Pós-Graduação em Ciência da Computação

EVANDRO SOUZA DE PAULA CORDEIRO

FATORES CRITICOS DE SUCESSO PARA O APRIMORAMENTO DA MATURIDADE DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO DAS INSTITUIÇOES FEDERAIS DE ENSINO SUPERIOR

Universidade Federal de Pernambuco
posgraduacao@cin.ufpe.br
www.cin.ufpe.br/~posgraduacao

RECIFE
2017

Evandro Souza de Paula Cordeiro

FATORES CRITICOS DE SUCESSO PARA O APRIMORAMENTO DA MATURIDADE DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO DAS INSTITUIÇOES FEDERAIS DE ENSINO SUPERIOR

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. José Gilson de Almeida Teixeira Filho, Doutor

RECIFE

2017

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

C794f Cordeiro, Evandro Souza de Paula
Fatores críticos de sucesso para o aprimoramento da maturidade da gestão da segurança da informação das instituições federais de ensino superior / Evandro Souza de Paula Cordeiro. – 2017.
199 f.: il., fig., tab.

Orientador: José Gilson de Almeida Teixeira Filho.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2017.
Inclui referências, apêndices e anexos.

1. Segurança da informação. 2. Maturidade. I. Teixeira Filho, José Gilson de Almeida (orientador). II. Título.

005.8 CDD (23. ed.) UFPE- MEI 2017-68

Evandro Souza de Paula Cordeiro

Fatores Críticos de Sucesso para o Aprimoramento da Maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior

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 15 de fevereiro de 2017.

Aprovado em: 15/02/2017.

BANCA EXAMINADORA

_____

Prof. Dr. Leandro Maciel Almeida
Centro de Informática / UFPE

_____

Prof. Dr. Décio Fonseca
Centro de Ciências Sociais e Aplicadas / UFPE

_____

Prof. Dr. José Gilson Teixeira de Almeida Filho
Centro de Ciências Sociais e Aplicadas / UFPE
(Orientador)

Dedico este trabalho aos meus pais, Paulo José de Paula Cordeiro e Edmara Ribeiro de Souza Cordeiro, pela cobrança durante os tempos de escola, pelo total apoio na vida acadêmica e pelos ensinamentos que levaram a formação do meu caráter.

AGRADECIMENTOS

Agradeço primeiramente a Deus e ao meu Senhor Jesus Cristo, pelo dom da vida e pelas muitas bênçãos que venho recebendo todos esses anos e por mais esta conquista.

A minha família, especialmente a minha amada esposa Gigliane Pereira da Silva Marques e aos meus filhos Enzo e Levi, pelo apoio e compreensão. Ao meu irmão e irmã, que sempre me apoiaram.

Ao Instituto Federal de Rondônia – Reitoria, pelo apoio.

Ao meu orientador, professor Dr. José Gilson de Almeida Teixeira Filho, pela confiança e orientação em todas as etapas da pesquisa.

Um agradecimento especial aos meus amigos Jhordano Malacarne Bravim, Fábio Mamoré Conde e Orlivaldo Kleber Lima Rios, pelo apoio, ajustes e ideias que auxiliaram na confecção deste trabalho.

A todos os colegas de mestrado que compartilharam comigo os momentos de aprendizado, em especial à Denilson Souza do Nascimento, Joilson Dantas Siqueira Silva e Gleidson Antonio da Silva Sa Barreto.

A todas as instituições participantes desse estudo, diretorias de tecnologia da informação e seus profissionais.

Ao programa de pós-graduação de mestrado profissional em ciência da computação do Centro de Informática da Universidade Federal de Pernambuco e a todos os professores e colaboradores.

Enfim, a todos aqueles que contribuíram de forma direta ou indireta para a conclusão deste trabalho de pesquisa.

“O que não se conhece não se pode controlar.
O que não se controla não se pode mensurar.
O que não se mensura não se pode gerenciar.
O que não se gerencia não se pode aprimorar. “
Marcos Sêmola

RESUMO

O Índice de Governança da TI de 2014 (iGovTI2014), realizado pelo Tribunal de Contas da União, através da Secretaria de Fiscalização de TI, apresentou o quadro crítico da Gestão Corporativa de Segurança da Informação em que se encontram os órgãos da Administração Pública Federal. Considerando esse quadro crítico, este trabalho teve como objetivo identificar os fatores críticos de sucesso responsáveis pelo aprimoramento da maturidade da gestão da segurança da informação das Instituições Federais de Ensino Superior. A metodologia aplicada baseou-se nas abordagens quantitativa e qualitativa, utilizando procedimentos bibliográficos, através de uma revisão sistemática da literatura, e a técnica de estudo de campo com a aplicação de dois questionários: (1) baseado no *Information Security Program Assesment Tool* da EDUCAUSE, buscou diagnosticar a maturidade da gestão da segurança da informação das instituições pesquisadas e identificar as melhores avaliadas. O diagnóstico da maturidade foi organizado em duas etapas: Maturidade Geral da Gestão da Segurança da Informação e Maturidade por Domínio; (2) baseado nos fatores críticos de sucesso encontrados na revisão sistemática, buscou identificar o grau de importância dos fatores para o aprimoramento da maturidade de gestão da segurança da informação das instituições pesquisadas. Cada fator encontrado foi explicado com detalhes, dando maior ênfase àqueles com maior grau de importância. Como resultado, foram identificados 12 fatores considerados críticos para o aprimoramento da maturidade da gestão da segurança da informação das instituições federais de ensino superior, dentre eles destacaram-se os fatores Treinamento e Conscientização, Gestão de Riscos, Cultura de Segurança da Informação e Apoio da Alta Gestão.

Palavras-chave: Gestão de Segurança da Informação. Maturidade. Fatores Críticos de Sucesso. Instituições Federais de Ensino Superior.

ABSTRACT

The IT Governance Index of 2014 (iGovTI2014), carried out by the Federal Audit Court through the IT Supervisory Secretariat, presented the critical situation of the Corporate Information Security Management in which the Federal Public Administration agencies are located. Considering this critical framework, this work aimed to identify the critical success factors responsible for improving the maturity of the information security management of the Federal Institutions of Higher Education. The applied methodology was based on the quantitative and qualitative approaches, using bibliographic procedures, through a systematic review of the literature, and the technique of field study with the application of two questionnaires: (1) based on EDUCAUSE's Information Security Program Assessment Tool, sought to diagnose the information security management maturity of the institutions surveyed and identify the best evaluated ones. The diagnosis of maturity was organized in two stages: General Maturity of Information Security Management and Maturity by Domain; (2) based on the critical success factors found in the systematic review, sought to identify the degree of importance of the factors to improve maturity. Each factor was explained in detail, giving greater emphasis to those with greater degree of importance. As a result, 12 critical factors were identified for improving the maturity of the information security management of the federal institutions of higher education, among them stood out the factors Training and Awareness, Risk Management, Information Security Culture and High Management Support.

Keywords: Information Security Management. Maturity. Critical Success Factors. Federal Institutions of Higher Education.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIAÇÕES

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
COBIT	Control Objectives for Information and related Technology
DSIC	Departamento de Segurança da Informação e Comunicações
FCS	Fatores Críticos de Sucesso
GSI	Gestão de Segurança da Informação
GSIPR	Gabinete de Segurança Institucional da Presidência da República
HEISC	Higher Education Information Security Council
IEC	International Electrotechnical Commission
IFES	Instituição Federal de Ensino Superior
iGovTI	Índice de Governança de TI
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSEA	Internationl Systems Security Engineering Association
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
LDBEN	Lei de Diretrizes e Bases da Educação Nacional
MEC	Ministério da Educação
O-ISM3	Open Information Security Management Maturity Model
RSL	Revisão Sistemática da Literatura
SEFTI	Secretaria de Fiscalização de Tecnologia da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação

SSE-CMM Systems Security Engineering – Capability Maturity Model

TCU Tribunal de Contas da União

TI Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

A administração pública, dotada pelos governos tem sofrido mudanças ao longo dos tempos, em especial motivadas pelas mudanças da sociedade e pela globalização que o mundo enfrenta hoje em dia. Todas estas transformações atingem a administração pública e fazem com que esta esteja apta para responder cada vez com mais agilidade e qualidade (BRAVIM, 2015). Para isso, é necessário comprometimento com modernas práticas de gestão, distanciando-se do antigo modelo burocrático (CARNEIRO, 2010, apud Bravim, 2015). Neste cenário de crescimento, a informação manipulada nestas instituições deve ser devidamente protegida, garantindo assim a continuidade do negócio. A Gestão da Segurança da Informação (GSI) deve alinhar-se aos objetivos estratégicos de negócio, ocupando lugar de destaque nas tomadas de decisões que influenciam o modelo de trabalho das organizações.

Segundo o acórdão 1.603/2008, é responsabilidade dos órgãos e entidades vinculadas a Administração Pública Federal (APF) promover a segurança das informações, mitigando os riscos de indisponibilidade de suas operações, a fim de atingir seus objetivos institucionais (BRASIL, 2008). Este mesmo acórdão evidencia a importância das informações nos órgãos públicos quanto ao correto tratamento para com a confidencialidade, a integridade e a disponibilidade, além da autenticidade, da responsabilidade e da garantia de não repúdio.

A falta de um diagnóstico adequado de GSI pode levar a instituição a adotar controles menos eficientes do que deveriam, expondo-a ao risco. Por outro lado, pode ocorrer o desperdício de recursos em controles superdimensionados (RIGON e WESTPHALL, 2013).

Neste contexto surgem os modelos de maturidade que servem como guia para que a organização identifique onde e como está de acordo com as métricas estabelecidas nestes modelos. De acordo com ITGI (2007), a vantagem em se utilizar um modelo de maturidade está no detalhamento que os gerentes terão ao analisarem os processos, avaliar as variáveis envolvidas e se há necessidade de melhoria. Com isso, é possível enxergar os principais fatores responsáveis pela atual situação de maturidade da organização, focando seus esforços naqueles considerados críticos ao negócio.

O presente trabalho identificou os Fatores Críticos de Sucesso (FCS) necessários para aprimorar o nível de maturidade da GSI nas Instituições Federais de Ensino Superior (IFES), através de um diagnóstico de maturidade, utilizando a *Information Security Program Assessment Tool*[1] disponibilizado pelo *Higher Education Information Security Council*[2] (HEISC) da EDUCAUSE, de uma Revisão Sistemática da Literatura e das normas de segurança internacionalmente reconhecidos como a ISO/IEC 27001, 27002, 27005 e 21827.

