	10	6	5	99	2,68
11.Meu instituto toma decisões estratégicas considerando os níveis de risco de TI definidos.	7	11	13	6	1	90	2,5
23.Na minha instituição a equipe técnica possui treinamento periódico em auditoria de TI.	16	15	6	1	0	68	1,79

Segundo ANDRADE A.; ROSSETTI (2004), a eficácia na gestão de TI poderá ser atingida se toda a organização, e não só a alta liderança, perceber a importância da área na transformação das empresas. Os resultados da presente pesquisa demostraram que o apoio nos Institutos Federias de Educação ainda não é o ideal, 55% dos respondentes concordaram.

Com isso, as respostas às perguntas seguintes da Figura 3.7, são consequência dessa falta de apoio, desdobradas em ações como falta de criação de coordenação específica e de apoio à capacitação dos servidores. A falta de apoio e investimentos da Alta Administração (reitores e diretores de TI) no quesito da gestão de TI pode ser considerado um dos fatores preponderantes para a baixa adoção de gestão de TI na APF, incluindo a gestão de risco. Na visão de CAVALCANTI FILHO et al. (2011), o aspecto crítico para que se garanta esses resultados é a participação da alta gerência em todo o processo, principalmente na identificação de indicadores necessários para essas avaliações.

3.5.3 Implantação para o processo de mitigação de riscos de TI

Conforme a questão 8, 76,31% dos Institutos Federais de Educação possuem uma diretriz representados por especialistas da área de TI, porém 81,57% dessas instituções não definem especificamente essas diretrizes conforme a questão 9. Por fim 84,21% não definem a gestão de riscos de TI.

Figura 22 – Apoio nos processos de riscos

Questões	Respostas						
	1	2	3	4	5	MP	RM
8. A minha instituição dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização.	0	6	3	14	15	152	4
9.O instituto define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto.	9	9	13	5	2	96	2,53
10.O instituto define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI.	10	11	11	5	1	90	2,37

Conforme relatório do acórdão 3117/2014-TCU, para que a TI seja bem governada, entre as condições que devem ser satisfeitas, está, definir e estabelecer processos para implementar as políticas e entregar os resultados esperados, bem como para garantir a continuidade das ações, inclui-se dentre os processos o gerenciamento de problema (TCU, 2014a). De acordo com o Acórdão 1.603/08 TCU (2008) não está explícita a necessidade de uma Central de Serviços, mas consegue-se perceber que é necessária a existência de uma infraestrutura adequada para tratar de incidentes, eventos de segurança, capacidade e mudanças que ocorrem nos serviços de TI da organização, impulsionando assim a criação de uma estrutura organizacional que seja responsável pela gestão dos serviços.

Pode-se elencar como atividades do gerenciamento de riscos (FREITAS, 2010), p. 283-285:

Detecção e Registro do Problema: análise de incidentes recorrentes ou incidentes não identificados pela Central de Serviços ou pelo Gerenciamento de Incidentes. Todos os problemas devem conter informações importantes para o atendimento do problema e, quando partir de um registro de incidentes, o problema deve herdar as informações relevantes do registro de incidentes como todo o histórico anterior;

Categorização do Problema: os problemas devem ser categorizados da mesma forma que os incidentes, podendo ser categorizados em grupos como: hardware, software, rede, etc;

Priorização do Problema: a priorização dos problemas ocorre da mesma forma que os incidentes;

3.5.4 Recomendações do SISP

Quando questionados sobre a questão 5, se existe PDTI na sua instituição, percebe-se um alto grau de concordância (92%), o equivalente a RM de 4,58. Ao serem indagados se existe um comitê de TI ou similar na questão 6, o resultado foi próximo com RM de 4,32, conforme apresentados na Figura 3.9.

Figura 23 – Apoio da alta administração baseado no SISP

Questões	Respostas						
	1	2	3	4	5	MP	RM
5.Na minha instituição existe um Plano Diretor de Tecnologia da Informação (PDTI).	0	0	3	10	25	174	4,58
6.Na minha instituição existe um Comitê Gestor de Tecnologia da Informação (CGTI) ou similar.	0	4	3	8	23	164	4,32

Os resultados apresentados na figura 3.9 demonstram que as instituições têm atendido às recomendações referentes à elaboração do PDTI e, ainda, tem criado os Comitês de TI, conforme recomenda o SISP. Conforme o acórdão 3117/2014-TCU, observa-se também uma situação de evolução com relação ao número de organizações que dispõem de comitê de TI, haja vista ter saltado de 72% em 2012 para 87% em 2014 (8% parcialmente e 79% integralmente) o percentual de organizações que declararam adotar a prática. Esse crescimento é observado, inclusive, quando a comparação é realizada apenas com as organizações que adotam integralmente a prática, tendo em vista a variação positiva de sete pontos percentuais (79% em 2014, contra 72% em 2012) (TCU, 2014a).

A elaboração e atualização periódica do PDTI pelos órgãos é uma orientação estabelecida no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), que agrega atividades de planejamento, coordenação, organi-

zação, operação, controle e supervisão dos recursos de dos órgãos e entidades da Administração Pública Federal (SLTI, 2015a).

O Comitê de TI é ainda, parte do sistema de Governança de TI e, por este motivo, de modo a cumprir seus objetivos, realiza as atividades básicas desta disciplina: direcionar, monitorar e avaliar a gestão de TI. É também um fórum de debates, negociações, tomada de decisões e resolução de problemas em relação aos assuntos de TI (SLTI, 2015a).

3.5.5 Cenário atual sobre o mapeamento de vulnerabilidades das IFE

A seguir é apresentado o cenário atual do mapeamento de vulnerabilidades das IFE, baseado nas respostas do questionário utilizado na pesquisa de campo.

Sobre a questão 17, apenas 29% fazem uso de algum recurso de monitoramento de rede com valor RM 2,71. Em relação a questão 18, este monitoramento está baseado em uma das normas/práticas com 1,57% com RM 2,29. Quanto ao processo de gerenciamento dessas vulnerabilidades sobre a questão 19, esses monitoramentos, cerca de 60% dos participantes não levam em conta as práticas citadas na questão anterior. Quanto a questão 20 em relação ao controle de segurança dos ativos da intituição 65,78% não realizam o processo de gestão dos mesmos com RM 3. Em relação ao controle desses ativos apenas 21% das instituições respondentes registram os incidentes classificando-os conforme a severidade na questão 21 com RM 2,5. Em relação a (questão 22) , 86,84% com RM 2,11 das instituições respondendes sequer realizam auditorias em seus ativos, resultado pela qual a falta de uma das adoções de práticas de gestão de risco conforme a questão 18. Sobre a adoção dessas auditorias (questão 24) em ativos nas instituições, apenas 2,63% dos respondentes fazem o uso de auditoria e controle de ativo com o menor RM de 1,47.

Figura 24 – Mapeamento de processo vulnerabilidades

Questões	Respostas						
	1	2	3	4	5	MP	RM
19.A minha instituição executa processo de monitoramento do uso dos recursos de TI com objetivo de detectar atividades não autorizadas.	2	9	12	13	2	118	3,11
20.A minha instituição executa o processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.	2	10	13	12	1	114	3
17.A minha instituição faz uso ou tem implantado algum tipo de serviço de gerenciamento de Risco em TI (Nmap, Nessus, OpenVAS…).	8	10	9	7	4	103	2,71
21.Todos os incidentes são registrados e classificados quanto ao risco (alta, média, baixa probabilidade de um evento ocorrer.)	9	10	11	7	1	95	2,5
18.Em caso afirmativo, esse gerenciamento de Risco em TI está baseada em uma das normas/metodologias (ABNT NBR ISO/IEC 31000:2009, ABNT NBR ISO/IEC 27002:2013, NIST SP800-30, OSSTMM, ISSAF...).	15	3	14	6	0	87	2,29
22.Minha instituição realiza periodicamente a auditoria em TI.	13	14	6	4	1	80	2,11
24.A minha instituição possui um contrato de terceiros com auditoria em TI.	25	9	3	1	0	56	1,47

Observa-se que na figura 3.10 que a adoção do gerenciamento de processos de TI ainda é muito baixa nos IFE, tem-se um resultado ainda mais baixo quando se analisa o processo de rerenciamento de riscos. Considerando ser uma recomendação aos órgãos pertencentes ao SISP e a ocorrência de levantamentos a cada dois anos pela Sefti/TCU, faz-se necessário avançar na adoção desses processos.

Nessa dimensão dos controles da gestão de processos em TI, que derivaram em sua maioria da jurisprudência do TCU, as normas técnicas, os guias e os modelos de boas práticas, avaliar o gerenciamento de riscos de TI da APF (TCU, 2014a). Motivo pelo qual esta pesquisa tem como essência as boas práticas recomendadas nas publicações ISO 27002, NIST, OSSTMM, PTES E ISSAF.

Percebe-se ainda, que muitos gestores ainda não identificam que práticas de gerenciamento de riscos de TI têm o objetivo de facilitar o controle dos recursos e os processos da área de TI. A complexidade da área é uma das possíveis razões do surgimento no mercado de melhores práticas, mas, sem consciência e convicção dos potenciais benefícios e sem conhecimento dos demais aspectos envolvidos, pode-se ter ainda mais complexidade sem um benefício significativo de gestão (LUCIANO; TESTA;

AZEVEDO BRAGAN, 2012).

ALBERTIN (2004) utiliza uma organização de fatores críticos de sucesso para a administração da informática, agrupando esses fatores em quatro categorias: fatores críticos da função planejamento, fatores críticos da função organização, fatores críticos da função pessoal, fatores críticos da função direção e fatores críticos da função controle exemplificados na figura 3.10 . Alguns dos instrumentos importantes para reforçar a Governança de TI nos órgãos setoriais e seccionais do SISP são um conjunto de instruções normativas, padrões e especificações geradas pela SLTI com o apoio da Comissão de Coordenação do SISP, outros que se alinham com os objetivos estratégicos são: o plano de capacitação e as portarias que regulam as matérias relativas ao provimento de cargos e gratificações no sistema, visto que a retenção de profissionais de TI na APF é considerada questão estratégica, principalmente em relação ao pessoal de nível gerencial (FERNANDES; DE ABREU, 2014).

A Gestão de Ativos é um tema de suma importância para a segurança da informação. Os ativos compõem os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada, os equipamentos em que são manuseados, transportados e descartados, isso demonstra a importância de uma gestão eficaz dos ativos (SÊMOLA, 2013).

A análise de ameaças também é um item importante para a Gestão de Riscos. As ameaças são eventos negativos que ocorrem quando uma vulnerabilidade ou fraqueza é explorada e que podem ter impacto nos objetivos do negócio, podendo resultar em perda, divulgação ou avaria de um ativo da organização ou é algo que terá um efeito adverso na organização. O objetivo da análise das ameaças é identificar as ameaças que tem o potencial para explorar as vulnerabilidades e afetar negativamente os ativos (CASACA, 2015).

O objetivo da análise de riscos é identificar e avaliar todos os riscos e sugerir um conjunto de controles que permitem reduzir os riscos para um nível aceitável (CASACA, 2014).

Para Tuyikeze e Flowerday (2014) a “avaliação de risco ajuda as organizações tomarem suas decisões sobre quais os riscos estão dispostos a aceitarem e aos quais se deve mitigar”. Eles descrevem cinco atividades que a organização precisa realizar

na análise de riscos, são elas:

- Identificar os ativos que devem ser protegidos;
- Listar todas as ameaças que podem causar danos aos ativos;
- Identificar em definitivo essas ameaças;
- Avaliar essas ameaças e suas vulnerabilidades e
- Identificar os controles que devem ser implementados a fim de mitigar os riscos encontrados.

Os resultados obtidos demonstram que poucas instituições realizam a comunicação e consulta dos riscos junto a alta administração, item esse fundamental em um processo de gestão de riscos. As figuras 3.11 a 3.15 demonstram de forma detalhada o resultado do questionamento realizado.