Este primeiro capítulo apresenta uma visão introdutória e geral do trabalho de pesquisa e está subdividido nas seguintes seções:

- **Motivação:** seção responsável por passar ao leitor o contexto, a motivação e a justificativa para realização desta dissertação;
- **Problema da Pesquisa:** seção responsável por apresentar a questão a ser respondida pela pesquisa em questão;
- **Objetivos:** especifica os objetivos geral e os objetivos específicos do trabalho;
- **Contribuição Científica:** apresenta as contribuições que este trabalho de pesquisa trará a ciência.
- **Metodologia da Pesquisa:** seção responsável por apresentar a metodologia, técnicas e métodos utilizados para se atingir o objetivo da pesquisa;
- **Organização da Dissertação:** esta seção demonstra de maneira geral como estão organizados os tópicos principais deste trabalho de pesquisa.

1.1 Motivação

A norma complementar 02/IN01/DSIC/GSIPR, através da Instrução Normativa 01, de 13 de junho de 2008, elaborada pelo Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR), define a metodologia de gestão de segurança da informação e comunicações que deve ser utilizada pelos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

---

[1] Ferramenta de Avaliação do Programa de Segurança da Informação

[2] Conselho de Segurança da Informação do Ensino Superior

> A administração pública no Brasil se divide em direta e indireta. No âmbito do Executivo Federal, a primeira é composta pela Presidência da Republica, os ministérios e as secretarias especiais. Já a administração indireta é composta por órgãos com personalidade jurídica própria, mas que desempenham funções do Estado de maneira descentralizada e em todas as esferas – federal, estadual, distrital e municipal (Brasil 2012).

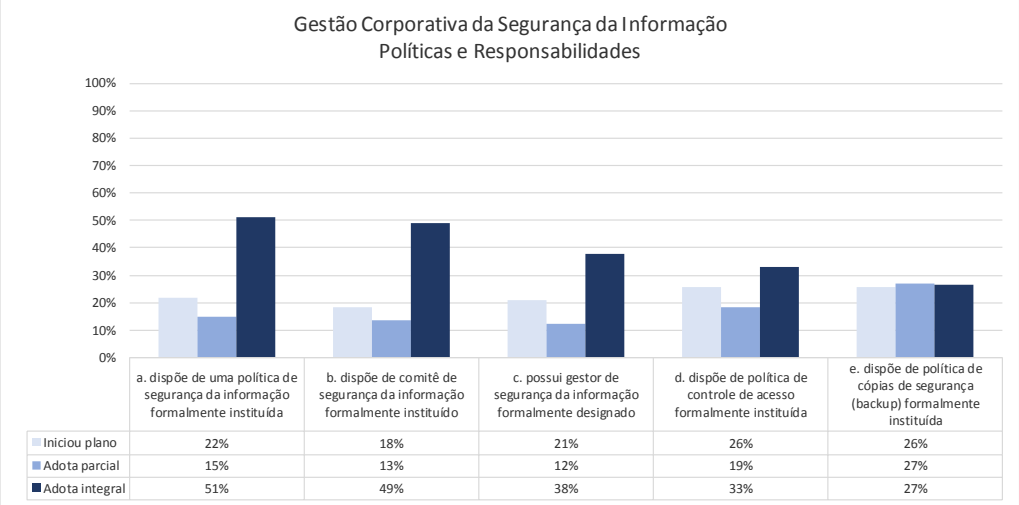
Num primeiro levantamento de governança de TI realizado no ano de 2007 pelo Tribunal de Contas da União (TCU) nas instituições da APF, revelou uma situação preocupante quanto ao tratamento dado pelos órgãos públicos a segurança das informações sob sua responsabilidade, na oportunidade a norma utilizada para avaliar os aspectos da segurança da informação foi a NBR ISO/IEC 17799:2005.

Em 2010, um novo levantamento foi realizado, utilizando a norma NBR ISO/IEC 27002:2005 como critério de avaliação da segurança da informação, como resultado o acórdão 2.308/2010-TCU-Plenário revelou que não houve melhoras nos indicadores de segurança da informação em relação ao levantamento de 2007. Neste mesmo período, o TCU criou o iGovTI (índice de Governança de TI), buscando refletir a situação da governança de TI das instituições avaliadas.

Em 2012, por meio do Acórdão 2.308/2010-TCU-Plenário, a Secretaria de Fiscalização de Tecnologia da Informação (Sefti) estabeleceu um processo de avaliação da governança de TI na APF em ciclos de dois anos (BRASIL, 2014).

Nos anos de 2012 e 2014 novos levantamentos foram realizados, demonstrando que as medidas adotadas pelos órgãos governamentais superiores e pelo TCU estavam surtindo efeito. O ultimo levantamento, realizado em 2014, demonstrou uma melhora nos índices da Gestão Corporativa da Segurança da Informação, como pode ser visto na Figura 1.

Figura 1. Situação da Gestão da Segurança da Informação em 2014

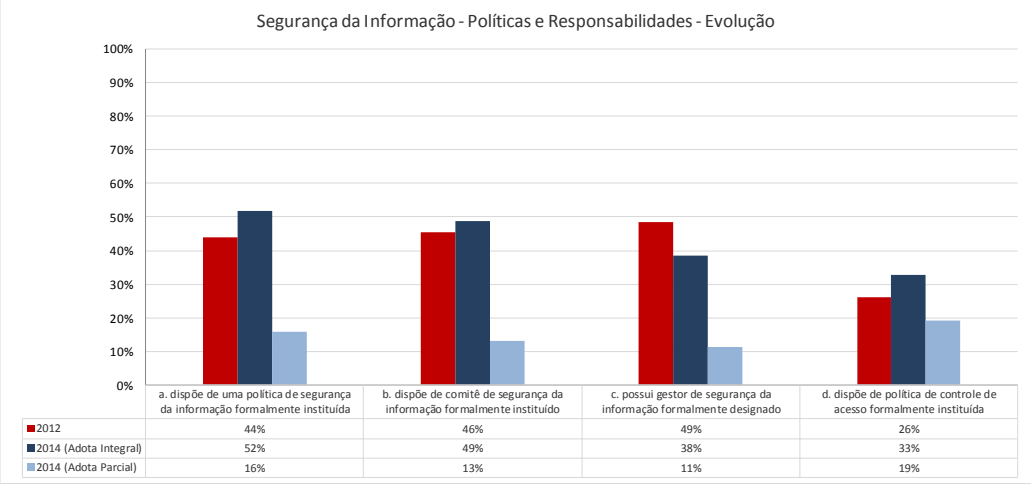


	a. dispõe de uma política de segurança da informação formalmente instituída	b. dispõe de comitê de segurança da informação formalmente instituído	c. possui gestor de segurança da informação formalmente designado	d. dispõe de política de controle de acesso formalmente instituída	e. dispõe de política de cópias de segurança (backup) formalmente instituída
Iniciou plano	22%	18%	21%	26%	26%
Adota parcial	15%	13%	12%	19%	27%
Adota integral	51%	49%	38%	33%	27%

Fonte: Brasil (2014)

Quanto ao aspecto da Segurança da Informação o crescimento não foi significativo (BRASIL, 2015). Um comparativo entre os últimos anos (2012 e 2014) em que foi realizado o iGovTI pode ser melhor observado na Figura 2.

Figura 2. Situação da GSI – Comparativo 2012 x 2014



	a. dispõe de uma política de segurança da informação formalmente instituída	b. dispõe de comitê de segurança da informação formalmente instituído	c. possui gestor de segurança da informação formalmente designado	d. dispõe de política de controle de acesso formalmente instituída
2012	44%	46%	49%	26%
2014 (Adota Integral)	52%	49%	38%	33%
2014 (Adota Parcial)	16%	13%	11%	19%

Fonte: Brasil (2014)

É possível observar que apenas 8 pontos percentuais subiram, entre os levantamentos de 2012 e 2014, no domínio Política de Segurança da Informação. Outro fator avaliado foi o comitê de segurança da informação formalmente instituído, neste domínio apenas 3 pontos percentuais diferem os levantamentos de 2012 e 2014. Este resultado demonstra a baixa maturidade em que os órgãos da APF estão com relação a gestão da segurança da informação.

E é exatamente nesse cenário atual vivido pelos órgãos da APF, que se encontrou a motivação para a realização deste trabalho em identificar os fatores críticos de sucesso para aprimorar o nível de maturidade da Gestão de Segurança da Informação nas Instituições Federais de Ensino Superior (IFES), levando em consideração a especificidade dessas instituições e utilizando como base as normas ABNT NBR ISO/IEC 27001, 27002, 27005 e a ISO/IEC 21827.

Como resultado, esta pesquisa buscou realizar um diagnóstico de maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior e identificar os Fatores Críticos de Sucesso (FCS) e o seu grau de importância para o aprimoramento dessa maturidade.

1.2 Problema da Pesquisa

Diante do baixo índice de gestão corporativa da segurança da informação nos órgãos e entidades da APF, dos quais as IFES também fazem parte, surge a seguinte questão de pesquisa: **Quais Fatores Críticos de Sucesso podem aprimorar o nível de maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior?**

1.3 Objetivos

Esta seção descreve o objetivo geral da pesquisa e os objetivos específicos necessários para que o primeiro possa ser alcançado.

1.3.1 Objetivo Geral

Identificar os fatores críticos de sucesso para o aprimoramento do nível de maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior.

1.3.2 Objetivos Específicos

Para alcançar o objetivo geral acima enunciado, os seguintes objetivos específicos devem ser seguidos:

- Realizar levantamento bibliográfico referente aos conceitos, regulamentos e modelos de melhores práticas de Gestão de Segurança da Informação gerais e no âmbito da Administração Pública Federal;
- Realizar uma revisão sistemática da literatura, buscando os principais trabalhos científicos relevantes ao tema da pesquisa;
- Diagnosticar a maturidade de Gestão de Segurança da Informação das Instituições Federai de Ensino Superior por meio da aplicação de um questionário;
- Inserir os dados coletados do questionário no *Information Security Program Assesment Tool* do HEISC para avaliação de maturidade;
- Identificar os fatores críticos de sucesso e o seu grau de importância para aprimorar os níveis de maturidade de Gestão de Segurança da Informação das Instituições Federai de Ensino Superior;
- Consolidar os dados referente ao grau de importância dos fatores críticos de sucesso com os níveis de maturidade de Gestão de Segurança da Informação, possibilitando as Instituições Federais de Ensino Superior focar seus esforços nos fatores mais importantes para alcance dos níveis adequados.

1.4 Metodologia da Pesquisa

Este tópico apresenta os métodos de pesquisa aplicados na elaboração deste trabalho. De acordo com Waslawick (2014), o método de pesquisa descreve o caminho para se atingir o objetivo proposto, ou seja, se os passos definidos no método forem executados, os resultados obtidos serão satisfatórios. A metodologia utilizada pode ser melhor observada no Quadro 1.

Quadro 1. Metodologia Científica Aplicada a Pesquisa

METODOLOGIA	ESPECIFICAÇÕES
Método	Indutivo
Natureza	Aplicada
Objetivo	Descritiva e Exploratória
Abordagem	Quantitativa e Qualitativa
Procedimentos utilizados	Bibliográfico Documental Levantamento (Survey)

Técnicas de Coleta de Dados	Questionário
Perspectiva e Área de Concentração	Sistemas de Informação - Segurança da Informação

Método cientifico é o conjunto de processos ou operações mentais que se devem empregar na investigação, ou seja, é a linha de raciocínio adotada no processo de pesquisa (SILVA e MENEZES, 2005). Os mesmos autores informam que os métodos que fornecem as bases lógicas para uma investigação são: dedutivo, indutivo, hipotético-dedutivo, dialético e fenomenológico.

Este trabalho de pesquisa utilizou-se do **método indutivo**, para o alcance do objetivo proposto. Esse método é caracterizado pelo fato de que o pesquisador parte da observação de fatos ou fenômenos cujas causas deseja conhecer, partindo de algo mais particular para uma questão mais ampla. Silva e Menezes (2005), afirmam que esse método considera que o conhecimento é fundamentado na experiência, não levando em conta princípios preestabelecidos.

Segundo Waslawick (2014) e Silva e Menezes (2005), a classificação de uma pesquisa pode ter os seguintes pontos de vista: quanto a sua natureza; quanto aos objetivos; quanto à abordagem do problema; e quanto aos procedimentos técnicos. Ainda de acordo com os mesmos autores, a presente pesquisa foi classificada da seguinte forma:

- **Quanto à natureza**:
    - **Aplicada**, pois gera conhecimentos para aplicações práticas, voltados a solução de problemas específicos. Esses conhecimentos foram adquiridos por meio de um levantamento e diagnóstico do nível de maturidade da gestão de segurança da informação (GSI) das instituições federais de ensino superior (IFES), posteriormente foram identificando os fatores críticos de sucesso e o seu grau de importância para o aprimoramento dessa maturidade.
- **Quanto aos objetivos**:
    - **Descritiva**, pois os fatos foram observados, registrados, analisados, classificados e interpretados, utilizando como técnica de coleta de dados um questionário;

- **Exploratória**, pois visa proporcionar maior familiaridade com o problema para torna-lo explicito ou para construir hipóteses. Foram realizadas pesquisas bibliográficas, revisão sistemática da literatura e levantamento de dados por meio da aplicação de um questionário, buscando identificar a atual situação de maturidade da GSI das IFES.

- **Quanto a abordagem do problema**:
  - **Quantitativa**, pois apresenta números e porcentagens originados a partir da coleta de dados (questionário) aplicada as IFES, dessa forma, foi possível utilizar recursos estatísticos, como a porcentagem, para a análise e apresentação dos resultados;
  - **Qualitativa**, pois foi identificado uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. A interpretação dos fenômenos e a atribuição de significados foram alcançadas através revisão sistemática da literatura, levantamento bibliográfico, documentos oficiais e nas informações adquiridas no estudo de campo. Dessa forma, foi possível alcançar os fatores críticos para o aprimoramento da maturidade de GSI.

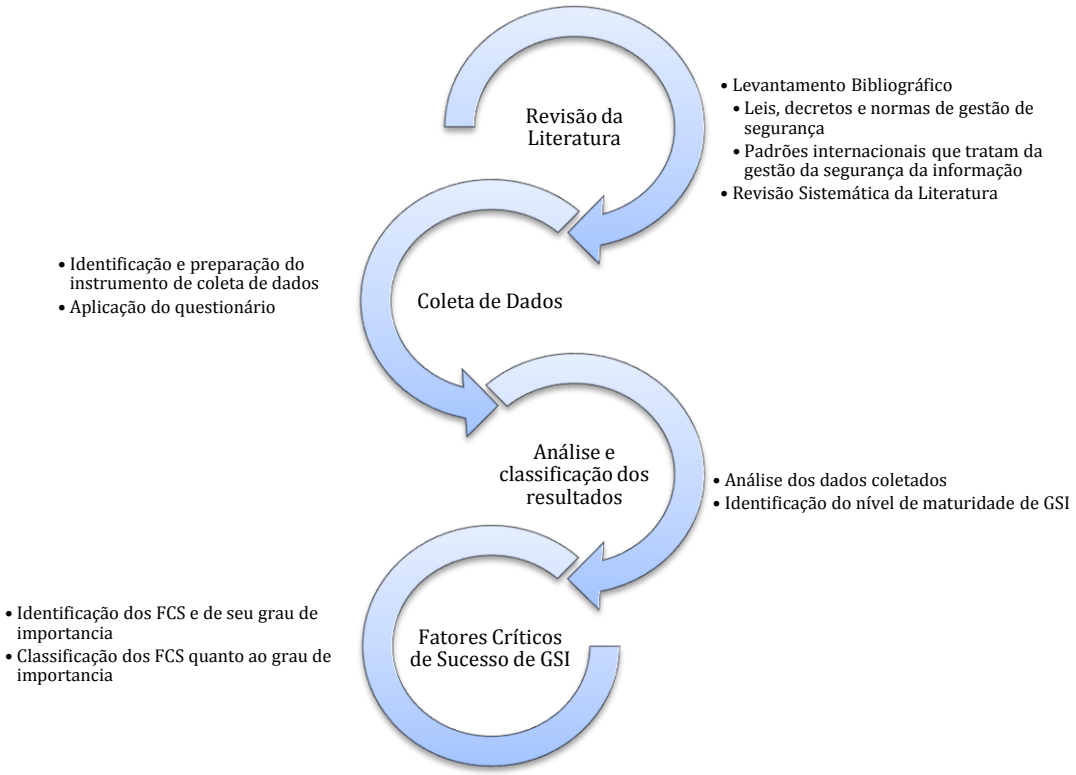
- **Quanto aos procedimentos técnicos**:
  - **Bibliográfica**, pois implica o estudo de artigos, teses, livros e outras publicações usualmente disponibilizadas por fontes indexadas, sendo um estudo sistematizado e compilado. Neste trabalho utilizou-se de uma revisão sistemática da literatura, onde foi possível identificar os trabalhos científicos mais relevantes para o tema pesquisado. Dentre os trabalhos encontrados estão artigos de periódicos, monografias, dissertações e teses. A Revisão Sistemática está melhor detalhada no APÊNDICE A. A;
  - **Documental**, pois implica o estudo de materiais que ainda não receberam tratamento analítico. Neste caso, foram utilizados documentos oficiais do governo federal, como os levantamentos realizados pelo Tribunal de Contas da

União, Instruções Normativas, Normas Complementares, Decretos e Leis relacionadas ao tema segurança da informação nos órgãos da Administração Pública Federal.

- **Levantamento,** pois envolveu a interrogação direta das pessoas cujo comportamento se deseja conhecer. Desta forma, foi disponibilizado um questionário as Diretorias de Tecnologia da Informação das IFES, buscando-se conhecer a atual situação da maturidade da segurança da informação e identificação do grau de importância dos fatores críticos de sucesso para aprimoramento da maturidade de GSI.

O planejamento de um trabalho de pesquisa deve representar a lógica que interliga todas as fases da pesquisa, desde seu início até as conclusões e resultados a serem alcançados (YIN, 2013). Esta pesquisa pode ser dividida em quatro fases ou etapas, conforme Figura 3:

Figura 3. Fases do projeto de pesquisa



1.5 Estrutura da Dissertação

Esta dissertação está organizada em seis capítulos. No primeiro capítulo é realizada uma introdução ao tema da pesquisa, as motivações, objetivos pretendidos e a metodologia de pesquisa.

No capítulo 2 é descrito o referencial teórico e revisão sistemática da pesquisa, sendo o responsável por apresentar um arcabouço teórico e conceitual sobre o tema, descrevendo os principais conceitos-chave que estão alinhados com o problema e objetivos definidos na pesquisa.

No capítulo 3 é apresentado sobre como foi realizado o levantamento dos dados para realização do diagnóstico da maturidade da GSI, o instrumento de pesquisa e o cálculo da amostra da população.

No capítulo 4 foi realizado o diagnóstico de fato da maturidade da GSI, avaliando os dados colhidos após a aplicação do questionário e analisando os resultados.

No capítulo 5 são definidos os fatores críticos de sucesso e seu grau de importância para o aprimoramento do nível de maturidade de GSI das IFES.

No capítulo 6 são apresentadas as conclusões a respeito da pesquisa, suas contribuições e apontados os trabalhos futuros.

2 REFERENCIAL TEÓRICO

Este capítulo é responsável por apresentar um arcabouço teórico e conceitual sobre o tema, descrevendo os principais conceitos-chave que estão alinhados com o problema e objetivos definidos na pesquisa (Gunther, 2004). Ele está subdividido nas seguintes seções:

- **Segurança da Informação:** essa seção apresenta os conceitos relacionados a área de segurança da informação, sua gestão e importância para as organizações;
- **Publicações Oficiais de GSI no Âmbito da APF:** apresenta as principais publicações oficiais relacionadas a segurança da informação no âmbito da APF;
- **Modelos de Maturidade:** apresenta os conceitos principais por traz dos modelos de maturidade, e apresenta alguns modelos já conceituados no mercado;
- **Fatores Críticos de Sucesso (FCS):** apresenta os conceitos a respeito dos FCS e os trabalhos já publicados sobre o tema;
- **Revisão Sistemática da Literatura:** apresenta os procedimentos realizados para selecionar os principais trabalhos científicos relacionados ao tema dessa pesquisa, utilizando as principais bases científicas;

2.1 Segurança da Informação

Segundo a norma ABNT NBR ISO/IEC 27002:2013, a segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança. Todos esses controles necessitam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados para que assegurem que os objetivos de negócio e a segurança da informação da organização sejam atendidos. Esta segurança pode ser obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.

Três princípios básicos norteiam a implementação da prática da Segurança da Informação, são eles (SÊMOLA, 2013):

- Confidencialidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação do seu acesso e uso apenas às pessoas autorizadas.
- Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protege-la contra alterações indevidas, intencionais ou acidentais.
- Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento me que eles necessitem delas para qualquer finalidade.