Figura 25 – Tempo do ativo em operação

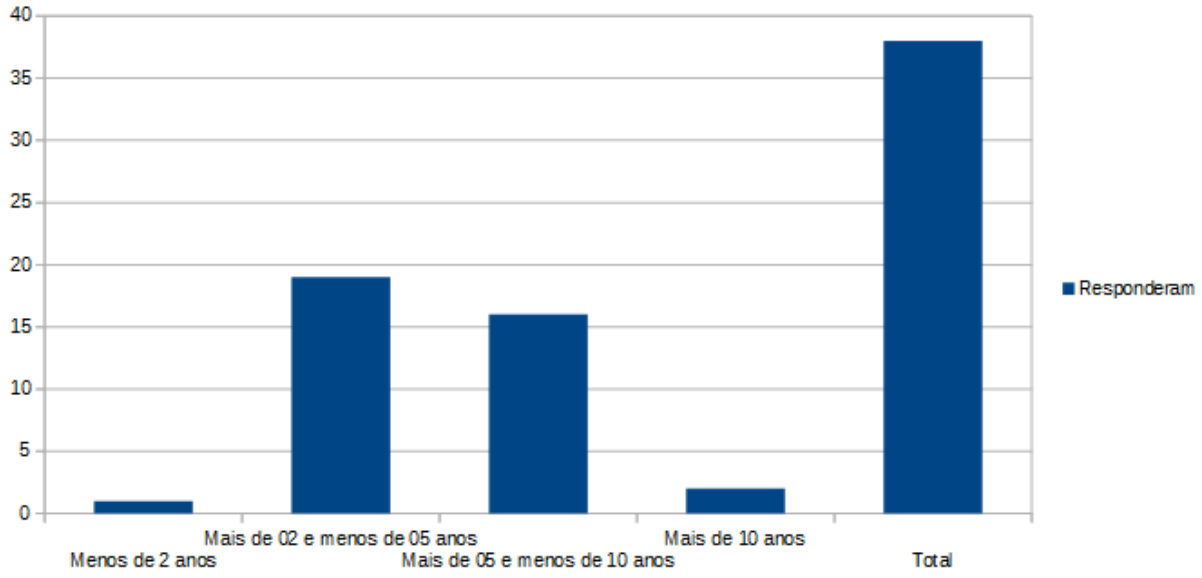


Figura 26 – Tipos de perdas do ativo

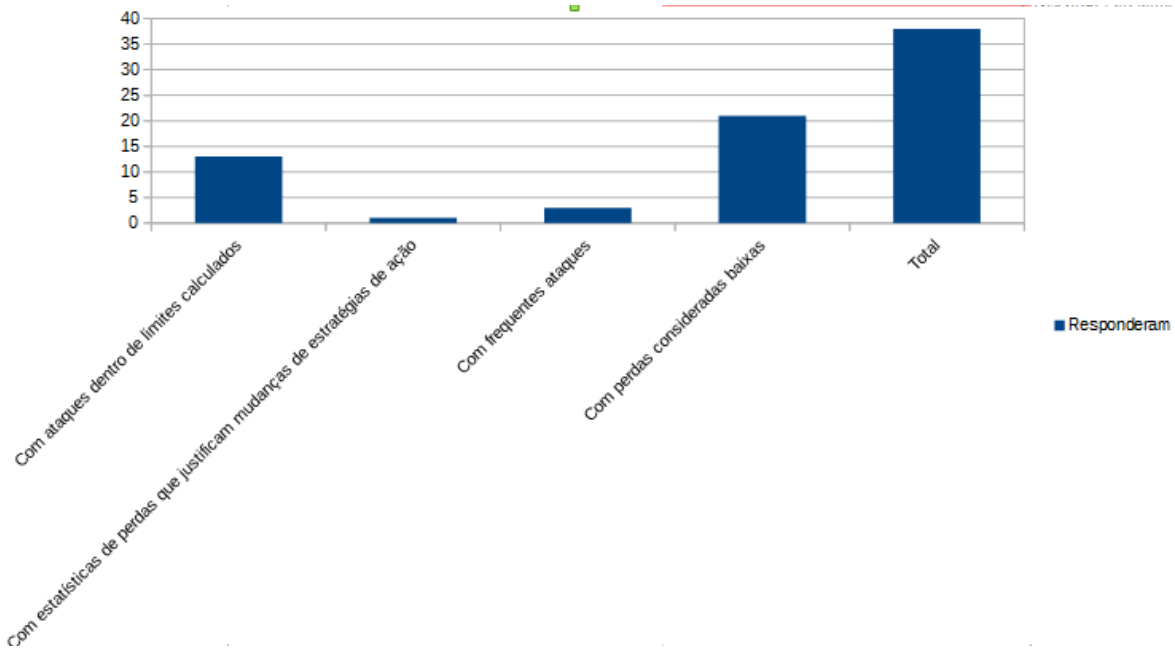


Figura 27 – Localização do ativo em risco

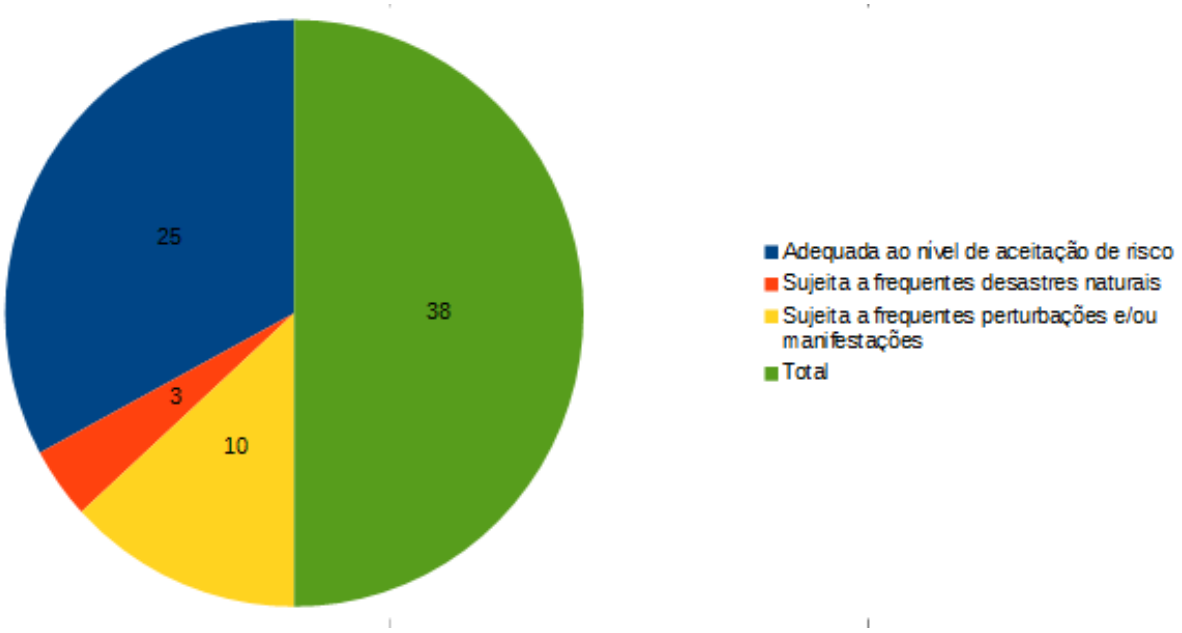


Figura 28 – Plataforma do ativo

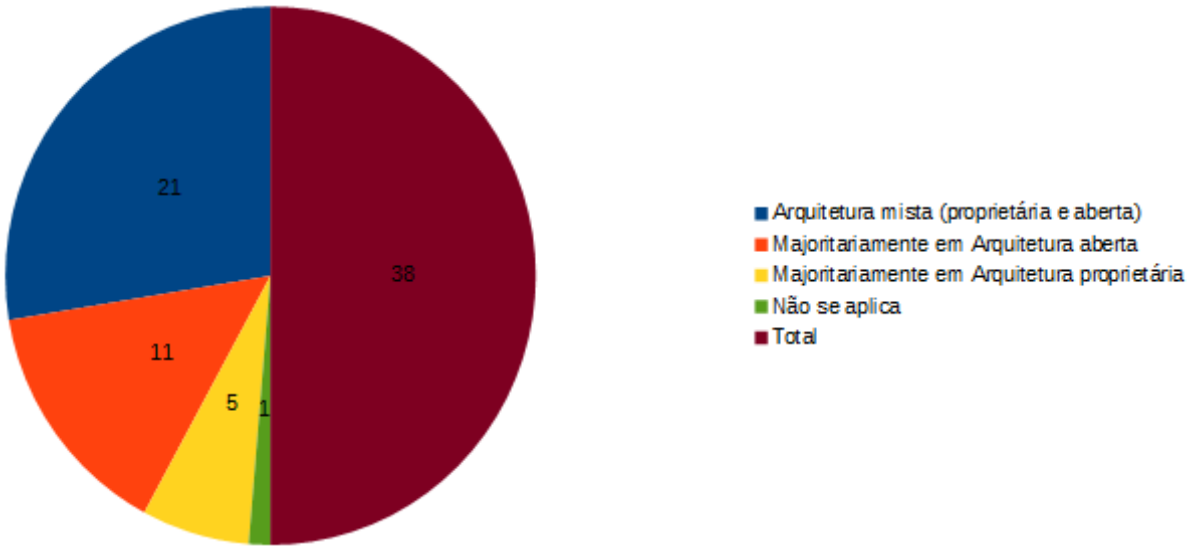
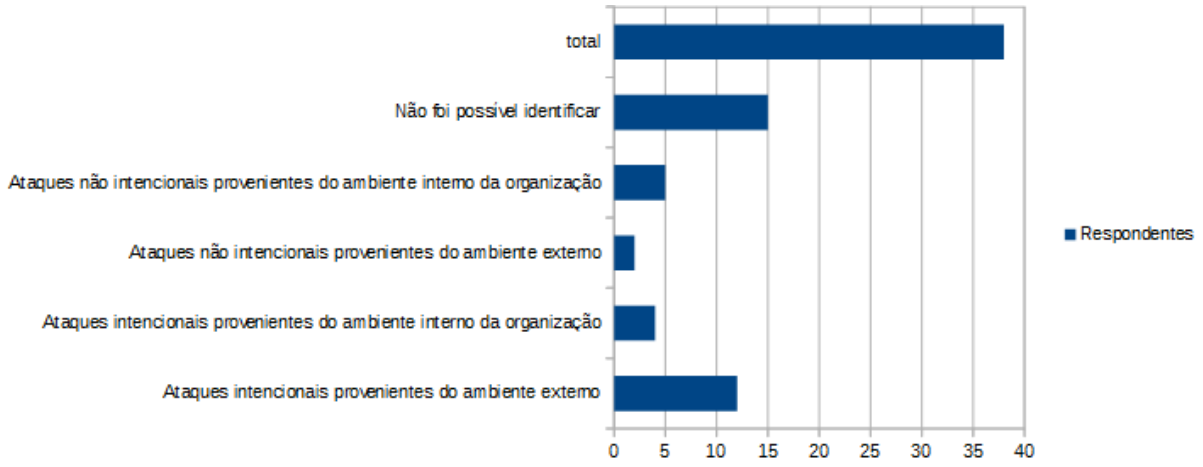


Figura 29 – Histórico de incidentes

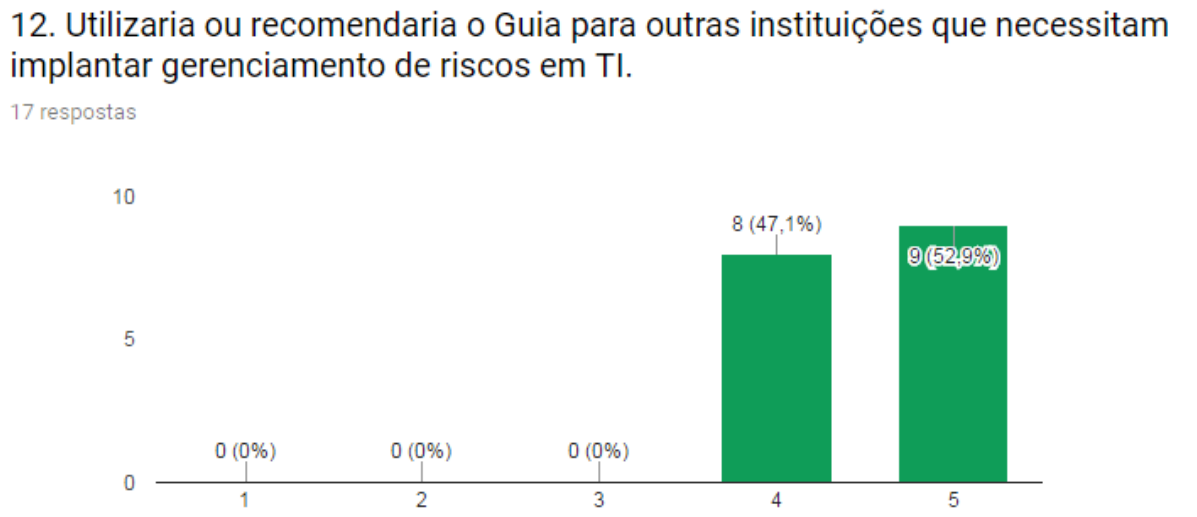


3.5.6 Processo de implantação do guia baseado no mapeamento de vulnerabilidades

Para identificar se seria viável a utilização de um guia de implantação com base nas melhores práticas da ISO 27002, OSSTMM, ISSAF, PTES E NIST , a pergunta opcional, no intuito de orientar e facilitar a implantação do processo de gerenciamento

de riscos na instituição, a figura 3.16, apresenta a visão geral de todos os participantes da pesquisa, quadro esse que justifica a produção do objeto de pesquisa deste estudo.

Figura 30 – Implantação do guia



3.6 SÍNTESE DO CAPÍTULO

Este capítulo teve como objetivo apresentar e caracterizar o campo de pesquisa, as técnicas utilizadas para alcançar o público alvo, a ferramenta utilizada e a definição da amostra. Apresentou-se a forma de seleção dos dados, bem como os critérios adotados para a sua organização, buscando levantar informações, consistentes para futuras análises. Ao longo do capítulo, elencaram-se informações sobre a análise e a interpretação dos resultados obtidos com a pesquisa nos institutos federais de educação localizados no território brasileiro com o objetivo de identificar o nível de adoção do guia. A partir desse levantamento verificou-se que apenas 1,57% das instituições pesquisadas se baseiam em normas internacionalmente utilizadas, comprovando a ausência de práticas relacionadas á área de gestão de riscos de TI. Outros fatores críticos apontados pelos especialistas é a falta da definição dos papéis de responsabilidades pela gestão de riscos com 84,21% , a falta de apoio da administração quanto a decisões estratégicas sobre os riscos com 81,57%, a falta de auditoria em gestão de riscos com 86,84% e a falta de definição e classificação quanto aos riscos com 78,49% e apenas 15,78% dos institutos pesquisados utilizam alguma prática de gestão baseada nas normas padrão recomendadas pelo SISP. Concluindo o capítulo, observou-se que

100% dos Institutos Federais de Educação concordariam na viabilidade de uso do guia para a mitigação de riscos de TI apresentado no capítulo seguinte.

4 PROPOSTA DO GUIA PARA IMPLANTAÇÃO

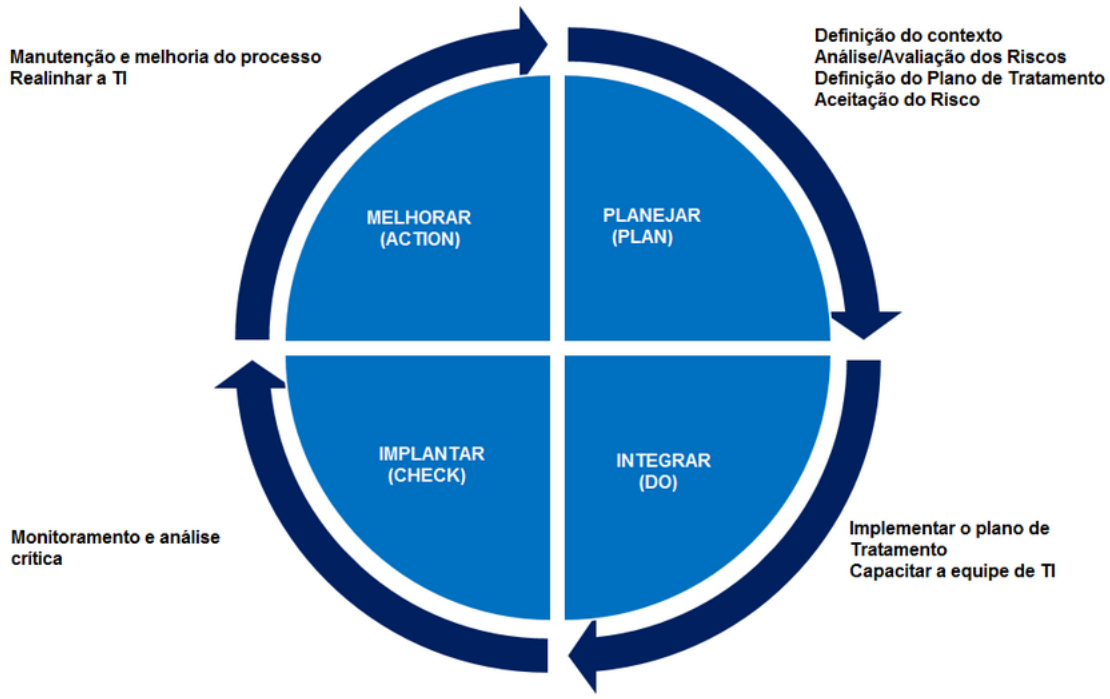
Este capítulo apresenta o guia de implantação proposto, tratando analítica e descritivamente das fases e atividades que compõe o escopo do trabalho envolvido na implantação do Guia de Melhores Práticas para Mitigação de Riscos em Incidentes de TI (GMRITI), buscando definir um processo com uma estrutura simplificada, sem, contudo, deixar de abordar conceitos definidos na literatura relacionada.