Sêmola (2013) também afirma que o modelo de gestão corporativa de segurança da informação relaciona-se diretamente com os desafios do negócio e que diante dessa abrangente orientação, dois outros conceitos ganham autonomia:

- Autenticidade – É um conceito extraído dos precursores confidencialidade e integridade, originalmente, cumprindo o papel de sinalizar o comprometimento de aspectos associados a autenticidade das informações e das partes envolvidas na sua troca.
- Conformidade – Tem o papel de garantir o cumprimento das obrigações organizacionais, englobando desde compromissos com *stakeholders* a aspectos legais e regulatórios relacionados á administração das empresas.

Os requisitos de segurança da informação devem ser identificados para que os controles adequados sejam estabelecidos. Torres et al. (2010), afirma que esses requisitos podem ser identificados por meio de análises sistemáticas dos riscos de segurança da informação, através das quais ajudarão a direcionar e estabelecer as ações apropriadas e as prioridades gerenciais dos riscos, na implementação dos controles definidos para a proteção contra esses riscos.

Jirasek (2012, apud Rigon et al., 2013), afirmam que é necessário uma avaliação crítica e sistemática dos controles de segurança da informação pois as tecnologias, processos de negócios

e as pessoas mudam constantemente, alterando o nível dos riscos atuais e criando novos riscos para a organização.

Com a identificação dos requisitos de segurança, seus riscos e as decisões de tratamento desses riscos, controles apropriados devem ser implementados para que eles sejam reduzidos a níveis toleráveis dentro da estratégia organizacional. Esses controles podem ser selecionados a partir de uma norma vigente ou criados, visando atender as necessidades de segurança da organização, estando em total conformidade com a legislação e regulamentações específicas, nacional e internacional (TORRES et al., 2010).

2.1.1 Gestão de Segurança da Informação (GSI)

As organizações em diferentes ramos de atividades, sejam elas públicas ou privadas, possuem diferentes requisitos de negócios e tolerância aos riscos. Sendo assim, para que o processo de segurança da informação seja eficaz, este deve ser documentado, medido e gerenciado corretamente (The Open Group, 2011).

Os aspectos principais de gestão da segurança da informação podem ser elencados da seguinte forma (COELHO et al., 2014):

- Preparando a organização – antes de se pensar em gestão da segurança da informação em uma organização, é preciso definir que ativos da organização necessitam de proteção, quais ameaças podem afetar a organização, de que forma e por quem essas ameaças podem ser exploradas, como cada recurso de informação participa do processo de negócio, que requisitos de proteção o negócio exige e que nível de proteção é necessário, que recursos estão disponíveis para os objetivos de segurança e o que pode ser feito com os recursos existentes e o que a alta gestão espera da segurança da informação para o negócio da organização;
- Requisitos de Segurança – considera-se neste aspecto a análise e avaliação de riscos da organização, legislação vigente, estatutos, regulamentações e cláusulas contratuais da organização e os conjuntos de princípios, objetivos e requisitos do negócio;

- Análise/avaliação de riscos – gastos com controles precisam ser balanceados de acordo com os dados potenciais, resultados devem direcionar e determinar as ações gerenciais e tarefas periódicas devem ser realizadas para se contemplar mudanças;
- Seleção de controles – controles devem ser implementados para garantir a redução de riscos, são dependentes das decisões da organização e podem ser selecionados a partir de normas preestabelecidas ou de conjunto de controles específicos, como as normas ABNT NBR ISO/IEC 27001:2013 e 27002:2013;
- Itens relevantes – política de segurança da informação, segurança organizacional, gestão de ativos, segurança em recursos humanos, segurança física e do ambiente, gestão das operações e comunicações, controle de acesso, gestão de incidentes de segurança da informação e gestão de continuidade do negócio;
- Atividades envolvidas – gerencia de segurança dos sistemas, dos serviços de segurança, dos mecanismos de segurança e da auditoria de segurança.

De acordo com Dey (2007), as normas de segurança da informação fornecem uma abordagem de gerenciamento sistemática adotada para melhoria das práticas de segurança, contribuindo para qualificar um nível aceitável de risco e implementar medidas apropriadas de segurança que garantam os pilares da segurança da informação: integridade, disponibilidade e confidencialidade. Uma norma tem o propósito de definir regras, padrões e instrumentos de controle que garantam uma padronização a um processo, produto ou serviço (SÊMOLA, 2014).

As principais referências normativas específicas para a GSI são as normas da "família 27000" da Organização Internacional de Normatização (ISO), conforme Quadro 2.

Quadro 2. Normas da "família" ISO/IEC 27000

NORMAS	DESCRIÇÃO
ABNT NBR ISO/IEC 27001:2013	Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI) documentado dentro do contexto dos riscos do negócio. Ela especifica requisitos para implementação de controles de segurança personalizados para as necessidades individuais das organizações ou suas partes.
ABNT NBR ISO/IEC 27002:2013	Esta norma fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

ABNT NBR ISO/IEC 27004:2010	Esta Norma fornece diretrizes para o desenvolvimento e uso de métricas e medições a fim de avaliar a eficácia de um Sistema de Gestão de Segurança da Informação (SGSI) implementado e dos controles ou grupos de controles, conforme especificado na ABNT NBR ISO/IEC 27001.
ABNT NBR ISO/IEC 27005:2011	Esta norma fornece diretrizes para o processo de gestão de riscos de segurança da informação.

Fonte: ABNT Catálogo (2016)

GSI é um processo dinâmico de tomada de decisões contínua que envolve todos os componentes cruciais como a infraestrutura organizacional, fatores humanos e práticas de segurança da informação (TU, 2015).

2.1.1.1 ABNT NBR ISO/IEC 27002

A norma ISO/IEC 27002, anteriormente conhecida como ISO/IEC 17799:2000, e derivada da primeira parte da norma britânica BS 7799, define um código de prática para a gestão de segurança da informação (SÊMOLA, 2014). Ainda segundo mesmo autor, além de quatro seções iniciais, que definem os aspectos gerais de segurança da informação, a norma contém 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles. Esta norma pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas para uma instituição, ou seja, não é necessário que todos os controles e diretrizes contidos na norma precisem ser aplicados. Além do mais, controles adicionais e recomendações de outros frameworks podem ser necessários (ABNT, 2013).

Coelho et al. (2014a, p.19) afirma que:

> A norma ISO/IEC 27002:2013 (Tecnologia da Informação – técnicas de segurança – Código de prática para controles de segurança da informação), foi preparada para servir como um guia prático para o desenvolvimento e a implementação de procedimentos e controles de segurança da informação em uma organização (COELHO et al., 2014a, p.19).

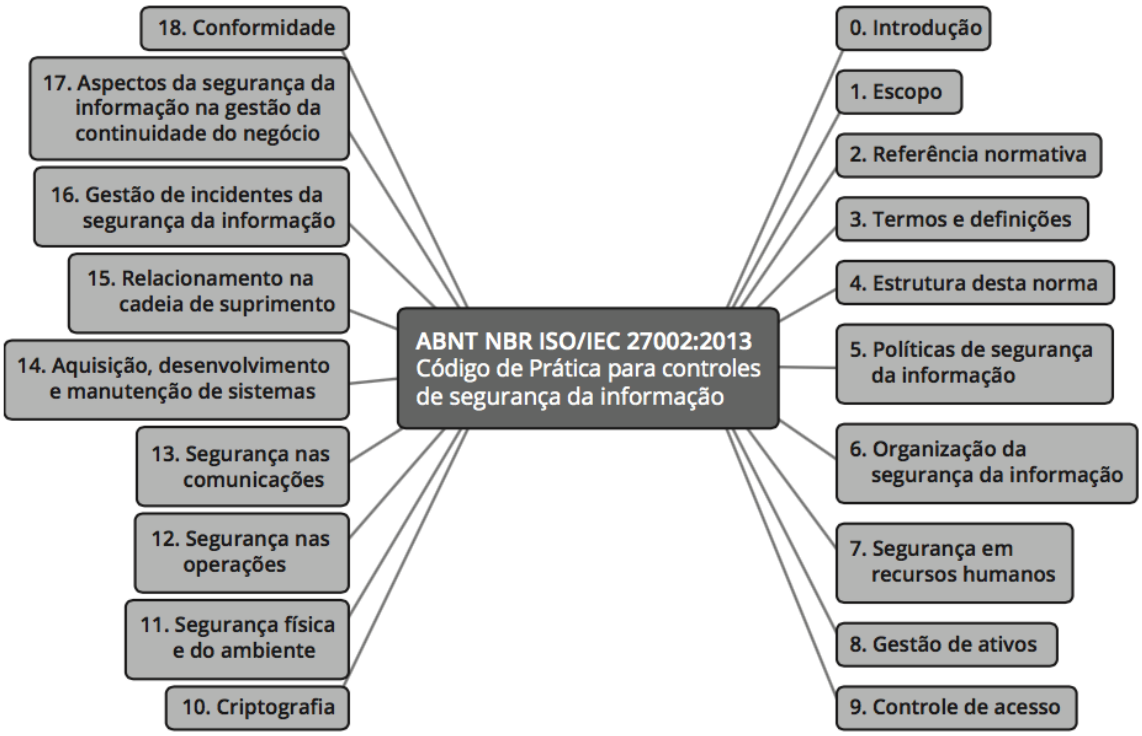
Sêmola (2014), informa que a ISO 27002 não tem as mesmas características de certificação da norma ISO 27001, mas sugere, por meio de um modelo menos formal, a preocupação com aspectos importantes e a utilização de controles que orientem as organizações a reduzir os riscos operacionais, que potencialmente causariam impactos aos negócios. O mesmo autor afirma o objetivo da norma é orientar as organizações que estão frente ao desafio do

gerenciamento da segurança da informação, apontando “o que” fazer, sem se preocupar com os detalhes associados ao “como” fazer.

A norma ABNT NBR ISO/IEC 27002, afirma que esta norma é considerada como um ponto de partida para a elaboração de diretrizes específicas das organizações, de forma que nem todos os controles e diretrizes contidos na norma precisam ser aplicados, além disso podem ser necessários outros controles não especificados na norma. Se novos controles forem desenvolvidos, é recomendável realizar uma referência cruzada com as seções da Norma para facilitar a verificação de conformidade por auditores e parceiros (ABNT, 2013).

O documento que compõe a norma ABNT NBR ISO/IEC 27002 de 2013, está estruturado em 18 capítulos, dos quais do 0 ao 4 são apresentados os temas introdutórios da Norma e do 5 ao 18 estão as 14 seções de controles de segurança da informação, conforme ilustrado na Figura 4.

Figura 4. Seções da Norma ABNT ISO/IEC 27002:2013



Fonte: Coelho et al. (2014a)

Os controles da norma ABNT NBR ISO/IEC 27002 de 2013, são utilizados para avaliação da maturidade no instrumento de coleta de dados adotado nesta pesquisa. Este instrumento está melhor detalhado na seção 3.2 deste trabalho.

2.1.2 Sistema de Gestão de Segurança a Informação (SGSI)

O Sistema de Gestão de Segurança da Informação (SGSI), do inglês *Information Security Management System (ISMS),* é um processo estruturado de tratamento da segurança da informação em vários setores. O SGSI é o resultado da aplicação planejada de objetivos, diretrizes, politicas, procedimentos, modelos e outas medidas administrativas que de forma conjunta, definem como são reduzidos os riscos para segurança da informação (SILVA, 2009). Ainda segundo a mesma autora, ele tem por finalidade proteger os recursos da empresa diminuindo o nível de exposição aos riscos existentes em todos os ambientes. Dessa forma a organização tem liberdade para criação de novas oportunidades de negócio.

Coelho et al. (2014) afirma que a adoção de um SGSI deve ser uma decisão estratégica para a organização, pois sua especificação e implementação são influenciadas pelas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho da estrutura da organização.

A estruturação dos processos de um SGSI deve seguir o modelo Plan-Do-Check-Act (PDCA), de acordo com a norma ISO/IEC 27001. O Quadro 3 especifica com detalhes cada etapa desse processo.

Quadro 3. Modelo PDCA aplicado aos processos do SGSI

ETAPAS DO CICLO PDCA	ATIVIDADES
***Plan* (planejar) (estabelecer o SGSI)**	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
***Do* (fazer) (implementar e operar o SGSI)**	Implementar e operar a política, controles, processos e procedimentos do SGSI.
***Check* (checar) (monitorar e analisar criticamente o SGSI)**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* (agir) (manter e melhorar o SGSI)**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Fonte: ABNT (2013)

De acordo com Silva (2009), o SGSI pode e deve ser um processo sustentável, onde pode-se ter um processo de proteção da informação que ele próprio gere mais condições para a continuidade de vida do próprio processo.

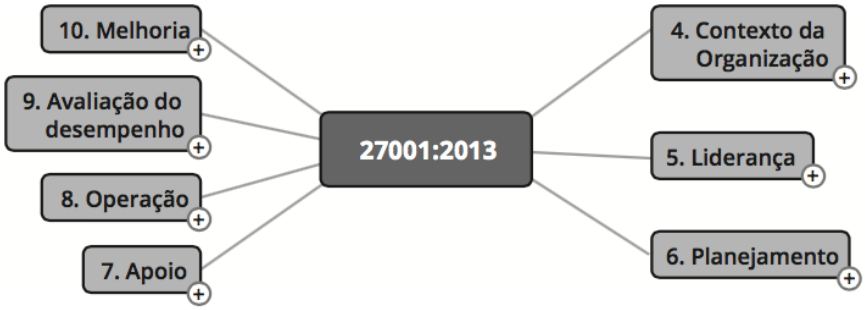
2.1.2.1 ABNT NBR ISO/IEC 27001

Antes conhecida como BS7799, a primeira versão da norma 27001 foi publicada pela ISO e pela IEC em outubro de 2005. A segunda versão da norma foi publicada em 2013. Esta norma faz parte do conjunto de normas da família 27000, criadas pela ISO para o tratamento da gestão da segurança da informação, com foco específico na gestão de um SGSI (SANTOS, 2014).

A norma complementar 02/IN01/DSIC/GSIPR que define a metodologia de gestão de segurança da informação e comunicaçòes utilizada pelos orgãos e entidades da Administração Pública Federal, direta e indireta, utiliza como referencia a norma ISO/IEC 27001 de 2006. Essa norma complementar baseia-se no processo de melhoria contínua, o ciclo PDCA (Plan-Do_check-Act), utilizado pela norma ISO/IEC 27001 (BRASIL, 2008).

A norma ISO/IEC 27001 de 2013 foi desenvolvida para estabelecer implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI. Ela está estruturada em dez sessões e um anexo. As sessões de 1 a 3 tratam do escopo. As demais a partir da 4 buscam de forma objetiva e genérica apresentar os requisitos aplicáveis a todas as organizações, independente do tipo, tamanho ou natureza. As fazes da gestão de um SGSI são demonstradas na Figura 5 (ABNT, 2013).

Figura 5. Sessões da Norma ABNT ISO/IEC 27001:2013



Fonte: Coelho et al. (2014a)

Contexto da Organização

Para iniciar o projeto de um SGSI, é preciso antes de tudo a aprovação e apoio da direção da organização. Para que isso aconteça, é importante que a primeira atividade a ser realizada seja de reunir as informações relevantes que demonstrem os benefícios de um SGSI para a

organização, deixando claro a real necessidade de implantação de um SGSI (COELHO et al., 2014a).

Os mesmos autores afirmam que a organização deve definir todas as partes interessadas importantes para o SGSI e os requisitos que essas partes demandam de segurança da informação. Deve também, considerar as questões internas e externas, os requisitos e as interfaces, e dependências entre as atividades desempenhadas pela organização.

Para contextualização da organização as seguintes atividades são necessárias:

- Definição do escopo e limites organizacionais;
- Escopo e limites de tecnologia da informação e comunicação (TIC);
- Escopo e limites físicos;
- O negócio, a organização, sua localização, ativos e aspectos tecnológicos do escopo e políticas.

Liderança

Coelho et al. (2014a), afirma que a liderança é um importante requisito para o sucesso do SGSI, através do envolvimento da Alta direção, sua liderança e comprometimento durante todo o processo do SGSI. Esta liderança se inicia através do estabelecimento da politica de segurança e os objetivos de segurança da informação compatíveis com a direção estratégica da organização.

Planejamento

As etapas de planejamento de um SGSI incluem definir e aplicar um processo de avaliação de riscos de segurança da informação, documentado e retido. Esse processo de avaliação e tratamento dos riscos precisa estar alinhado com os princípios e diretrizes das normas ABNT NBR ISO 31000 e ABNT NBR ISO 27005 (COELHO et al., 2014a). Os mesmos autores afirmam que esse processo é essencial para a conformidade e a implementação bem-sucedida de um SGSI.

Apoio

Atividades de comunicação e conscientização são etapas de destaque para o sucesso de um SGSI. A instituição deve implementar um projeto de conscientização, treinamento e educação

em segurança da informação para que todos os funcionários entendam seus papéis e suas responsabilidades na execução das atividades que compreendem o SGSI.

Operação

A instituição deve planejar e implementar todas as ações necessárias para o perfeito atendimento dos requisitos de segurança da informação, documentando todos os processos e alterações que vierem a surgir, para que aja a garantia de que tudo está saindo como planejado.

Através da norma ABNT NBR ISO/IEC 27005 a instituição precisa implementar uma metodologia para realização das avaliações de risco e, a partir da sua aplicação, implementar um plano de tratamento dos riscos identificados.

Avaliação do Desempenho

O monitoramento é fator de grande importância para verificação da eficácia do SGSI implementado. Este deve ser avaliado em períodos pré-definidos de tempo através de auditorias internas e independentes. Essa auditoria precisa ser planejada levando em consideração o status e a importância dos processos e áreas a serem auditadas, bem como o resultado das auditorias anteriores.

As atividades de avaliação de desempenho são fundamentais para o sucesso de um SGSI, pois permitem o acompanhamento, por meio de evidências, e também o processo de melhoria contínua.

Melhoria

De acordo com Coelho et al. (2014), um processo bem definido e implantado na instituição deve ser o de melhoria contínua, buscando sempre o aperfeiçoamento e melhoria do SGSI. Ações corretivas devem ser tomadas para eliminar as causas das não conformidades com os requisitos estipulados pelo SGSI.

Ainda segundo os mesmos autores, ações preventivas também devem ser criadas para eliminar as causas de não conformidades potenciais com os requisitos do SGSI, evitando a sua ocorrência.

2.2 Publicações Oficiais de GSI no Âmbito da APF

De acordo com Vieira (2008), o Brasil não possui uma lei única para tratar da segurança da informação, porém várias instruções normativas, normas e decretos podem ser aplicadas ao tema. A Instrução Normativa 01 do Gabinete de Segurança Institucional da Presidência da República de 2008 (IN01/GSI/PR/2008), estabelece os critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão da Segurança da Informação e Comunicações, no âmbito da APF (Brasil, 2008).

A IN01/GSI/PR/2008 possui mais 21 normas complementares, conforme Quadro 4.

Quadro 4. Normas Complementares a IN01/GSI/PR/2008

NORMAS COMPLEMENTARES	DESCRIÇÃO
Norma Complementar nº 01/IN01/DSIC/GSIPR	Atividade de Normatização (DOU Nº 200, de 15 Out 2008 - Seção 1)
Norma Complementar nº 02/IN01/DSIC/GSIPR	Metodologia de Gestão de Segurança da Informação e Comunicações (DOU Nº 199, de 14 Out 2008 - Seção 1)
Norma Complementar nº 03/IN01/DSIC/GSIPR	Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal (DOU Nº 125, de 03 Jul 2009 - Seção 1)
Norma Complementar nº 04/IN01/DSIC/GSIPR	Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal (DOU Nº 37, de 25 Fev 2013 - Seção 1)
Norma Complementar nº 05/IN01/DSIC/GSIPR	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal (DOU Nº 156, de 17 Ago 2009 - Seção 1).
Norma Complementar nº 06/IN01/DSIC/GSIPR	Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. (DOU Nº 223, de 23 Nov 2009 - Seção 1)
Norma Complementar nº 07/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. (DOU Nº 134, de 16 Jul 2014 - Seção 1)
Norma Complementar nº 08/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (DOU Nº 162, de 24 Ago 2010 - Seção 1)
Norma Complementar nº 09/IN01/DSIC/GSIPR	Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta (DOU Nº 134, de 16 Jul 2014 - Seção 1)
Norma Complementar nº	Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos

10/IN01/DSIC/GSIPR	de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF (DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 11/IN01/DSIC/GSIPR	Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF (DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 12/IN01/DSIC/GSIPR	Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta (DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 13/IN01/DSIC/GSIPR	Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF) (DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 14/IN01/DSIC/GSIPR	Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta (DOU Nº 30, de 10 Fev 2012 - Seção 1)
Norma Complementar nº 15/IN01/DSIC/GSIPR	Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta (DOU Nº 119, de 21 Jun 2012 - Seção 1)
Norma Complementar nº 16/IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta (DOU Nº 224, de 21 Nov 2012 - Seção 1)
Norma Complementar nº 17/IN01/DSIC/GSIPR	Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF) (DOU Nº 68, de 10 Abr 2013 - Seção 1)
Norma Complementar nº 18/IN01/DSIC/GSIPR	Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da APF (DOU Nº 68, de 10 Abril 2013 - Seção 1)
Norma Complementar nº 19/IN01/DSIC/GSIPR	Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da APF, direta e indireta. (DOU Nº 134, de 16 Jul 2014 - Seção 1)
Norma Complementar nº 20/IN01/DSIC/GSIPR	Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da APF, direta e indireta. (DOU Nº 242, de 15 Dez 2014 - Seção 1)
Norma Complementar nº 21/IN01/DSIC/GSIPR	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta (DOU Nº 196, de 10 Out 2014 - Seção 1)

Fonte: BRASIL (2015)

As normas listadas no Quadro 4 devem ser seguidas por todos os órgãos da Administração Pública Federal, dentre estes estão as Instituições Federais de Ensino Superior, estudadas neste trabalho.