4.1 SOBRE O GUIA

4.2 FASES DA IMPLANTAÇÃO

Este Guia está fundamentado no ciclo PDCA com o intuito de executar todas as ações a que se propõe, estando o mesmo estruturado em quatros fases de implantação: Planejamento, Integração, Implantação e Melhoria, mostradas na Figura 4.1. As quatro fases-chave do PDCA são identificadas como: planejar, fazer, verificar e agir (em inglês plan, do, check, act – PDCA), após cada fase consolidada, é usado um círculo que promove a melhoria contínua dos Processos de Serviços de TI nas organizações, procurando a excelência das atividades desenvolvidas por seus usuários, de forma a produzir, executar, manter e melhorar de modo contínuo os seus processos. A consolidação das fases de implantação possibilita à instituição absorver as lições aprendidas em cada fase do PDCA, assegurando que o aperfeiçoamento continuará embutido no processo.

Figura 31 – Ciclo PDCA
Fonte: adaptado de CAMPOS (1992)



PLANEJAR: Sugere-se que nesta fase seja realizado e documentado o diagnóstico da situação atual, como levantamento de requisitos. Em seguida, inicie-se o cronograma de implantação, criação de plano de capacitação e reunião para garantir apoio da Alta Gestão (Diretores Gerais, Reitor e Pró-Reitores). Após tais ações, deve-se definir quais os meios necessários para se atingir os resultados esperados para a implantação do processo de gerenciamento de problema.

INTEGRAR: Nesta fase, teremos a execução do plano definido, a capacitação da equipe de TI, a definição do Catálogo de Serviços, a implantação da central de serviços e a integração com os outros processos de Gerenciamento de serviços de TI, caso já estejam implantados na instituição.

IMPLANTAR: Nesta terceira fase, é feita a análise e a preparação para implantação do processo e o monitoramento dessa implantação. Durante a análise é importante fazer a comparação dos resultados obtidos com os resultados estabelecidos na fase “planejar”, verificando se o trabalho está sendo feito conforme estabelecido e, em seguida, deve-se prosseguir com a implantação do processo.

MELHORAR: Nesta fase, as ações irão depender dos resultados obtidos através implantação, para analisar o que pode ser melhorado nos processos. Recomenda-se que se realinhe a TI com os objetivos definidos no PDTI da Instituição, bem como se realizem reuniões da equipe para identificação e aplicação de mudanças. Finalizando

esta etapa, deve-se voltar para a fase de planejamento para adequar as suas ações. Conforme indicado na figura 4.1, o PDCA é uma ferramenta cíclica, um processo contínuo de melhorias.

4.3 PAPÉIS E RESPONSABILIDADES

Conforme, SLTI (2015a) as atividades que devem ser executadas para se planejar e acompanhar a implantação são realizadas por pessoas ou grupos, aqui referenciados como papéis. Os papéis descrevem as entidades envolvidas nos processos, as quais têm a responsabilidade de executar alguma atividade durante o processo de implantação. Um papel possui um conjunto de atribuições e/ou responsabilidades sobre as atividades do processo, ou seja, representam as funções a serem desempenhadas pelos profissionais envolvidos. Vale ressaltar que um papel não identifica diretamente uma pessoa, já que um indivíduo pode desempenhar mais de um papel no processo, além de que pode haver situações em que um mesmo papel seja desempenhado por mais de uma pessoa. Isso também é importante para que os processos sejam independentes das pessoas, as quais podem sair da organização ou mudar de função. Para identificar os papéis envolvidos em cada ação, das fases de implantação do processo de GMRITI, foi utilizada a notação para modelagem de processos de negócio denominada Business Process Modeling Notation – BPMN. Notação utilizada no ePING como padrão de modelagem de processos do SISP (SLTI, 2015a). Na elaboração deste Guia, os papéis são apresentados e identificados durante processo de implantação. Entre eles, destacam-se os principais papéis e responsabilidades dos envolvidos, como se pode visualizar na Figura 4.2.

Figura 32 – Papéis e Responsabilidades
Fonte: autor

Papel	Responsabilidade
Alta Gestão	É o membro da alta gestão, autoridade máxima da instituição. Corresponde a reitores e diretores dos campi.
Coordenador de Gestão de TI	É o líder do projeto de implantação deve atuar para garantir a aplicação dos estágios para a implantação dos processos e direciona as iniciativas no sentido de alcançar os objetivos de implantação e posteriormente a aplicação das práticas do processo. Sugere-se que essas pessoas tenham ou adquiram conhecimento satisfatório em governança de TI, essencialmente em Gestão de Riscos.
Equipe de TI	É a equipe técnica responsável por alcançar os objetivos de cada estágio de implantação e posterior implementação desses processos.
Servidores em Geral	Pessoas de qualquer setor pertencente ao quadro de servidores dos Institutos Federais

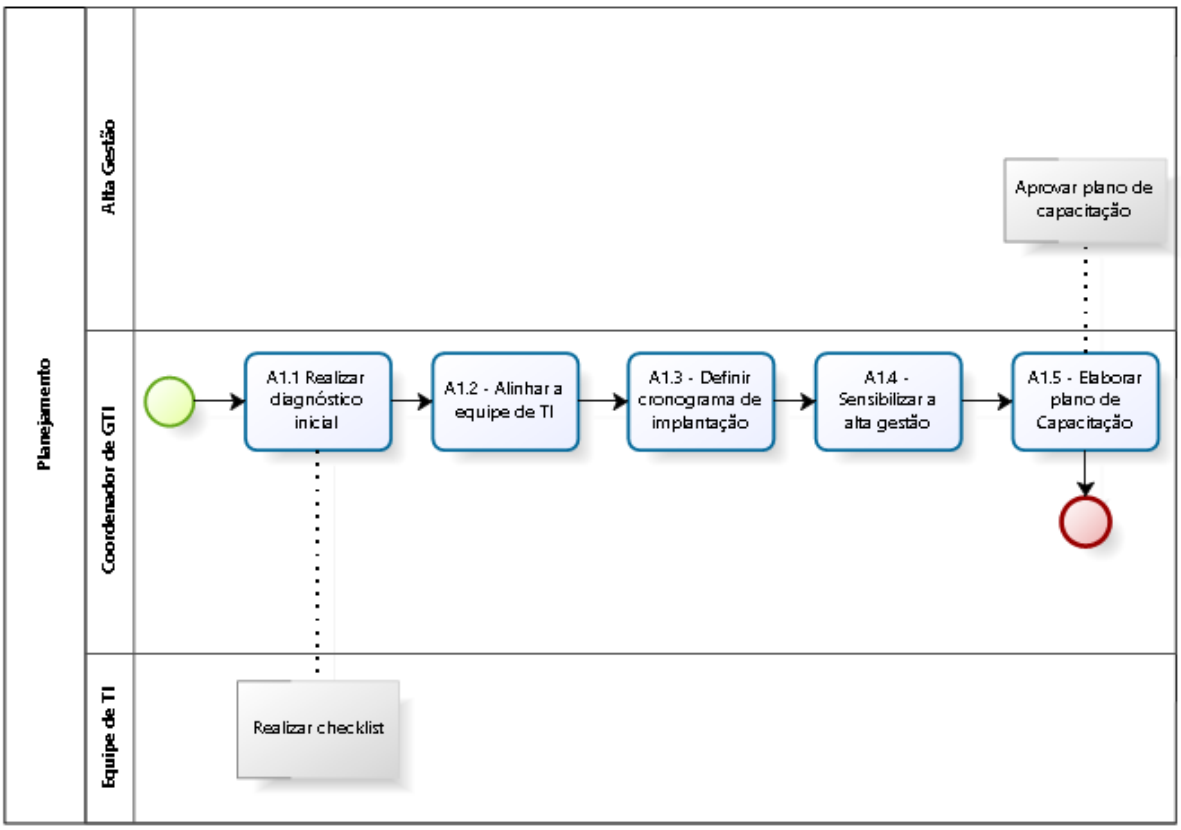
4.4 GUIA DE IMPLANTAÇÃO

Nesta seção apresenta-se o Guia de Implantação do GMRITI que contempla a descrição das fases e as ações, o seu objetivo e os passos a serem executados: as entradas necessárias, as ferramentas e técnicas, além dos resultados esperados. São descritos também as recomendações úteis para a realização de cada ação e o embasamento necessário para a sua criação, demonstrado pelos estudos realizados. Os quadros utilizados no Guia foram adaptados de Oliveira Júnior (2015) da sua proposta de implantação de Governança de TIC em Instituições Federais de Ensino.

4.4.1 Fase 1 – Planejamento

Para realizar a implantação de um processo com sucesso, devemos seguir alguns passos e tratar todo o processo de implantação como um projeto, é importante definir um cronograma, além de envolver a Alta Gestão desde o início. A seguir, são descritas as ações para esta fase de planejamento.

Figura 33 – Fase de Planejamento de implantação do GMRITI



Ação 1.1 Diagnóstico Inicial

O objetivo da ação de Diagnóstico Inicial é levantar a situação atual da instituição. Essa etapa é o alicerce para todo o processo de planejamento.

Figura 34 – Diagnóstico Inicial

FINALIDADE		
Diagnosticar a situação atual da instituição em relação ao processo de gerenciamento de riscos em TI através de checklist proposto por este guia, com o objetivo de identificar as ações que encontram-se realizadas em inciativas anteriores.		
ETAPAS		
1 – Reunião com a equipe de TI		
2 – Aplicação do checklist com a equipe de TI		
3 – Apurar o resultado da aplicação do checklist		
4 – Levantas as necessidades para a implantação		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Checklist de diagnóstico inicial para implantar o processo de gestão de riscos.	Ferramentas de criação de formulários (GOOGLE FORMS, 2017) ou similar	Relatório com diagnóstico inicial para a implantação do processo de gerenciamento de riscos.
RECOMENDAÇÕES		
Realizar o questionário na forma de checklist de acordo com o quadro 2. Este diagnóstico reflete se já existe alguma ação proposta neste guia. Para facilitar o checklist e apuração dos dados é viável a transformação desses em formato WEB.		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FERREIRA E ARAÚJO (2009); FONTES (2011, 2012); OGC (2007); OLIVEIRA JUNIOR (2015)].		

Para complementar a ação de Diagnóstico Inicial, recomenda-se a realização do *checklist* proposto na figura 4.5 que visa levantar o estado atual da instituição em termos de apoio, processos e ferramentas que subsidiarão o processo de implantação do GMRITI. Pode-se observar que esse *checklist* traz uma proposta simples, podendo ser revisado pela instituição.

Ação 1.2 Alinhar a TI ao Processo a ser Implantado

É fundamental que a ação alinhar a TI ao processo a ser implantado seja executada logo após a ação do diagnóstico inicial. Este alinhamento da equipe de TI é essencial para nivelar o conhecimento da equipe e encorajá-la na realização da implantação, além de colaborar para o entendimento da função de cada membro da equipe dentro do processo. OLIVEIRA JÚNIOR (2015) compreende que as prioridades devem ser acordadas mutuamente a partir da negociação das necessidades do negócio e da área de TI, já que o alinhamento evita que exista, na instituição, um suporte ineficaz da área de TI na consecução da missão da organização, evitando decisões incompatíveis com as suas necessidades.

Figura 35 – *Cheklist* inicial

Perguntas	**Existe**	**Não Existe**	**Não se Aplica**
Existe o apoio da alta administração quanto à gestão de riscos em TI ?			
Existem procedimentos definidos para reporte dos incidentes?			
Os incidentes de segurança comunicados são registrados?			
Os incidentes de segurança ocorridos são reportados a alguma área da instituição?			
São adotadas medidas pró-ativas para contenção dos incidentes conhecidos?			
Existem procedimentos para concessão de acesso as localidades críticas?			
As mudanças emergenciais são submetidas a aprovação da gerência de TI?			
São realizadas previsões, quanto ao crescimento do volume de operações que envolvam determinados recursos e a capacidade máxima suportada por este?			
O instituto possui um plano de contingência formalizado?			

Ação 1.3 Definir Cronograma de Implantação

Na ação definir cronograma de implantação, recomenda-se a elaboração do cronograma da implantação do processo do GMRITI, constando o período, atividades e os responsáveis.

Ação 1.4 Sensibilizar a Alta Gestão

A etapa de sensibilização da Alta Gestão é muito importante para o sucesso de implantação do processo do GMRITI. Para FERNANDES; DE ABREU (2014), esta sensibilização é crucial, já que o apoio da Alta Administração é primordial no alcance de sucesso em qualquer iniciativa desta natureza. Conforme recomendação do TCU (2014b), com base nas boas práticas contidas no Código das Melhores Práticas de Governança Corporativa do IBGC, deve-se sensibilizar os membros da Alta Administração acerca de sua responsabilidade no tocante a estabelecer e monitorar as políticas corporativas da entidade, a exemplo do código de ética, da política de segurança da informação e das demais políticas relativas à Governança de Tecnologia da Informação.

Ação 1.5 Planejar a capacitação da equipe de TI

A ação de planejar a capacitação da equipe de TI é necessária e importante, pois visa levar a equipe a imbuir-se de um novo processo que será implantado, com o objetivo de garantir que as habilidades necessárias sejam desenvolvidas e aprimoradas. Em seguida, tal ação deve obter a aprovação da Alta Gestão para garantir que serão realizadas todas as ações necessárias. O TCU (2012b) recomenda a execução de um plano anual de capacitação dos servidores de TI, cuja elaboração, aprovação e acompanhamento se constituem responsabilidade das instituições, de forma a prover e aprimorar o conhecimento necessário para a Gestão e Operação de TI.

Figura 36 – Alinhamento da TI no processo

<table>
<tr><td colspan="3">FINALIDADE</td></tr>
<tr><td colspan="3">Esta ação tem o objetivo de certificar se existe o conhecimento da equipe de TI com o processo de gerenciamento de riscos, baseado nas normas/práticas ISO 31000, ISO 27005, ISO 27002, NIST, FIRM e OSSTMM.</td></tr>
<tr><td colspan="3">ETAPAS</td></tr>
<tr><td colspan="3">1 – Reunião com a equipe de TI</td></tr>
<tr><td colspan="3">2 – Realizar apresentação do processo de gerenciamento de riscos com a equipe de TI</td></tr>
<tr><td colspan="3">3 – Sensibilizar a equipe para a garantia de sucesso</td></tr>
<tr><td colspan="3">4 – Definir a capacitação da equipe</td></tr>
<tr><td>ENTRADAS</td><td>FERRAMENTAS E TÉCNICAS</td><td>SAÍDAS</td></tr>
<tr><td>ISO 31000</td><td rowspan="8">Reuniões</td><td rowspan="8">Alinhamento da equipe no processo</td></tr>
<tr><td>ISO 27005</td></tr>
<tr><td>ISO 27002</td></tr>
<tr><td>NIST</td></tr>
<tr><td>FIRM</td></tr>
<tr><td>OSSTMM</td></tr>
<tr><td>Acórdão 3117/2014 – TCU - Plenário</td></tr>
<tr><td colspan="3">RECOMENDAÇÕES</td></tr>
<tr><td colspan="3">Analisar acórdão 3.732/2014 – 2 – TCU – Plenário (Brasil,2016)</td></tr>
<tr><td colspan="3">REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FERREIRA E ARAÚJO (2009); FONTES (2011, 2012); ISACA (2012); OGC (2007); OLIVEIRA JUNIOR (2015)].</td></tr>
</table>

Figura 37 – Definição do cronograma

FINALIDADE		
Esta ação tem o objetivo de elaborar p cronograma de implantação do processo do GMRITI, constando: período, atividades e responsáveis.		
ETAPAS		
1 – Reunião com a equipe de TI		
2 – Apresentar o relatório de diagnóstico inicial e checklist		
3 – Definir cronograma		
4 – Solicitar aprovação da alta administração		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Relatório de diagnóstico inicial	Reuniões RedMine/GanttProject	Cronograma elaborado
RECOMENDAÇÕES		
Utilizar RedMine ou GanttProject para a elaboração e acompanhamento do cronograma		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FONTES (2011, 2012); OGC (2007); OLIVEIRA JUNIOR (2015)].		

Figura 38 – Assistir a gestão

FINALIDADE		
Obter o apoio da alta gestão neste processo de implantação, uma vez que o apoio é importante para o sucesso e garante o comprometimento da equipe. Além de prover serviços de TI alinhados com a necessidades da instituição		
ETAPAS		
1 – Fazer uma apresentação do processo de gerenciamento de riscos apresentando seus benefícios		
2 – Apresentar os benefícios que serão alcançados com o apoio da alta gestão		
3 – Agendar reunião com a alta gestão para garantir apoio		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Relatório de diagnóstico checklist Benefícios da implantação do processo	Reuniões	Ata da reunião do apoio firmado
RECOMENDAÇÕES		
Convite de um palestrante da área de TI que tenha conhecimentos na área de gestão de riscos em TI, baseado em uma das boas práticas: ISO 31000, NIST, FIRM...		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FONTES (2011, 2012); LUNA (2011); OGC (2007); OLIVEIRA JUNIOR (2015)].		

4.4.2 Fase 2 – Integração

Na fase de integração, deve ocorrer a ação de execução de capacitação da equipe de TI, após esta ação, recomenda-se definir o Catálogo de Serviços, seguir com a implantação da Central de Serviços e a integração com os outros processos de gerenciamento de serviços, caso já estejam implantados na instituição.

Figura 39 – Plano de capacitação

FINALIDADE		
Assegurar que todos os servidores de TI desenvolvam as habilidades necessárias para criar e manter processos de gerenciamento de riscos em TI e que adquiram o conhecimento e competência, alinhado ao PDTI da instituição. A formação deve ser fornecida sempre que um novo processo é implantado ou quando a tecnologia existente é alterada.		
ETAPAS		
1 – Analisar o relatório do diagnóstico inicial		
2 – Levantar habilidades da equipe de TI e sugerir um plano de capacitação		
3 – Solicitar aprovação do plano de capacitação		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Relatório de diagnóstico checklist	Reuniões	Plano de capacitação elaborado
PDTI atual da instituição	Redmine	Aprovação do plano de capacitação
Acórdão 3.117/2014 – TCU - Plenário		
RECOMENDAÇÕES		
Participar de eventos criados pelo SISP, inclusive palestras on-line		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FONTES (2011, 2012); LUNA (2011); OGC (2007); OLIVEIRA JUNIOR (2015)].		

Ação 2.1 Capacitar a Equipe de TI

A ação capacitar a equipe de TI é o momento em que deve ser realizado o que foi planejado no plano de capacitação (Ação 1.5), visando que a equipe adquira o conhecimento necessário para implantação do processo, além de preparar e motivá-la para implantação ou revisão de outros processos de Gerenciamento de Serviços de TI na instituição. Em consonância com o item 9.11.9 do Acórdão 1.233/2012-TCU-Plenário, é recomendado que se elabore, aprove e acompanhe a execução de um plano anual de capacitação do pessoal do setor de TI dos órgãos da APF. A capacitação deverá se tornar algo contínuo na instituição, fazendo com que os profissionais estejam sempre

preparados para novos desafios e também para as metas a serem cumpridas, uma vez que, sem investimentos em capacitação, a organização não estará apta a atingir objetivos estratégicos (TCU, 2012b).

Ação 2.2 Elaborar o Catálogo de Serviços

Elaborar o catálogo de serviços é uma ação muito importante para a implantação dos processos de gerenciamento de serviços na instituição. Os processos de gestão de serviços, conforme definidos na norma 27005 (2011), compreendem diversos aspectos relacionados ao fornecimento dos serviços, tais como a organização de um catálogo de serviços de TI, o estabelecimento de acordos de níveis de serviço com as áreas de negócio, os mecanismos de monitoramento dos serviços e dos acordos pactuados (SLTI, 2015a). Por meio do Acórdão nº 1233/2012 TCU-Plenário, no TC 011.772/2010-7 versando sobre relatório de auditoria na gestão e uso de Tecnologia da Informação em 315 organizações públicas federais o TCU recomendou, no seu item 9.2.9, a implantação de estrutura de controles para mitigar riscos nos processos de Gerenciamento de Serviços de TI (subitem 9.2.9.6). É essencial a aprovação formal pela Alta Administração do Catálogo de Serviços de TI, a não aprovação pode acarretar na sua não implementação e, consequentemente, em prejuízo da integridade das propriedades e especificações dos serviços oferecidos (TCU, 2012b). O catálogo de serviços é o meio de o usuário saber quais são os serviços providos e em que condições. Além do mais, faz a ligação entre as linhas de serviços oferecidas e os ativos dos clientes (FERNANDES; DE ABREU, 2014). É ainda de fundamental importância para o provedor de serviços (Central de Serviços) realizar seu serviço, e base para o plano de continuidade do negócio, já que qualquer ação de restabelecimento da normalidade dos serviços deve seguir os níveis de serviços acordados no catálogo de serviços.

Figura 40 – Fase de integração

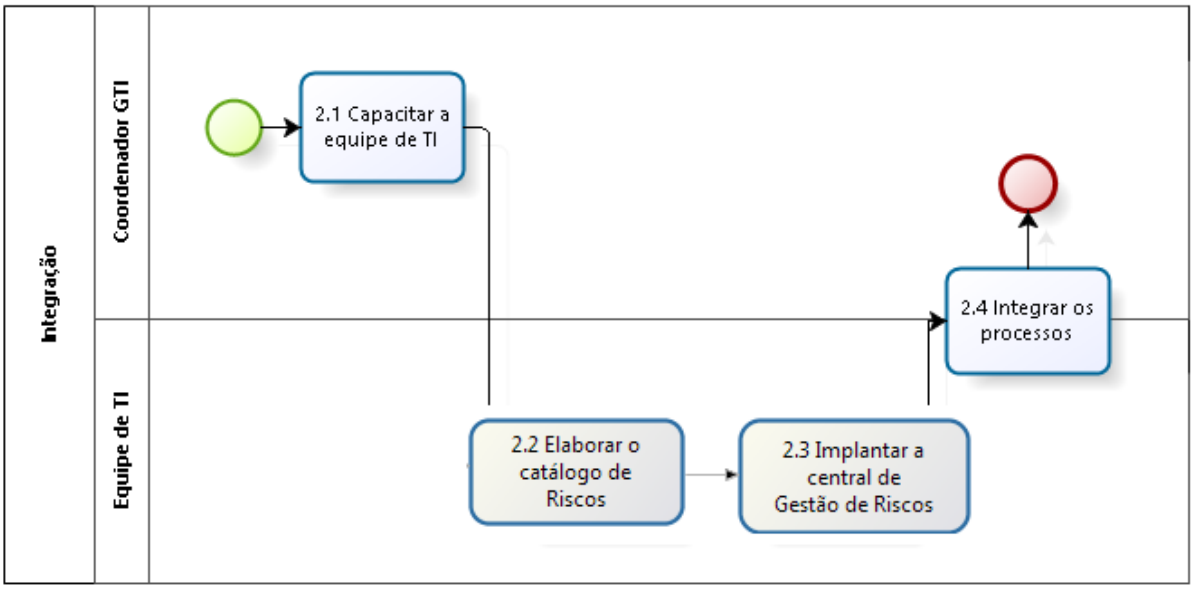


Figura 41 – Capacitação da equipe

FINALIDADE		
Executar o plano de capacitação planejado na ação 1.2, é necessário capacitar todos os profissionais envolvidos no processo de implantação, proporcionando o conhecimento adequado para que as atividades sejam executadas e concluídas com êxito e agregando valor aos processos de trabalho.		
ETAPAS		
1 – Analisar o plano de capacitação		
2 – Fazer o levantamento de onde pode ser realizado o treinamento da equipe de TI e licitar se necessário.		
3 – Executar o cronograma de capacitação		
4 – Desenvolver um relatório da conclusão da execução do plano de capacitação		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Plano de capacitação	Reuniões	Execução da capacitação de equipe Relatório de conclusão da execução do plano de capacitação
RECOMENDAÇÕES		
Verificar agenda e conteúdo dos cursos da ESR/RNP		
Participar de eventos criados pelo SISP, incluindo palestras on-line		
Analisar acórdão 3.732/2014/2014 – 2 – TCU – Plenário (BRASIL, 2016)		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FONTES (2011, 2012); LUNA (2011); OGC (2007); OLIVEIRA JUNIOR (2015)].		

Figura 42 – Elaborar catálogo

FINALIDADE		
Elaborar um documento relacionando todos os serviços de TI existentes que são prestados pela instituição. O objetivo é o de assegurar que um catálogo de riscos de TI é produzido e mantido, contendo informação precisa de todos os riscos possíveis e disponíveis que foram, e que serão, analisados.		
ETAPAS		
1 – Identificar os ativos mais críticos da instituição (hardware e software)		
2 – Classificar as atividades desenvolvidas em cada setor da instituição		
3 – Catalogar os horários de funcionamento dos setores mais críticos da instituição		
4 – Mapear os serviços e seus responsáveis diretos nos diversos setores da instituição		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
ISO/IEC 31000 PDTI atual	Reuniões	Catálogo de serviços documentado e acordado
RECOMENDAÇÕES		
Leitura da biblioteca ITIL e Cobit		
Participar de eventos criados pelo SISP, incluindo palestras on-line		
Analisar acórdão 3.732/2014/2014 – 2 – TCU – Plenário (BRASIL, 2016)		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FONTES (2011, 2012); LUNA (2011); OGC (2007); OLIVEIRA JUNIOR (2015)].		

Ação 2.3 Implantar a Central de Serviços

A ação de implantar a central de serviços é fundamental para que se estabeleça o controle efetivo e a gestão das demandas que chegam à TI, trata-se de um canal especializado de atendimento ao público, o qual irá contribuir para uma gestão de serviço eficiente. A central de serviços é uma função, descrita pela ITIL (Information Technology Infrastructure Library) como uma unidade funcional que tem o intuito de ser o ponto único de contato para os usuários de TI OGC (2007). Consoante os Acórdãos 1.603/2008, 2.585/2012 e 3.117/2014, não é explícita a necessidade de uma central de serviços, porém, é perceptível que existe a necessidade de uma infraestrutura adequada para gerenciar os incidentes que ocorrem nos serviços de TI da instituição, impulsionando assim a criação de uma estrutura organizacional que seja capaz de gerenciar os serviços (TCU, 2008), (TCU, 2014a).

Figura 43 – Implantando serviços

FINALIDADE		
Implantar uma central de serviços na instituição, proporcionando um ponto único de contato, fundamental para que se estabeleça o controle efetivo e a gestão das demandas que chegam a TI, aprimorando a qualidade dos serviços prestados através de um centro especializado, onde serão gerenciados os incidentes e problemas de forma distinta. É essencial que a existência de um banco de dados para que o gerenciamento desses incidentes sejam realizados em sua amplitude.		
ETAPAS		
1 – Identificar se já existem outros processos de gerenciamento de serviços de TI implantados		
2 – Propor infraestrutura para a central de serviços, caso não possua ou necessite substituir		
3 – Desenvolver relatório de conclusão da implantação de central de serviços		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Catálogo de Riscos	Reuniões Recomendamos GLPI OTRS ou CITSMartITSM	Central de serviços implantada Relatório de conclusão da execução da implantação da central de serviços
RECOMENDAÇÕES		
Leitura da biblioteca ITIL e Cobit		
Participar de eventos criados pelo SISP, incluindo palestras on-line		
Analisar acórdão 3.732/2014/2014 – 2 – TCU – Plenário (BRASIL, 2016)		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); LUNA (2011); OGC (2007); OLIVEIRA JUNIOR (2015)].		

Ação 2.4 Integrar os Processos

Esta ação integrar os processos é importante para a instituição que já possui algum processo de Gerenciamento de Serviços de TI implantado, pois visa aproveitar a ferramenta existente, caso contemple o processo de Gerenciamento de Problema. Deve ser analisado o relacionamento com outros processos, a exemplo do gerenciamento de incidentes, que tem uma relação muito próxima com outros processos de. Para analisar resolver um determinado incidente, normalmente a equipa técnica verifica o ICs (Itens de Configuração) em questão, de maneira a poder determinar a causa, e talvez a solução para o incidente, observa-se neste caso que está diretamente ligado com a Gestão de Configurações. Se o incidente possui uma causa ou origem desconhecida, o mesmo passa de incidente a problema, e é reencaminhado para o Gerenciamento de Problema, logo possui também uma relação com este processo. Apesar do processo de gerenciamento de problema ser muito similar ao processo de gerenciamento de incidentes, ambos são processos independentes e irão utilizar as mesmas ferramentas, usar o mesmo tipo de categorização, impacto, prioridade, etc. O que diferencia ambos é a sua causa raiz, haja vista um incidente ser considerado como tendo uma causa raiz

bem definida Já um problema, noutra vertente, trata-se de um incidente cuja causa raiz é desconhecida.