Segundo Araujo (2012), existem ainda todo um conjunto de normas e instruções normativas, não listadas na tabela 2, por outros órgãos reguladores, e com foco em Segurança da Informação. A Saber:

- Banco do Central: normas específicas de segurança da informação que devem ser seguidas por instituições financeiras atuantes no Brasil;
- Conselho Nacional de Justiça: estabelece normas de segurança da informação para o judiciário;
- Estados da Federação: legislação específica de cada estado brasileiro;
- Ministério do Planejamento, Orçamento e Gestão: elaborou o documento e-Ping, que trata sobre os padrões de interoperabilidade de Governo Eletrônico;
- Comitê Gestor da Internet no Brasil: elaboração e disponibilização de documentos e serviços sobre segurança da informação para a comunidade em geral.

2.3 Modelos de Maturidade

Os modelos de maturidade são ferramentas que possibilitam a uma organização medir em que nível de maturidade está posicionada, de acordo com as métricas do modelo utilizado, identificando quais processos precisam ser restruturados para que se possa alcançar os níveis desejados.

Segundo o *Information Technology Governance Institute* - ITGI (2007), modelos de maturidade têm sido cada vez mais utilizados por gestores de TI para auto avaliação e podem prover uma abordagem comum para que profissionais de TI entendam e se atentem para as prioridades e áreas que exijam maior atenção.

De acordo com Chapin e Akridge (2005), modelos de maturidade são baseados na melhoria de processos e em fundamentos que servem para guiar e mensurar a implementação e a melhoria destes processos.

Diversas pesquisas relacionadas ao uso de modelos com a finalidade de medir a maturidade de Sistemas de Gestão de Segurança da Informação foram realizadas ao longo dos anos por autores como: Woodhouse (2008), Park et al. (2008), Rigon e Westpahll (2013), Matrane et al. (2014).

Segundo ITGI (2007, apud Teixeira Filho, 2010), os modelos de maturidade procuram as seguintes informações:

- O desempenho atual da empresa: onde a empresa está atualmente?
- O estado atual do setor ou da indústria: *benchmarking* (comparação com o mercado).
- As metas da empresa para melhoria da maturidade: aonde a organização quer chegar?
- O caminho necessário a percorrer: “como está agora” e “como quer ser no futuro”.

Nos próximos tópicos serão apresentados os principais modelos de maturidade que possuem relação com aspectos da gestão da segurança da informação, citados durante a análise dos estudos do Referencial Teórico e da Revisão Sistemática.

2.3.1 MMPE-SI/TI (Gov)

O Modelo de Maturidade para Planejamento Estratégico de SI/TI (Sistemas de Informação/Tecnologia da Informação) direcionado às Organizações Governamentais Brasileiras – MMPE-SI/TI (Gov), foi um modelo criado por Teixeira Filho (2010) para avaliar o nível de maturidade do planejamento estratégico de SI/TI de organizações governamentais brasileiras. Este mesmo autor, informa que para possibilitar um fácil acesso às melhores práticas mundiais, levou os seguintes aspectos em consideração na definição do modelo:

- Flexibilidade: para proporcionar as organizações de diferentes esferas do governo (federal estadual e municipal) o uso de todas as características do modelo;

- Idioma em português: para facilitar a compreensão das organizações governamentais brasileiras;
- Facilidade/Praticidade: utilizando a mesma lógica padrão para todos os processos do modelo, tornando-o mais amigável.

Teixeira Filho (2010), afirma que o modelo MMPE-SI/TI (Gov) foi criado em conformidade com os principais modelos e normas nacionais e internacionais utilizados para definição e avaliação de processos. O mesmo autor, estruturou o modelo em três componentes:

- Modelo de Referencia (MR): contem 5 níveis de maturidade e 6 de capacidade, além de 16 processos. Foi definido tendo como principais referências as normas internacionais ISO/IEC 12207 e ISO/IEC 15504-1; e modelos como: MPS.BR: Guia geral, MMGP, COBIT, CMMI, PMMM e OPM3;
- Banco de Melhores Práticas (BMP): contem 124 melhores práticas para planejamento estratégico de SI/TI, voltado às organizações brasileiras;
- Método de Avaliação (MA): combina 3 fases distintas, que juntas permitem proceder uma avaliação completa da organização.

Os níveis de maturidade estabelecidos pelo modelo MMPE-SI/TI (Gov) está organizado em 5 níveis de maturidade, dos quais a organização pode evoluir gradativamente do nível 1 (inicial) até o nível 5 (otimizado), conforme Quadro 5 (TEIXEIRA FILHO, 2010).

Quadro 5. Níveis de Maturidade MMPE-SI/TI (Gov)

Nível de Maturidade	DESCRIÇÃO
Nível 1 – Inicial / ad hoc	Existem evidências que a organização reconheceu a existência de questões que precisam ser trabalhadas. No entanto, não existe processo padronizado, ao contrário, existem enfoques ad hoc que tendem a ser aplicados individualmente ou caso a caso. O enfoque geral de gerenciamento é desorganizado.
Nível 2 - Gerenciado	Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas que fazem a mesma tarefa. A padronização para os treinamentos e para a comunicação dos procedimentos entre os interessados ainda é insuficiente. A responsabilidade é deixada com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e consequentemente erros podem ocorrer.
Nível 3 - Definido	Processos foram padronizados, documentados e comunicados através de treinamento. É mandatório que esses processos sejam seguidos, no entanto, é improvável que os desvios sejam detectados. Os processos são sofisticados, mas ainda existe uma formalização e uso restritos.
Nível 4 - Medido	A alta administração monitora e mede a aderência aos processos e adota ações corretivas para aqueles que não estão funcionando muito bem. Os processos estão em constante aprimoramento e avaliação. Ferramentas ainda estão sendo utilizadas de maneira limitada ou fragmentada.
Nível 5 - Otimizado	Os processos e as melhores práticas foram refinados com base nos resultados de melhoria

	contínua e de modelagem da maturidade percebidos em outras organizações. SI/TI é utilizado como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade, a eficiência e a eficácia, tornando a organização cada vez mais rápida, principalmente para se adaptar às mudanças.

Fonte: adaptado de Teixeira Filho (2010)

Os níveis de maturidade são fornecidos a partir dos níveis de capacidade alcançados pela organização durante a execução dos processos. Teixeira Filho (2010) definiu os seguintes níveis de capacidade: Nível 0 - Processo Incompleto; Nível 1 - Processo Executado; Nível 2 – Processo Gerenciado; Nível 3 Processo Definido; Nível 4 – Processo Medido e; Nível 5 – Processo Otimizado.

Os 16 processos definidos no MMPE-SI/TI (Gov) são atribuidos aos níveis de maturidade já apresentados no Quadro 5. A cada um dos processos há um conjunto de melhores práticas a serem seguidas. Dentre esses processos dois se destacam com relação a Gestão da Segurança da Informação. São eles (TEIXEIRA FILHO, 2010):

- Nível 3 – Gerenciar Infraestrutura de SI/TI: cuja melhor prática, denominada Definir os Requisitos da Infraestrutura de SI/TI, estabelece que a organização deve definir os requisitos de infraestrutura de SI/TI para apoiar o desempenho dos processos. Requisitos de infraestrutura podem incluir: segurança; acesso aos dados e requisitos de compartilhamento; backup e recuperação; facilidade de acesso remoto; espaço físico e equipamentos; requisitos de suporte ao usuário e requisitos de manutenção;
- Nível 4 – Gerenciar Riscos: cuja melhor prática, denominada Identificar os Riscos, estabelece que a organização deve definir as estratégias adequadas para identificar, analisar, tratar e monitorar cada risco ou conjunto de riscos no nível de planejamento estratégico de SI/TI e organizacional.

2.3.2 Modelo de Maturidade do COBIT

Um dos modelos de avaliação de maturidade mais citados na Revisão Sistemática da Literatura (RSL) foi o do *Control Objectives for Information and Related Technology* (COBIT) da *Information System Audit Control Association* (ISACA). O COBIT possui um modelo de maturidade derivado do *System Engineering Capability Maturity Model* (SE-CMM). Os

processos de TI do COBIT assumem os controles das aplicações que são regidos pelos proprietários dos processos de negócio, logo eles são integrados com os processos de negócio.

Os níveis de maturidade do COBIT são destinados a descrever os estados possíveis desses processos de TI. Eles não são destinados para uso como um modelo de execução, onde o cumprimento dos requisitos de nível mais baixo é a chave da elegibilidade para a promoção de níveis mais elevados (STAMBUL e RAZALI, 2011). O modelo de maturidade do COBIT estabelece seis níveis de maturidade da segurança da informação, conforme Quadro 6.

Quadro 6. Níveis de Maturidade do COBIT

Nível de Maturidade	DESCRIÇÃO
Nível 0 – Inexistente	A organização não reconhece a necessidade de segurança de TI. Há uma completa falta de um processo de administração de segurança do sistema reconhecível.
Nível 1 – Inicial / Ad hoc	A organização reconhece a necessidade de segurança de TI. Mas, a organização considera os riscos de TI de uma forma ad hoc, sem seguir processos ou políticas definidas.
Nível 2 – Repetitivo, mas intuitivo	Responsabilidades e obrigações para a segurança de TI são atribuídos a um coordenador de segurança de TI. Há um entendimento emergente que riscos de TI são importantes e precisam ser considerados. Alguma abordagem para avaliação de risco existe, mas o processo ainda é imaturo e em desenvolvimento.
Nível 3 – Processo Definido	Sensibilização para a segurança existe e é promovido pela administração. Uma política de gestão de risco em toda a organização define quando e como conduzir avaliações de risco. A avaliação de risco segue um processo definido que é documentada e disponível para todos os funcionários através de treinamento.
Nível 4 – Gerenciado e Mensurável	Responsabilidades para a segurança de TI são claramente atribuídos, geridos e aplicados. A avaliação do risco é um procedimento padrão e exceções a seguir o procedimento seria notado pela administração de TI.
Nível 5 - Otimizado	Segurança de TI é uma responsabilidade conjunta de negócios e gestão de TI e é integrado com os objetivos de negócios de segurança corporativa. A avaliação de risco tem desenvolvido para a fase em que um processo estruturado, em toda a organização é aplicada, seguido regularmente e bem gerido.

Fonte: Stambul e Razali (2011)

De acordo com Rigon et al. (2013), o modelo de maturidade do COBIT apresenta um conjunto de indicadores obtidos pelo consenso de especialistas, que são mais focados nos controles de atividades do que em sua execução. Esses controles ajudam a otimizar o investimento em TI, garantindo a prestação de serviços e fornecendo uma medida para julgar e permitir a comparação.

2.3.3 Open Information Security Management Maturity Model (O-ISM3)

Um segundo modelo de avaliação de maturidade, também muito citado na revisão sistemática da literatura, foi o *Open Information Security Management Maturity Model* (O-ISM3). Este é o modelo de maturidade da *The Open Group* para a gestão da segurança da informação. O modelo busca garantir que os processos de segurança da informação sejam implementados em total compatibilidade com os requisitos de negócio da organização. Ele define um número abrangente, porém controlável, de processos de segurança da informação suficientes para as necessidades da maioria das organizações. Para cada processo relevante, alguns controles de segurança são identificados e atuam como partes essenciais do processo. Nesse sentido, o modelo é compatível com os frameworks já estabelecidos internacionalmente como a ISO / IEC 27000:2009, COBIT e ITIL, no domínio da GSI (The Open Group, 2011).

O O-ISM3 auxilia os gerentes de segurança na avaliação do seu próprio ambiente operacional, planejando os processos de gestão de segurança para que eles sejam coerentes e de custos adequados para atendimento dos objetivos de negócio da organização (The Open Group, 2011). Esse modelo define cinco níveis de maturidade para os processos de gestão da segurança da informação, conforme Quadro 7.

Quadro 7. Níveis de Maturidade O-ISM3

Nível de Maturidade	DESCRIÇÃO
Nível 1 – Inicial	Práticas base da área de controle são geralmente realizadas numa base ad hoc. Há um consenso geral dentro da organização que identificou que ações devem ser executadas, e elas são executados quando necessário. As práticas não são formalmente aprovadas, acompanhadas e documentadas.
Nível 2 – Definido	Os requisitos básicos para a área de controle são planejadas, implementadas e repetíveis.
Nível 3 – Gerenciado	A principal distinção do Nível 2, Definido, é que além de ser repetitivo os processos utilizados são mais maduros: documentado, aprovado e implementado em toda a organização.
Nível 4 – Controlado	A distinção principal do Nível 3, Gerenciado, é que o processo é medido e confirmado (por exemplo, através de auditoria).
Nível 5 - Otimizado	A principal distinção do Nível 4, Controlado, é que os processos padrões definidos são regularmente revisados e atualizados. Melhorias refletem uma compreensão e resposta ao impacto de uma vulnerabilidade.

Fonte: The Open Group (2011)

Os modelos de maturidade citados neste trabalho são ferramentas de avaliação baseadas em padrões já conceituados e utilizados no mercado, projetados para garantir boas práticas de gestão de segurança da informação nas organizações e estão entre os métodos mais utilizados. O próximo modelo de maturidade, detalhado na seção seguinte, foi aquele definido na ferramenta de avaliação de maturidade utilizado nesta pesquisa.

2.3.4 ISO/IEC 21827 (SSE-CMM)

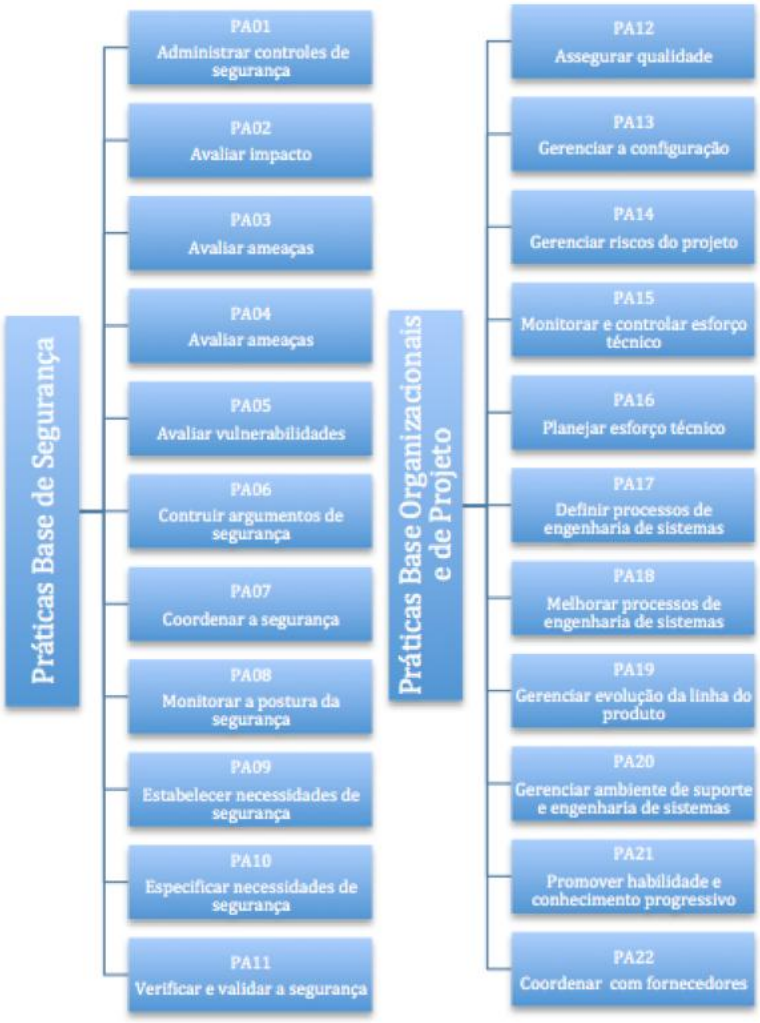
A norma 21827 desenvolvida pela ISO e pela IEC foi criada em alinhamento com o "*Systems Security Engineering - Capability Maturity Model"* (SSE-CMM), desenvolvido pela "*International Systems Security Engineering Association"* (ISSEA). A SSE-CMM está atualmente na versão 3 e é disponível publicamente (SSE-CMM, 2003).

De acordo com a norma 21827:2008, o SSE-CMM é um método para avaliação da gestão da segurança da informação e pode ser usado para avaliação das práticas de engenharia de segurança da informação e definição de melhorias nas organizações.

A norma ISO/IEC 21827:2008 não prescreve uma sequência ou um processo particular, mas captura as práticas que são geralmente observadas na indústria. Esta norma é designada para todos os tipos de organizações, sendo usada para a melhoria e avaliação da capacidade de maturidade dos processos de segurança (SG-SBP 2008, apud Kroll 2010).

A estrutura de desenvolvimento da gestão da segurança da informação proposta pela norma está estruturada em 22 Áreas de Processos (PA – Process Area), subdivididas em Práticas Base de Segurança e Práticas Base Organizacionais e de Projeto, conforme Figura 6 (KROLL, 2010).

Figura 6. Estrutura das Áreas de Processos da 21827



Fonte: adaptado de KROLL (2010)

A ISO/IEC 21827:2008 define seis níveis de maturidade para os processos de segurança da organização que são ampliados após o estabelecimento e cumprimento das práticas de segurança (Batista 2007, apud Kroll 2010). O processo mais "maduro" define uma organização cujos processos são melhores definidos e conduzidos. Cada um dos níveis consiste de um número de Práticas Genéricas - GP (Generic Practices) que suportam o desempenho das PAs (SSE-CMM, 2003). Uma descrição mais detalhada de cada nível de maturidade pode ser observada no Quadro 8.

Quadro 8. Níveis de Maturidade do SSE-CMM

Nível de Maturidade	DESCRIÇÃO
Nível 0 – Não Realiza	Não há nada implementado ou planejado, controles de segurança inexistentes.
Nível 1 – Realiza Informalmente	Práticas básicas de controle de segurança são geralmente realizadas. O desempenho dessas práticas não é rigorosamente planejado e monitorado. A execução depende do conhecimento e do esforço individual. Indivíduos dentro da instituição reconhecem que uma ação deve ser realizada, e há um consenso geral de que esta ação é realizada como e quando necessário. As práticas não são formalmente aprovadas, acompanhadas e documentadas.
Nível 2 – Planejado	O desempenho das práticas base dos processos são planejados e controlados. Os produtos de trabalho estão em conformidade com as normas e requisitos especificados. A medição é usada para rastrear o desempenho da área de processamento, permitindo que a organização gerencie suas atividades com base no desempenho real. A principal diferença do Nível 1, Realizado Informalmente, é que o desempenho do processo é planejado e gerenciado.
Nível 3 – Bem Definido	As práticas base são executadas de acordo com um processo bem definido usando versões aprovadas e adaptadas de processos padronizados e documentados. A principal distinção entre o Nível 2, Planejada, é que o processo é planejado e gerenciado usando um processo padronizado e aprovado pela organização.
Nível 4 – Controlado Quantitativamente	Medidas detalhadas de desempenho são coletadas e analisadas. Isto leva a uma compreensão quantitativa da capacidade do processo e uma capacidade melhorada para prever o desempenho. O desempenho é objetivamente gerenciado e a qualidade dos produtos de trabalho é quantitativamente conhecida. A distinção principal entre o nível 3, Bem Definido, é que os processos são quantitativamente compreendidos e controlados.
Nível 5 – Melhoria Contínua	Os objetivos de desempenho quantitativo (metas) para a eficácia dos processos e eficiência são estabelecidos, com base nas metas de negócios da organização. A melhoria contínua dos processos em relação a esses objetivos é possibilitada através de um feedback da execução dos processos definidos e do uso de ideias e tecnologias inovadoras. A principal diferença entre o nível 4, Controlado Quantitativamente, é que o processo definido e o processo padrão sofrem aperfeiçoamento e melhoria contínua, com base em uma compreensão quantitativa do impacto das mudanças nesses processos.