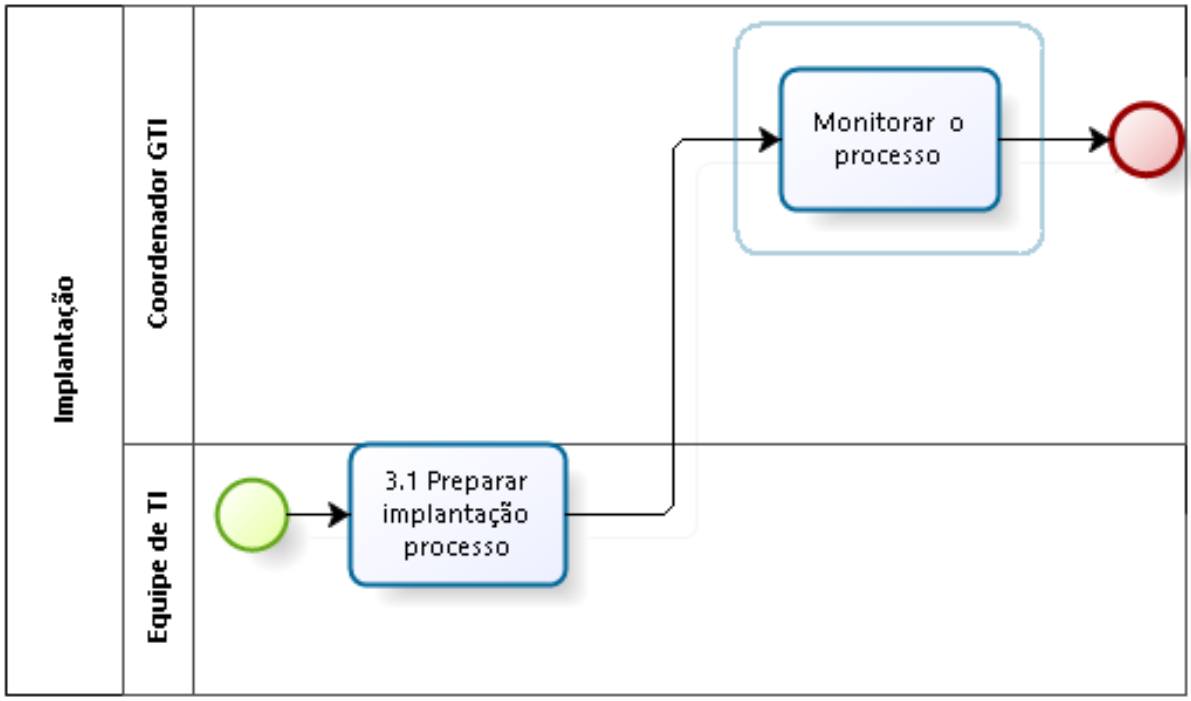
Figura 44 – Integração de processos

FINALIDADE		
Diagnosticar a situação atual da instituição em relação ao processo de gerenciamento de riscos em TI através de checklist proposto por este guia, com o objetivo de identificar as ações que encontram-se realizadas em inciativas anteriores.		
ETAPAS		
1 – Reunião com a equipe de TI		
2 – Aplicação do checklist com a equipe de TI		
3 – Apurar o resultado da aplicação do checklist		
4 – Levantas as necessidades para a implantação		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Checklist de diagnóstico inicial para implantar o processo de gestão de riscos.	Ferramentas de criação de formulários (GOOGLE FORMS, 2017) ou similar	Relatório com diagnóstico inicial para a implantação do processo de gerenciamento de riscos.
RECOMENDAÇÕES		
Realizar o questionário na forma de checklist de acordo com o quadro 2. Este diagnóstico reflete se já existe alguma ação proposta neste guia. Para facilitar o checklist e apuração dos dados é viável a transformação desses em formato WEB.		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); FERREIRA E ARAÚJO (2009); FONTES (2011, 2012); OGC (2007); OLIVEIRA JUNIOR (2015)].		

4.4.3 Fase 3 – Implantação

Esta fase é importante para que se identifique o andamento da execução do projeto e para que este seja consolidado. Neste ponto o processo é implantado.

Figura 45 – Implantação



Ação 3.1 Preparar a Implantação do Processo

A ação de preparar a implantação do processo é o momento em que se deve identificar o cumprimento de todas as ações propostas anteriormente para implantação do processo, com o objetivo de checar se tais ações foram desenvolvidas. Ao se buscar preparar a implantação do processo, é necessário que se considere aspectos como: preparação da infraestrutura de TI, preparação da equipe de TI, e a produção dos artefatos das ações propostas; a partir daí, o processo de Gerenciamento de Problema é, de fato, implantado na instituição. Nesta fase, é importante também que o conceito de serviço de TI esteja incorporado, entendido, praticado e disseminado dentro da TI (COUGO, 2013).

Ação 3.2 Monitorar a Implantação do Processo

A ação monitorar a implantação do processo é importante para que o projeto de implantação seja monitorado e acompanhado, evitando assim descontinuidade do processo, mitigando os riscos. Em consonância com o disposto no item 9.2.9 do Acórdão 1.233/2012-TCU-Plenário, a APF deve realizar auditorias periódicas na área de TI, em especial no que diz respeito à avaliação da Governança de TI, incluindo os processos de Gestão de TI (TCU, 2012b).

4.4.4 Fase 4 – Melhorias

Nesta fase devem ser realizadas as ações de melhorias, buscando obter uma melhoria contínua no processo.

Ação 4.1 Realinhar a Equipe de TI

A ação busca realinhar o conhecimento de toda a equipe de TI, com o objetivo de aprimorar a implantação do processo em curso e encorajá-la a implantar outros processos de Gerenciamento de Serviços de TI na instituição.

Figura 46 – Preparar implantação

FINALIDADE		
Esta ação tem o objetivo de identificar as habilidades desenvolvidas na implantação do processo de gerenciamento de riscos, além de realinhar a equipe ao processo, visando identificar falhas ocorridas e para que sejam aperfeiçoadas.		
ETAPAS		
1 – Reunião com toda a equipe de TI		
2 – Motivar a equipe a identificar as falhas ocorridas e corrigir		
3 – Motivar a equipe a capacitar-se e garantir sucesso da implantação do processo		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Acórdão 3.117/2014 – TCU-Plenário	Reuniões	Relatório de falhas ocorridas e corrigidas Equipe realinhada ao processo
RECOMENDAÇÕES		
Analisar acórdão 3.117/2014/2014 – 2 – TCU – Plenário (BRASIL, 2016)		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); OGC (2007)].		

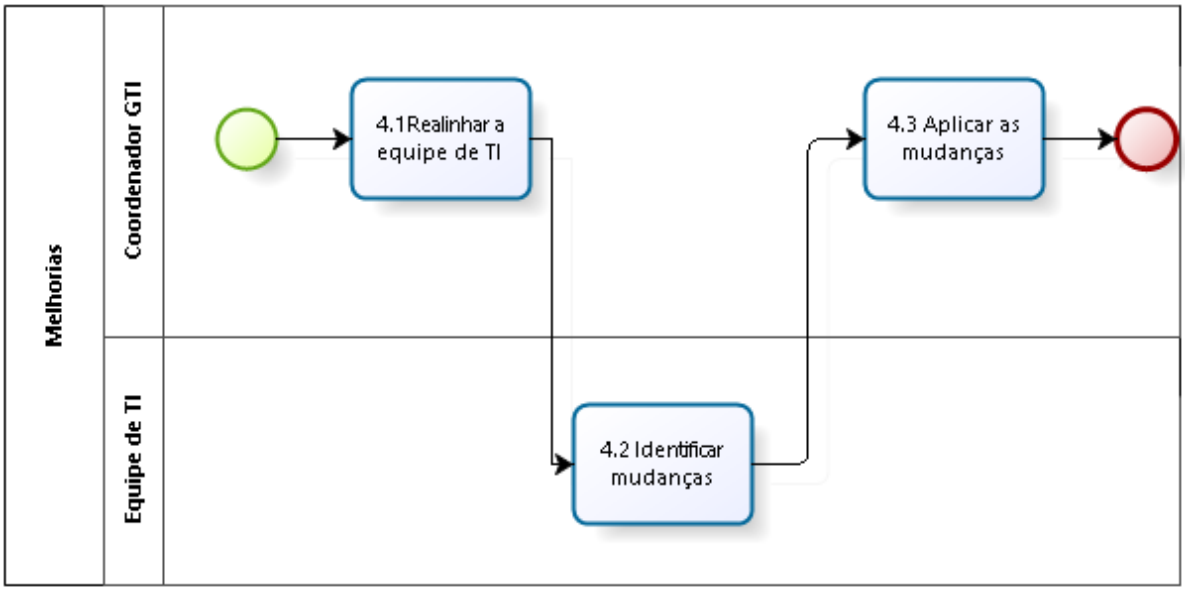
Figura 47 – Monitoramento da implantação

FINALIDADE		
É recomendado o monitoramento contínuo da implantação em termos de riscos ativos e medições objetivas do andamento e da qualidade, para mitigar os riscos que comprometam a execução do projeto de implantação		
ETAPAS		
1 – Monitorar o status do projeto de implantação		
2 – Resolver os problemas identificados		
3 – Desenvolver relatório de monitoramento (identificando algum incidente)		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Relatório de conclusão da implantação de gerenciamento de problema	Reuniões Redmine	Relatório de monitoramento
RECOMENDAÇÕES		
Manter contato com outras instituições que já possuem gerenciamento de serviços de TI integralmente implantados e em funcionamento.		
Analisar acórdão 3.732/2014/2014 – 2 – TCU – Plenário (BRASIL, 2016)		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009); OGC (2007)]		

Ações 4.2 Identificar e Aplicar as Mudanças

As ações de identificar e aplicar as mudanças têm a finalidade de assegurar que todas as mudanças necessárias sejam analisadas e aplicadas no processo de implantação de Gerenciamento de Problema. Faz-se necessário garantir que, com o processo já implementado, se continue a identificar a aplicar as melhorias que forem cabíveis, visto que essas melhorias devem ser contínuas (OGC, 2011).

Figura 48 – Melhorias do guia



4.4.5 Avaliação do Guia de Implantação do Processo de GMRTI

Nesta seção, expõe-se o desenvolvimento da avaliação do Guia de melhores práticas para mitigação de riscos em TI (GMRTI), apresentado na seção 4.5, bem como a análise e a discussão dos resultados. O propósito foi avaliá-lo através da opinião de especialistas, valendo-se da aplicação de um questionário, no qual o público alvo da avaliação foram Gestores e especialistas de TI dos IFEs.

Figura 49 – Aplicação das mudanças

FINALIDADE		
Esta ação tem o objetivo de identificar mudanças necessárias no projeto de implantação do processo, analisá-las e aplicá-las e após a implantação do processo, analisar os relatórios de problemas para tratamento da causa raiz dos incidentes.		
ETAPAS		
1 – Reunião com toda a equipe de TI		
2 – Motivar a equipe a identificar as mudanças necessárias		
3 – Analisar se as mudanças identificadas afetam outros processos		
4 – Motivar a equipe a aplicar as mudanças no projeto de implantação do processo e de infraestrutura		
ENTRADAS	**FERRAMENTAS E TÉCNICAS**	**SAÍDAS**
Relatório de problema	Reuniões	Relatório das mudanças identificadas, analisadas e se aplicadas.
RECOMENDAÇÕES		
Analisar acórdão 3.117/2014/2014 – 2 – TCU – Plenário (BRASIL, 2016)		
REFERÊNCIAS: [ABNT (2013); BRASIL (2009, 2015); OGC (2007, 2011)].		

4.5 DESCRIÇÃO DA AVALIAÇÃO DO GUIA

Para assegurar que o Guia de melhores práticas para Mitigação de Riscos em Incidentes de TI atinja o seu objetivo, foi necessário elaborar uma avaliação com profissionais especialistas da área de TI, como: Gestores de Segurança da Informação, Diretores de TI ou Coordenadores de TI que exercem função similar na área de segurança da informação, de forma a complementar os resultados obtidos com a realização da pesquisa e com a elaboração desse Guia. Para isso, foi elaborado um questionário (figura 4.20, figura 4.21 e figura 4.22) composto por 5 questões. Uma questão serviu para identificar a instituição, duas questões utilizaram a escala Likert e outras duas questões abertas serviram para que o respondente informasse o seu ponto de vista em relação à utilidade do Guia produzido. A avaliação foi fundamentada no Modelo de Aceitação de Tecnologia (Technology Acceptance Model - TAM), de Davis (1989). O modelo TAM sugere que fatores como a facilidade de uso percebida e utilidade percebida influenciam na intenção de uso de um novo sistema ou abordagem teórica e metodológica. Para Davis (1989), as pessoas tendem a usar ou não uma tecnologia com o objetivo de melhorar seu desempenho no trabalho – utilidade percebida. Porém, mesmo que essa pessoa entenda que uma determinada tecnologia é útil, sua utilização

poderá ser prejudicada se o uso for muito complicado, de modo que o esforço não compense o uso – facilidade percebida.

4.5.1 Descrição da Avaliação

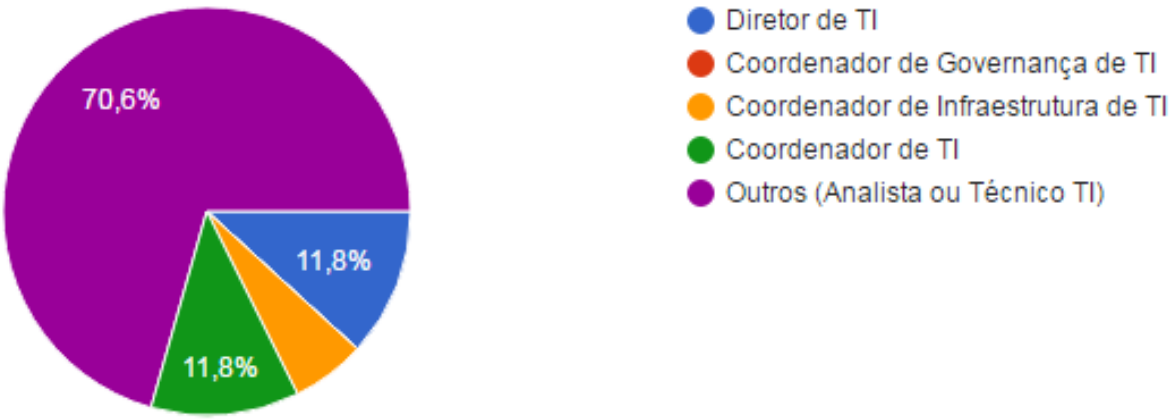
Inicialmente, os avaliadores foram convidados a conhecer o conteúdo do Guia, disponível no site: https://sites.google.com/a/cin.ufpe.br/gmpig/, encontra-se na seção 4 dessa dissertação, em seguida a avaliá-lo, através do questionário eletrônico, disponibilizado no endereço: https://goo.gl/forms/WFC8YjEKq26KtAHk2 . O questionário de avaliação teve a participação de dezessete avaliadores.

4.5.2 Análise e Discussão dos Resultados

Nesta seção apresenta-se uma leitura criteriosa dos dados coletados por meio do questionário aplicado aos Gestores de TI que atuam na APF lotados nos IFE.

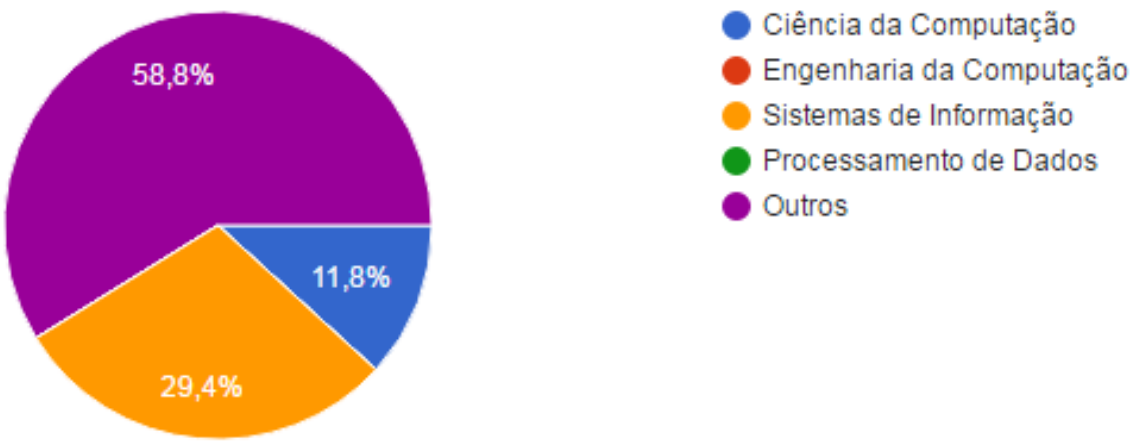
O gráfico da Figura 4.20 demonstra a função que cada um dos participantes ocupa na sua instituição, sendo demonstrado que mais de 62% dos avaliadores exercem funções de gestão, os Outros, 37,5%, tratam-se de analistas e técnicos de TI, sem a função de gestão nos IFE.

Figura 50 – Cargos dos respondentes da avaliação do guia



Em relação à área de formação dos participantes, 68,7% dos avaliadores, declararam possuir formação relacionada com a área de conhecimento Ciência da Computação, as áreas foram baseadas na Capes. Ainda tivemos 31,3% dos avaliadores que responderam como outros (cursos não identificados), demonstrando com isso que o resultado da avaliação corrobora o fato de os participantes terem o conhecimento, no mínimo básico, para contribuírem com a avaliação do Guia. O gráfico na Figura 4.21 apresenta a formação dos avaliadores envolvidos na pesquisa.

Figura 51 – Formação dos avaliadores

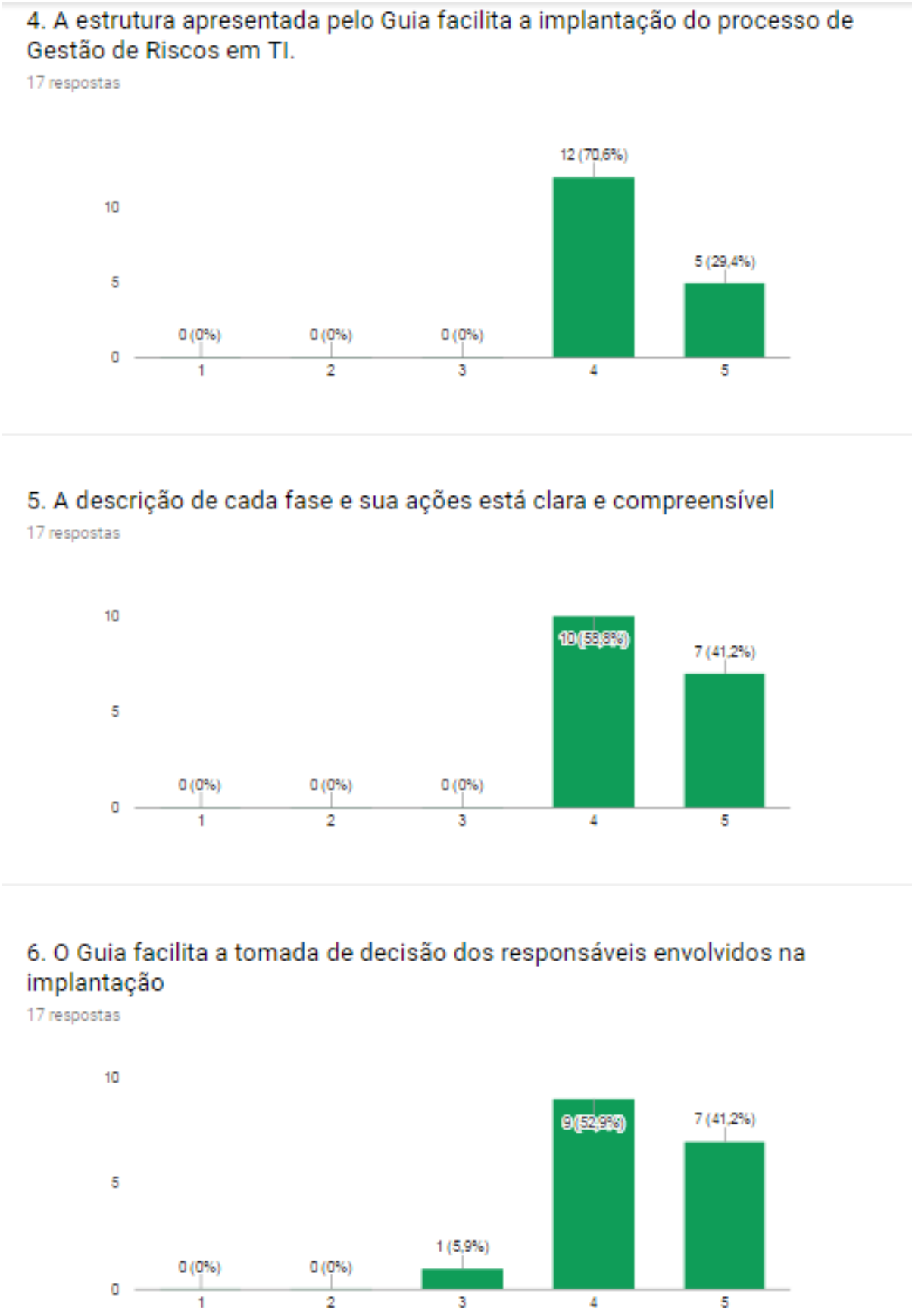


4.5.2.1 Avaliação da Percepção da Facilidade de Uso

Quanto ao aspecto de percepção de facilidade de uso foram disponibilizadas no questionário quatro afirmações relacionadas à facilidade de utilizar o Guia de Implantação de Processo , tendo sido utilizada a escala Likert com as seguintes opções de resposta: “Concordo plenamente”, “Concordo”, “Nem concordo nem discordo”, “Discordo”e “Discordo totalmente”. A avaliação dessas questões é considerada relevante para esta pesquisa, pois, conforme apresentado na figura 4.22, a partir da avaliação dos respondentes foi possível identificar o nível de esforço que o Guia exige para sua utilização. Em relação à facilidade de uso percebida, pode-se considerar que o resultado atende as expectativas, Ranking Médio (RM) calculado acima de 4,00 e não houve discordância dos avaliadores em nenhuma das perguntas, estes responderam que concordam parcialmente ou totalmente, apresentam-se os seguintes resultados: questões 4 e 5, 100% e questão 6: 94,1%. A partir dos resultados apresentados, pode-se considerar que o Guia proposto atende as expectativas daqueles a quem se destina,

esta foi a percepção dos avaliadores, para eles, o guia apresenta facilidade de uso na implantação do processo de gerenciamento de riscos em TI.

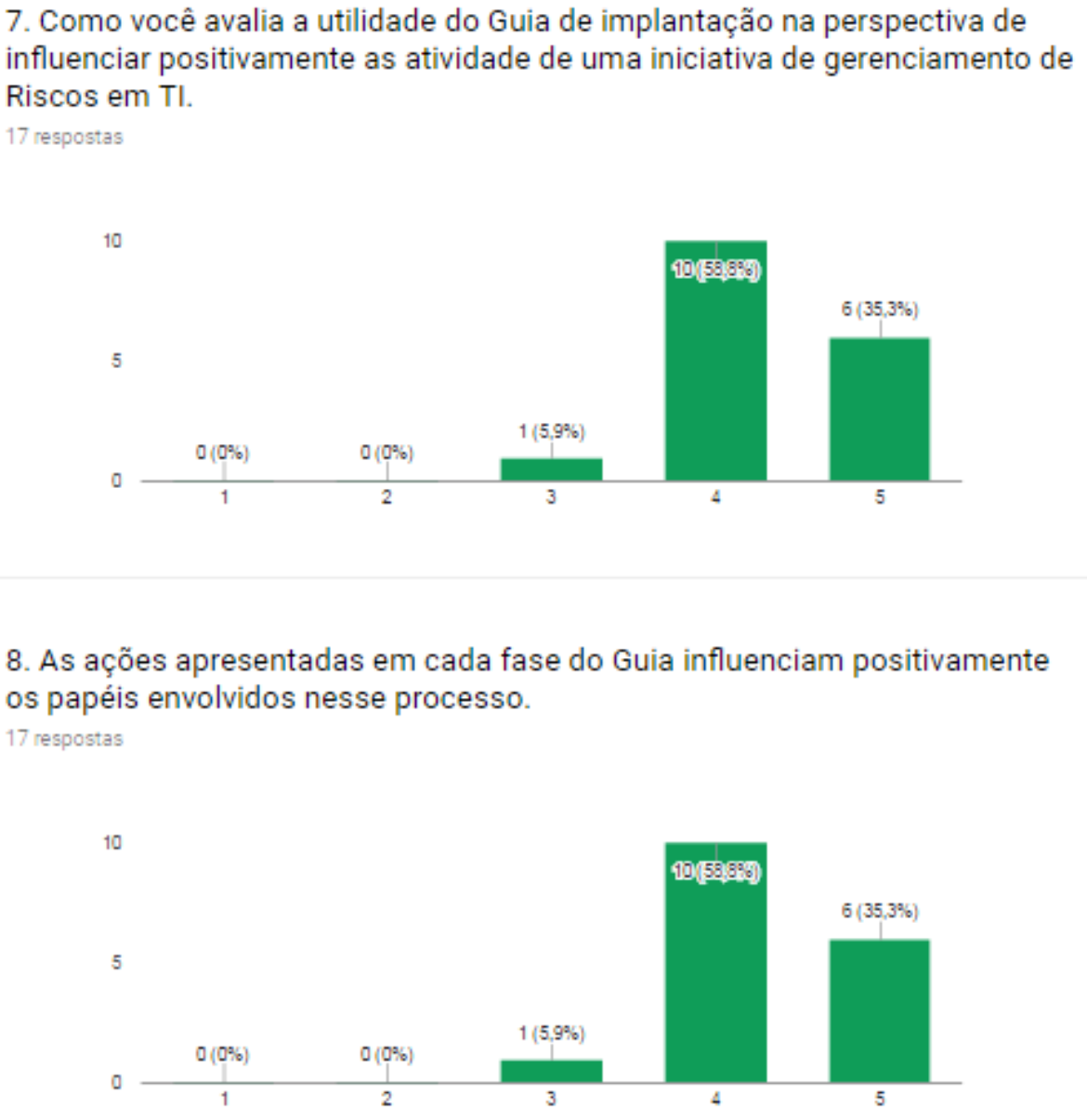
Figura 52 – Avaliação sobre facilidade de uso



4.5.2.2 Avaliação da Percepção da Utilidade

Quanto ao aspecto utilidade percebida, foram aplicadas cinco afirmações, utilizando-se também a escala Likert, conforme figura 4.23. A avaliação dessas questões mostra-se significativa para esta pesquisa, pois a partir das respostas dos participantes, foi possível identificar o quanto o guia proposto é considerado útil para auxiliar as instituições nas iniciativas de implantação do processo de gerenciamento de riscos. Em relação à utilidade percebida, a maioria dos avaliadores concordou que o guia de Implantação do processo de gerenciamento de riscos é muito útil, observa-se ainda na figura 4.22, Ranking Médio (RM) calculado acima de 4,00 em todas as questões, os avaliadores responderam que concordam parcialmente ou totalmente, constatando-se os seguintes resultados: 94,1% nas questões 7, 8 e 9. Na questão 10: 76,5%, na questão 11 foi de 70% e na questão 12 foi de 100%. Diante dos resultados apresentados na avaliação, através de gestores de TI e demais servidores que avaliaram o guia proposto, foi demonstrado que há intenção de se utilizar o referido guia, conforme apresentado a seguir:

Figura 53 – Avaliação sobre percepção de utilidade parte a



09. As ações apresentadas em cada fase do Guia favorecem o desenvolvimento de competências e habilidades para o processo de implantação do processo de gerenciamento de riscos em TI.

17 respostas

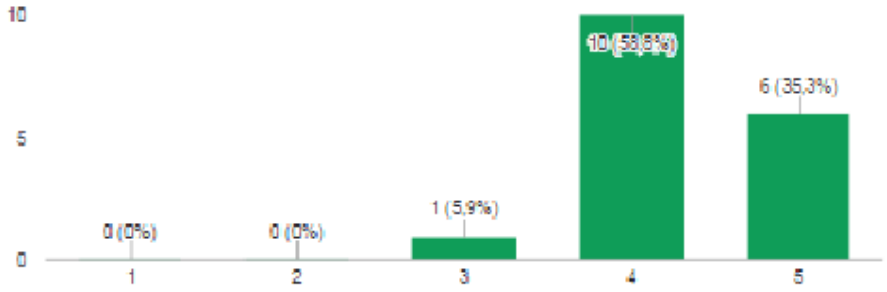
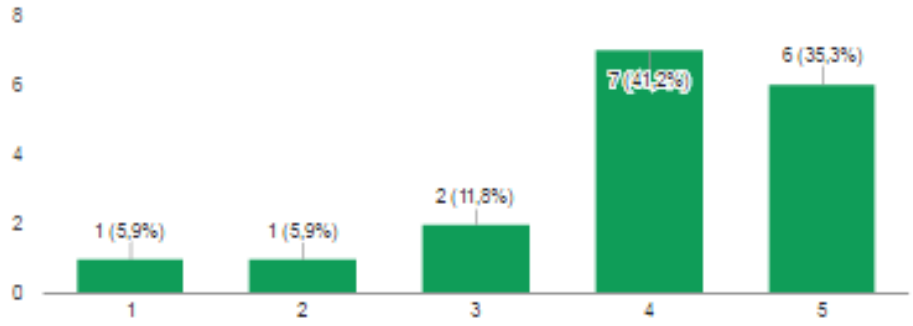


Figura 54 – Avaliação sobre percepção de utilidade parte b

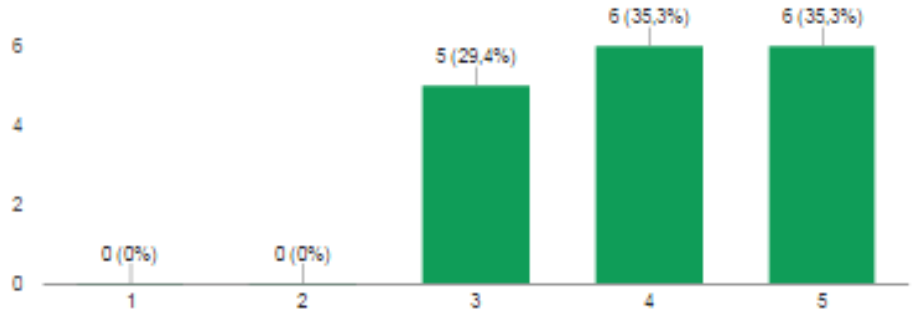
10. O Guia pode ser utilizado em qualquer instituto federal, independente de sua estrutura, sua cultura ou sua missão institucional.

17 respostas



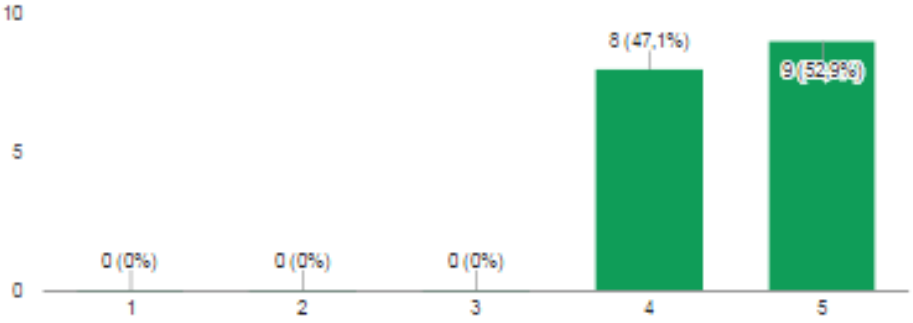
11. O conteúdo do Guia prepara o instituto federal para a implantação do processo de gerenciamento de riscos em TI.

17 respostas



12. Utilizaria ou recomendaria o Guia para outras instituições que necessitam implantar gerenciamento de riscos em TI.

17 respostas



4.5.2.3 Opinião dos Especialistas sobre os Benefícios e Limitações do Guia

Nas duas questões discursivas do questionário indagou-se a opinião dos especialistas, quanto aos benefícios e às limitações que as instituições teriam na utilização do guia de gereciamento de riscos, apresenta-se a seguir as respostas dos avaliadores nas figuras 4.25 e 4.26. De acordo com as opiniões dos avaliadores é importante a utilização do guia proposto nos Institutos Federais de Educação com o objetivo de padronizar e facilitar a tomada de decisões de riscos de TI. Percebeu-se também que os benefícios esperados sobre o uso desse guia podem ser ampliados dependendo do apoio da Alta Gestão.

Figura 55 – Opinião de especialistas sobre os benefícios do guia

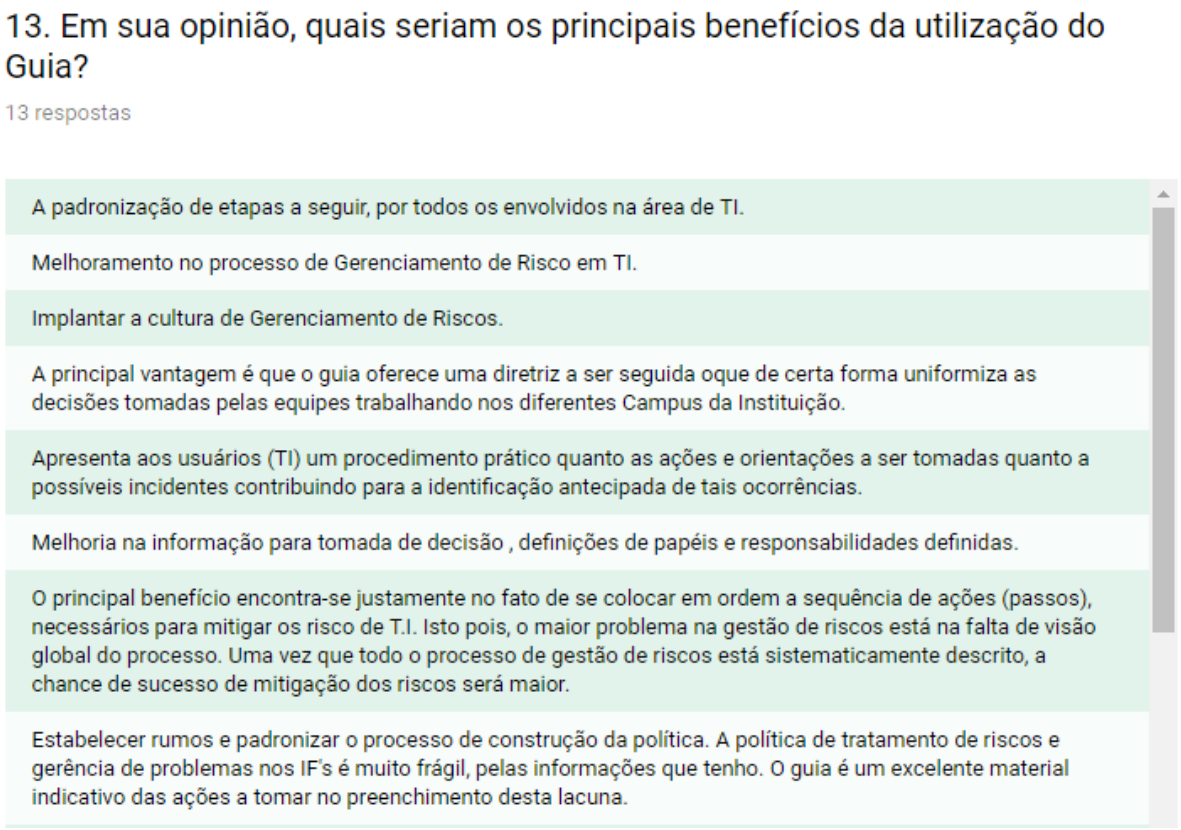
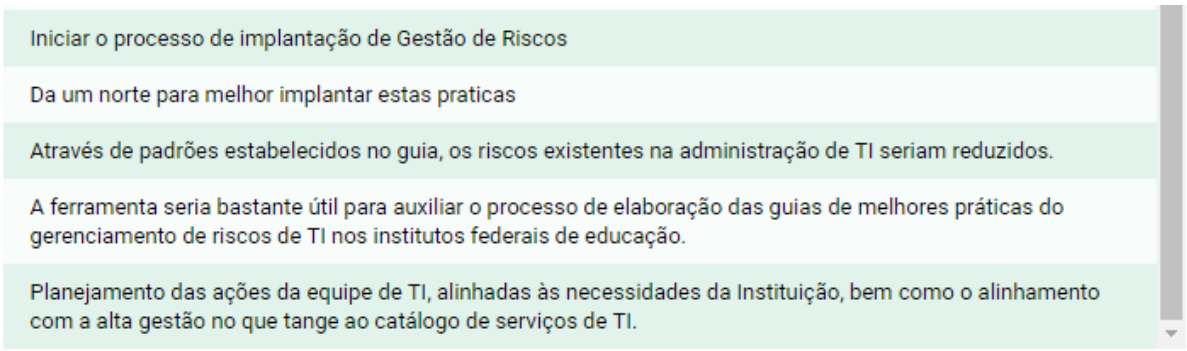


Figura 56 – Opinião de especialistas sobre os benefícios do guia



Os avaliadores também observaram que as limitações de capacidade de equipe de TI local e sensibilização da alta gestão, conforme figuras 4.27 e 4.28 são obstáculos a serem superados.

Figura 57 – Opinião de especialistas sobre as limitações do guia

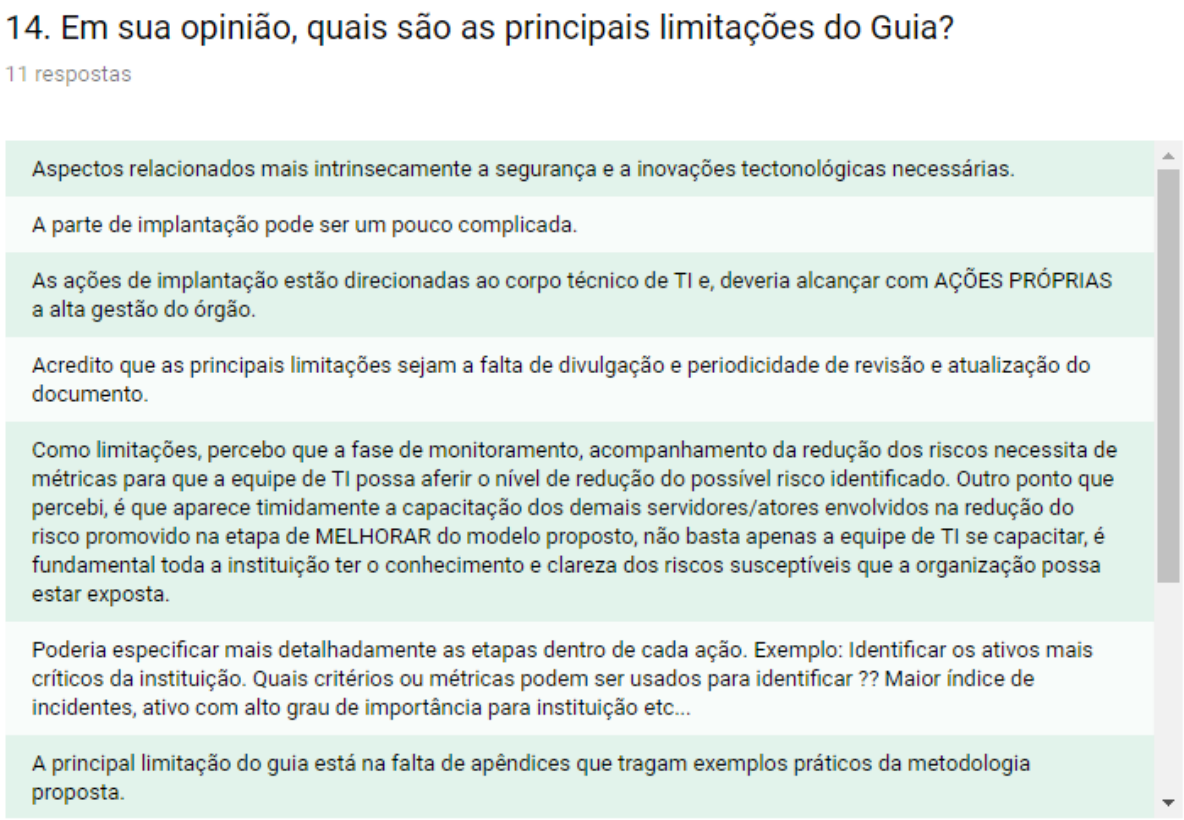
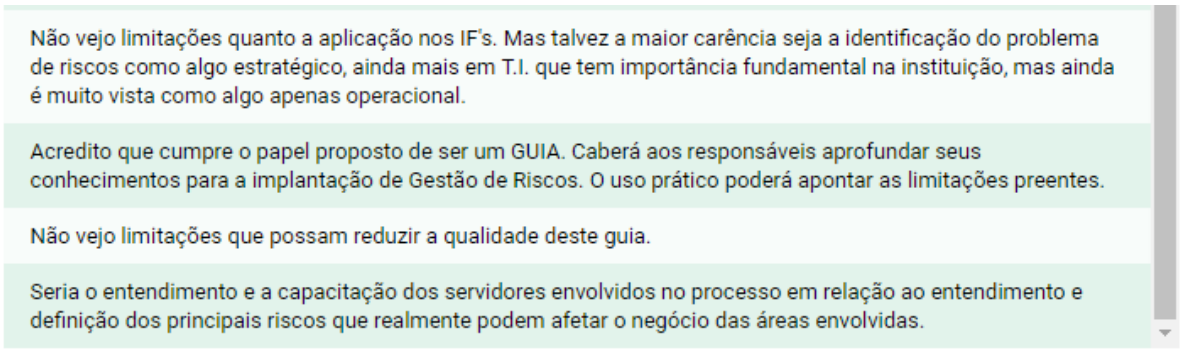


Figura 58 – Opinião de especialistas sobre as limitações do guia



4.6 SÍNTESE DO CAPÍTULO

Este capítulo apresentou uma proposta de Guia de melhores práticas para a mitigação de riscos em incidentes de TI, na qual apresentou um conjunto de ações necessárias que auxilie os IFE a atender às recomendações do TCU em relação à implantação do processo de gerenciamento de riscos de TI na APF. No Guia, foram sugeridas fases e ações advindas da pesquisa, com base na literatura especializada e em publicações de padrões de normas internacionais como: ISO 27002, OSSTMM, ISSAF, PTES E NIST 800-30, tais pesquisas tiveram a finalidade de produzir o GMRTI de forma objetiva, clara e consistente para facilitar o processo de gestão de riscos nas IFE. Foram apresentados os resultados da avaliação do Guia, levantados por meio de um questionário fundamentado no método de avaliação Technology Acceptance Model (TAM). Colheu-se a opinião de dezessete especialistas. O próximo capítulo vai abordar as considerações finais do trabalho como as conclusões e sínteses, apresentar limitações do estudo e apontar possíveis trabalhos futuros que poderão permitir a continuidade desta pesquisa.

5 CONSIDERAÇÕES FINAIS

Este capítulo apresenta os objetivos alcançados, buscando tecer conclusões e sínteses que evidenciem o conteúdo para o direcionamento deste estudo e nesse percurso, apresentam-se limitações e contribuições da pesquisa para a construção do conhecimento técnico-científico. Em determinada fase, aponta-se para o delineamento de possíveis trabalhos que poderão permitir a continuidade da presente pesquisa.

5.1 CONCLUSÃO

De acordo com os relatórios e acórdãos realizados pela TCU, evidencia-se um cenário de baixo nível de gestão de riscos de TI na APF. Esta pesquisa teve como objetivo a elaboração de um guia de melhores práticas para a mitigação de riscos em incidentes de TI que direcionou para a pergunta de pesquisa: Como mitigar o gerenciamento dos riscos de segurança da informação para atender os riscos que afetam os ativos de forma eficiente, a realidade das Instituições Federais de Educação ?

Com o objetivo de responder a essa pergunta e alcançar os objetivos da pesquisa, seguiram-se as etapas de pesquisa descritas no capítulo 3.

A primeira coleta de dados, realizada através de questionário, foi respondido por 48 IFE, de todas as regiões do Brasil. Após esse processo identificou-se o nível de adoção do gerenciamento de Serviços de TI e do processo de gestão de riscos de TI. O presente estudo teve como motivação a publicação do relatório de levantamento de governança de TI do ano de 2014, divulgado pelo TCU, o qual apenas 12% dos órgãos da APF tinham adotado integralmente e 29% tinham adotado parcialmente a gestão de riscos de TI.

Estes dados demonstram que a gestão de riscos não tem prioridade nas ações de segurança das IFE. Vários fatores foram observados, tais como: pouco conhecimento sobre gestão de riscos dos gestores por ser um novo tema, para implantar esse processo é necessária que alta administração apoie e pouco conhecimento sobre a prática de gestão de riscos dos colaboradoes.

Os demais objetivos específicos, também foram atingidos. Foi possível analisar o conjunto de melhores práticas para gerenciamento de riscos de TI na literatura e definido pelas melhores práticas como: ISO 27002, OSSTMM, ISSAF, PTES E NIST 800-30, apresentados na revisão bibliográfica do capítulo 2. Para a avaliação do guia proposto, aplicou-se um questionário, por meio do qual uma amostra significativa dos

mesmos participantes da coleta de dados pôde avaliar o grau de facilidade e utilidade percebida do referido guia, estes resultados apresentados no capítulo 4, Seção 4.4.5, foram considerados satisfatórios.

Por fim, pode-se afirmar que os objetivos dessa pesquisa foram alcançados e as suas respectivas perguntas de pesquisa foram respondidas com base em uma gama de levantamentos teóricos e técnico-científicos, bem como na opinião de especialistas.

5.2 CONTRIBUIÇÕES E LIMITAÇÕES DA PESQUISA

Ao ser proposto um guia de melhores práticas para mitigação de riscos de TI com o objetivo de minimizar e facilitar que as IFEs que necessitam elaborar sua política de construção e aprovação, algumas contribuições, por meio desse estudo, podem ser consideradas para a pesquisa científica, tais como:

Realização da Pesquisa Teórica por meio da aplicação de uma revisão sistemática, o que permitiu levantar trabalhos relevantes publicados nos últimos 6 anos, com base em critérios estabelecidos no protocolo de pesquisa.

Utilização de práticas profissionais e acadêmicas, em gestão de segurança da informação, que permitam adquirir informações necessárias para o desenvolvimento de modelos de forma ágil;

Possibilitar que órgãos da APF tenham um referencial em que possam medir a maturidade das práticas de segurança da informação ao utilizar os práticas ISO 27002, OSSTMM, ISSAF, PTES E NIST 800-30 para implantar suas politicas de gerenciamento de riscos;

Utilizar o guia proposto para aplicação em deiversos outros órgãos da APF para que permitam avaliar a maturidade de gestão de riscos dessas instituições.

Durante o desenvolvimento do trabalho, algumas limitações foram detectadas, o que impediram, de alguma forma, a sua elaboração de maneira mais consistente e mais concreta. As duas principais limitações identificadas neste trabalho foram:

Não estava no escopo desta pesquisa a realização de um estudo de caso, como método de procedimento, com a finalidade de aplicar o objeto de estudo produzido, essa limitação se deu pelo fato de que o período de implantação do processo poderia se alongar.

Os dados foram coletados somente em um órgão público da APF, em específico, no caso, os IFEs dentre vários outros que fazem parte da APF. A escolha dos IFE se deu pelo fato da facilidade de se conseguir atingir um número significativo das amostras e trazer uma contribuição para um problema da Rede Federal de Educação.

5.3 TRABALHOS FUTUROS

Ainda que este trabalho tenha cumprido seus objetivos, compreende-se que há oportunidades de pesquisa relacionadas ao gerenciamento de riscos de TI, em específico nos órgãos da APF, que podem ser exploradas em trabalhos futuros, essas pesquisas podem se tecer através de:

- Realização de estudo de caso para aplicar o Guia, em um IFE, com o objetivo de validá-lo, além disso, a instituição que se propõe a aplicar as boas práticas da ISO 27002, OSSTMM, ISSAF, PTES E NIST 800-30, pode trazer grande contribuição, no sentido de estabelecer o guia como fonte de consulta de TI na APF;
- A partir do estudo de caso aplicado, elaborar os artefatos ou modelos necessários para materializar as ações de cada fase sugerida no guia durante a implantação do processo.

REFERÊNCIAS

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança da Informação. Rio de Janeiro, 2013.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2011.

ABNT. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, NBR ISO/IEC 31000 – Gestão de Riscos. Rio de Janeiro, 2009

ALBUQUERQUE JUNIOR, Antônio Eduardo De; SANTOS, Ernani Marques Dos. Controles e práticas de segurança da informação em um instituto de pesquisa federal. Simpósio de Excelência em Gestão e Tecnologia, v. 8, 2011.

AL-HAMDANI, Wasim A.; DIXIE, Wendy D. Information security policy in small education organization. In: 2009 Information Security Curriculum Development Conference. ACM, 2009. p. 72-78.

ALVES, Luiz Cláudio Macena; MOREIRA, Jander. Gerenciamento da Política da Segurança da Informação. Revista TIS, v. 1, n. 2, 2012.

ARRUDA, Darlan Florêncio de. Um guia de seleção para implantação de Métricas de Software. Universidade de Pernambuco, Escola Politécnica de Pernambuco. Programa de Pós-Graduação em Engenharia de Computação. Dissertação de mestrado. Recife-PE. 2014.

BACKER, P. de. Gestão ambiental: a administração do verde. [S.l.]: Qualitymark, 1995.

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

BIOLCHINI, J.; Mian, P.G.; Natalli, A.C.C.; Travassos, G.H. (2005). Systematic Review in Software Engineering. Technical Report RT-ES 679/05, COPPE/UFRJ. Disponível em:< http://alarcos.infr.uclm.es/doc/MetoTecInfInf/Articulos/es67905.pdf>. Acesso em 10/02/2017.

BRASIL. Decreto nº 3.505 de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Casa Civil, Subchefia para Assuntos Jurídicos, 2000. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acessado em: 10/02/2017.

BRASIL. Tribunal de Contas da União. Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal. Brasília : TCU, Secretaria de Fiscalização e Tecnologia da Informação. Sumário Executivo, 2008. 48 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2515176.PDF>. Acessado em: 10/02/2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008. Orientações para Gestão de Segurança da Informação e Comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Brasília, DF, GSI/PR, 2008. 4. P. Disponível em: <http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf>. Acessado em: 10/02/2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar nº 03/IN01/DSIC/GSI/PR. Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2009. 5 p. Disponível em: < http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf > Acessado em: 10/02/2017.

BRASIL. Tribunal de Contas da União. Levantamento de governança de TI 2010. Brasília : TCU, Secretaria de Fiscalização e Tecnologia da Informação. Sumário Executivo, 2010. 49 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2056350.PDF>. Acessado em: 10/02/2017.

BRASIL. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF>. Acessado em: 10/02/2017.

BRASIL. Tribunal de Contas da União. Levantamento de Governança de TI 2012. Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação. Sumário Executivo, 2013. 56 p. Disponível em: <http://portal.tcu.gov.br/lumis/portal/file/

fileDownload.jsp?fileId=8A8182A14D78C1F1014D794A2FA80787>. Acessado em: 10/02/2017.

BRASIL. Tribunal de Contas da União. Levantamento de Governança de TI 2014. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2015. 94 p. Disponível em: <http://portal3.tcu.gov.br/portal/pls/portal/docs/2705176.PDF>. Acessado em: 10/02/2017.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Guia de Orientações ao Gestor em Segurança da Informação e Comunicações. Versão 2.0, Brasília, DF, GSI/PR, 2015. 5 p. Disponível em: < http://dsic.planalto.gov.br/documentos/guiagestor.pdf> Acessado em: 10/02/2017.

CASTILHO, Sérgio Duque. Política de segurança da informação aplicada em uma instituição de ensino mediante análise de risco. RETEC-Revista de Tecnologias, v. 5, n. 2, 2013.

CAVALCANTI FILHO, H. Investigação da influência da governança de TI nas instituições federais de ensino superior: estudo de caso. 2011. Tese (Doutorado em Ciência da Computação). Universidade Federal de Pernambuco. CIn.

CAVALCANTI, José Carlos. Enterprise architecture: an interface concept between the economics and the management of the firm. JISTEM-Journal of Information Systems and Technology Management, v. 6, n. 3, p. 525-550, 2009.

COHEN, Fred. Risk Management: Concepts and Frameworks. USA: Burton Group, 2011. 45 p.

D'ANDREA, Edgar et al. Segurança em Banco Eletrônico. São Paulo: Febraban, 2011. 134 p.

DANTAS, M. L., Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos. Pernambuco, 2011.

DAVIS F. D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quart. (1989) 13:319–339

DZAZALI, Suhazimah; HUSSEIN Zolait, Ali. Assessment of information security maturity: an exploration study of Malaysian public service organizations. Journal of Systems and Information Technology, v. 14, n. 1, p. 23-57, 2012.

FONTES, Edison Luiz Gonçalves. Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo. Centro Estadual de Educação Tecnológica Paula Souza. Dissertação de mestrado. São Paulo-SP. 2011.

GIL, A. C. Métodos e técnicas de pesquisa social. In: Métodos e técnicas de pesquisa social. [S.l.]: Atlas, 2010.

GUERRA, A. C.; ALVES, Â. M. Aquisição de produtos e serviços de software. Ed. Elsevier, Rio de Janeiro, [S.l.], 2004.

GUIMARAES, A. G., et al. Segurança em Redes Privadas Virtuais - VPNs, BRASPORT, 2009.

HERTZOG, P. OSSTMM - Open Source Security Testing Methodology Manual. Institute for Security and Open Methodologies, ISECOM. Disponível em: http://www. isecom. org/osstmm

INFORMATION SECURITY FORUM; Fundamental Information Risk Management –Implementation guide. USA: ISF, 2000. 93 p.

ISACA. COBIT. 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA, 2012.

KAUARK, Fabiana. Metodologia da pesquisa : guia prático / Fabiana Kauark, Fernanda Castro Manhães e Carlos Henrique Medeiros. – Itabuna : Via Litterarum, 2010. p. 88.

KIRAN, K.V.D. Information security Risk Management in Critical informative Systems, 2014

KITCHENHAN, Barbara et al. Systematic literature reviews in software engineering: A systematic literature review, Information and Software Technology. Technical report. Nov. 2008.

LAKATOS, E. M.; MARCONI, M. Técnicas de Pesquisa. 7th.ed. [S.l.]: Atlas São Paulo, 2009.

LIANG, L. The state of the art of risk assessment and management for information systems. Information Assurance and Security (IAS), 9th International Conference on. 2013.

MALHOTRA, N. K. Pesquisa de marketing: uma orientação aplicada. [S.l.]: Bookman Editora, 2012.

MATTES, Icaro Valente.; PETRI, Sérgio Murilo. Accounting Information Security: Procedures For The Preparation of A Security Policy Based On Iso 27001 and ISO 27002. In: 10th International Conference on Information Systems and Technology Management. 2013.

MAYER, N.; AUBERT, J. Sector-Specific Tool for Information Security Risk Management in the Context of Telecommunications Regulation (Tool demo). Glasgow, Scotland Uk, 2014

MELLO, Israel de Almeida. Uma Revisão Sistemática sobre Fatores que Levam à Redução de Falhas em Software. XI SEGeT, 2014.

MENG, M. The research and application of the risk evaluation and management of information security based on AHP method and PDCA method. 2013

MOYO, M. Information security risk management in small-scale organizations: A case study of secondary schools computerised information systems. South Africa, 2013

NASCIMENTO, Eduardo Camargos Lagares do. Fatores culturais e estruturais que impactam na implantação da política de segurança da informação: um estudo de caso sobre o Ministério do Desenvolvimento Agrário. Universitas: Gestão e TI, v. 2, n. 1, 2012.

OLIVEIRA JUNIOR, Nilson Cândido. Uma proposta de implantação de governança de TIC em Instituições Federais de Ensino. 2015. 192 f.: fig., tab. Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIN, Ciência da Computação, 2015.

OLIVEIRA, L. H. d. Exemplo de cálculo de Ranking Médio para Likert. Notas de Aula. Metodologia Científica e Técnicas de Pesquisa em Administração. Mestrado em Adm. e Desenvolvimento Organizacional. PPGA CNEC/FACECA: Varginha, [S.l.], 2005.

Open Information Systems Security Group. Information Systems Security Assessment Framework, 2006.

Penetration Testing Execution Standard. Technical Guidelines. Disponível em: http://www.pentest-standard.org

QUINTELLA, Heitor Luiz Murat de Meirelles; BRANCO, Marcelo Pereira de Oliveira. Fatores Críticos de Sucesso em Segurança da Informação em Um Órgão da Administração Pública Federal. Anais do II SINGEP e I S2IS – São Paulo – SP, Brasil. 2013.

SAFA Nader Sohrabi; ISMAILl Maizatul Akmar. A customer loyalty formation model in electronic commerce. Econ Model, Vol. 35, 2013, Pag 559–564.

SAMPAIO, R. F; MANCINI, M. C. Estudos de Revisão Sistemática: um guia para síntese criteriosa da evidência científica. Revista Brasileira de Fisioterapia, São Carlos, v. 11, n. 1, p. 83-89, jan./fev. 2007. Disponível em: $<$ http://www.scielo.br/pdf/rbfis/v11n1/12.pdf $>$. Acesso em: 01/03/2016.

SEDINIC, I., PERUSIC, T. Security Risk Management in complex organization. 2015.

SEMOLA, M. Gestão da Segurança da Informação: Uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2013.

SILVA, M. M. A multidimensional approach to information security risk management using (FMEA) and fuzzy theory, 2014

STONEBURNER, G., GOGUEM, A., FERINGA, A.. Risk Management Guide For Information Technology Systems – NIST SP 800-30 - Recommendations of the national institute of Standards and Technology. EUA, 2002.

SUSSY, Bayona. ISO/IEC 27001 implementation in public organizations: A case study. In: Information Systems and Technologies (CISTI), 2015 10th Iberian Conference on. IEEE, 2015. p. 1-6.

TRESCA, R. P.; DE ROSE JÚNIOR, D. Estudo comparativo da motivação intrínseca em escolares praticanteas e näo praticantes e näo praticantes de dança. Rev. bras. ciênc. mov, [S.l.], v.8, n.1, p.9–13, 2000.

TUYIKEZE, Tite; FLOWERDAY, Stephen. Information Security Policy Development and Implementation: A Content Analysis Approach. In:HAISA. 2014. p. 11-20.

WHITMAN, Michael E.; MATTORD, Hebert J.; Principles of Information Security. EUA: Course Technology, 2003. 560 p. ISBN: 0619216255

YEO, M. L. Risk Mitigation Decisions for IT Security. ACM Trans. Manage, 2014