Fonte: SSE-CMM (2003)

Este modelo é utilizado no instrumento de avaliação de maturidade empregado nesta pesquisa. O resultado de sua aplicação nas Instituições Federais de Ensino Superior pode ser observado no Capítulo 5 deste trabalho.

2.4 Fatores Críticos de Sucesso (FCS)

As instituições precisam adequar a gestão da segurança das informações (GSI) para proteger seus ativos de informações e garantir a confidencialidade, integridade e disponibilidades de suas informações. Entretanto, os custos elevados de planejamento, implementação e manutenção dos controles de segurança da informação tem dificultado a distinção entre os controles que as organizações de fato precisam e aqueles que são menos críticos (TU, 2015). O mesmo autor afirma que as organizações mais maduras concentram seus recursos limitados naquilo que realmente faz a diferença para o seu negócio.

As melhores práticas de segurança da informação encontram-se definidas através da família de normas ISO/IEC 27000. Entretanto os Fatores Críticos de Sucesso (FCS) variam de uma instituição para outra (QUINTELLA e BRANCO, 2013). Seguindo esse conceito, este trabalho de pesquisa buscou identificar os fatores críticos de sucesso para o aprimoramento de maturidade de GSI das instituições federais de ensino superior (IFES), visto que estas instituições possuem os mesmos objetivos, diretrizes e estrutura organizacional básica.

De acordo com Rockart (1982, apud Tu, 2015), a utilização de FCS já é um conceito definido e amplamente entendido para identificar os requisitos de desempenho considerados mais importantes para o sucesso da organização.

Rockart (1979), afirma que os FCS podem ser estudados de acordo com o seu relacionamento com as áreas ou processos da organização, eles foram criados originalmente para desenvolver o alinhamento de TI com o planejamento estratégico da organização. Ainda segundo o mesmo autor, os FCS são definidos como áreas de atividade chave, cujos resultados favoráveis são absolutamente necessários para os gerentes atingirem seus objetivos.

Nesse sentido, o conceito de FCS foi utilizado como base para elaboração de um método de definição de informações gerencias, envolvendo três aspectos (ROCKART, 1979):

- Um fator considerado como crítico deve receber atenção e investimentos, desde financeiros até tempo e esforço, assegurando o seu bom desempenho e garantindo assim o sucesso da organização.

- Um fator considerado crítico que recebe atenção e investimento citados acima, deve ser acompanhado de informações que permitam o seu devido controle e consequentes ações corretivas e de melhoria.
- O fator crítico estando intimamente ligado ao negócio da organização, os próprios executivos responsáveis por ele devem definir os fatores, suas formas de medição, seu padrão de desempenho e as informações necessárias.

Costa (2009, p.27), afirma que:

> FCS são pressupostos essenciais e devem ser indicados de acordo com o atendimento dos objetivos que se deseja alcançar. Teoricamente, sabe-se que o mau desempenho de competências organizacionais, recurso e processos levam a comprometer os resultados almejados. Alcançar o desempenho desejado em um ambiente de constante incerteza e mudanças é definido a partir de uma análise estratégica da organização, ou seja, da sua realidade em relação ao capital humano, sua missão, seus processos, sua tecnologia, seu mercado e sua visão do futuro (COSTA, 2009, p.27).

Considerando a importância na definição dos fatores críticos de sucesso para o correto funcionamento e andamento das organizações, considerando a definição de maturidade dos processos de segurança da informação já citados nos tópicos anteriores e considerando as boas práticas de segurança da informação propostas na família de normas ISO/IEC 27000. Torna-se visível a importância em definir os fatores críticos de sucesso para o aprimoramento do nível de maturidade da gestão da segurança da informação das IFES, proposto nessa pesquisa. Com isso será possível alocar recursos e esforços àqueles fatores específicos para a garantia de uma GSI eficaz, garantindo assim a continuidade do negócio.

2.5 Revisão Sistemática da Literatura

A revisão sistemática da literatura (RSL) foi uma etapa de extrema importância no desenvolvimento deste trabalho, pois foi um meio de identificar, avaliar e interpretar todas as pesquisas disponíveis e relevantes para a questão da pesquisa. Este tipo de pesquisa foi utilizado para identificar os trabalhos já desenvolvidos na área de Gestão de Segurança da Informação, a fim de buscar a fundamentação teórica e justificar o desenvolvimento do presente trabalho.

A RSL é baseada na aplicação de métodos com maior rigor científico, podendo alcançar melhores resultados e reduzir erros e o viés do pesquisador responsável pela pesquisa (COOK et al., 1997).

Foram estabelecidas três etapas para a realização do processo de revisão sistemática (TEIXEIRA FILHO, 2010), conforme detalhamento a seguir:

1. **Planejamento**: elaboração do protocolo para condução e validação dos estudos pesquisados contendo a questão de pesquisa, objetivos, fontes de busca, *strings* de busca, critérios de inclusão e exclusão e etapas de execução.
2. **Execução:** Utilização de formulários específicos que ajudaram a catalogar e conduzir nas avaliações futuras dos estudos. Esses formulários ajudaram a manter um histórico dos estudos escolhidos para revisão e validação.
3. **Análise/divulgação dos resultados:** dados são analisados de forma descritiva, levando-se em conta a qualidade dos estudos e relevância nas questões de pesquisa.

Todo o processo de pesquisa e seleção dos trabalhos foi realizado de forma eletrônica, utilizando-se a ferramenta Start para operacionalização do processo de revisão sistemática e das bases de pesquisas cientificas mais conhecidas como ACM, IEEE Xplore, Science Direct, Scopus e Google Scholar.

O desenvolvimento da RSL ocorreu em cinco etapas a seguir (TEIXEIRA FILHO, 2010):

ETAPA I – Realizar pesquisas de acordo com as strings de busca definidas para a pesquisa.

ETAPA II – Os trabalhos retornados serão inicialmente avaliados segundo o título, sem a necessidade de fichar no formulário de condução da revisão. Caso o título seja relevante ao contexto da pesquisa, o trabalho será potencialmente selecionado para a próxima etapa, caso contrário ele será excluído.

ETAPA III – Dos estudos pré-selecionados na primeira etapa, uma nova pesquisa (busca) será realizada, aplicando-se strings de busca de forma mais refinada. Os trabalhos que retornarem resultados com esse refinamento vão ter seus resumos (*abstract*) lidos, depois serão selecionados

para a próxima etapa e fichados no formulário de condução da revisão. Caso contrário eles serão excluídos.

ETAPA IV – Na próxima etapa será realizada uma leitura da introdução e conclusão de cada trabalho pré-selecionado. Se houver relevância com o contexto da pesquisa, o trabalho será selecionado para a próxima etapa e fichado no formulário de condução da revisão. Caso contrário ele será excluído.

ETAPA V – A última etapa aprimora a seleção principalmente, porque o trabalho será completamente lido, analisado e criticado haja vista a relevância contextual e filtro proporcionado pelas etapas anteriores. Nesta última etapa o trabalho será considerado apto e será fichado no formulário de aprovação dos estudos.

A quantidade de trabalhos selecionados em cada etapa pode ser melhor observada através da Tabela 1.

Tabela 1. Resultado da Revisão Sistemática da Literatura

Base	Etapa I	Etapa II	Etapa III	Etapa IV	Etapa V
ACM	368	11	3	1	1
IEEE Xplore	327	35	19	6	4
Science Direct	509	30	11	6	1
Google Scholar	114	44	25	19	15
Scopus	94	0	0	0	0
Outros	8	0	0	0	0
Total	**1420**	**120**	**58**	**32**	**21**

Ao final das etapas da RSL, somente 21 trabalhos mostraram-se com relevância quanto ao tema da pesquisa atual e serviram como fundamentação teórica para realização do diagnóstico de maturidade, identificação dos fatores críticos de sucesso e seu grau de importância para aprimorar o nível de maturidade de GSI nas IFES.

Os trabalhos selecionados na RSL foram lidos e utilizados como arcabouço teórico para essa pesquisa. Dessa forma, foi possível justificar a sua importância e relevância para os

objetivos propostos. No APÊNDICE A. é apresentado uma descrição completa de todas as etapas da revisão sistemática, bem como a análise e o protocolo utilizado.

2.5.1 Trabalhos Relacionados

Um tema muito discutido em trabalhos e revistas cientificas nos últimos anos é a Gestão da Segurança da Informação. Este assunto está presente em muitos trabalhos científicos voltados a segurança da informação, pois é através de uma gestão e procedimentos apropriados que a segurança da informação será o mínimo eficaz para as organizações.

Durante o processo da pesquisa, não foram encontrados trabalhos acadêmicos que buscaram identificar os fatores críticos de sucesso para o aprimoramento de maturidade da gestão da segurança da informação. Contudo, os trabalhos selecionados na revisão sistemática adotaram em suas pesquisas temas relacionados, como: Gestão da Segurança da Informação, Modelos de Avaliação de Maturidade de Segurança da Informação, Fatores Críticos de Segurança da Informação, entre outros.

O presente trabalho utilizou como um dos critérios de busca o intervalo dos anos de 2010 a 2016, onde foram selecionados vários estudos de relevância para a sua elaboração. Estes estudos foram lidos e estão resumidos nos próximos tópicos.

2.5.1.1 A Gestão da Segurança da Informação e seu Alinhamento Estratégico na Organização

Artigo publicado em 2010 pela revista Interface Tecnológica da Fatec de Taquaritinga. O trabalho apresenta os pontos críticos da Gestão da Segurança da Informação e propõe a aplicação de um código de boas práticas para conscientizar as empresas no tocante a adoção de um Sistema de Gestão de Segurança da Informação. A metodologia utilizada é baseada num levantamento histórico da Segurança da Informação em seu contexto empresarial, com enfoque nos impactos que podem causar uma falha de segurança. O artigo discute ainda aspectos voltados a gestão de riscos de segurança da informação e aspectos voltados aos controles das normas ABNT NBR ISO/IEC 27002:2005, 27001:2006, 27005:2008 e 27004:2010. Os autores descrevem as etapas

para a adoção de um Sistema de Gestão de Segurança da Informação (SGSI) referenciando os controles da Norma ABNT NBR ISO/IEC 27002 de 2005. O estudo é finalizado deixando como proposta que as empresas e organizações utilizem as boas práticas para gestão de segurança da informação na proteção de seus ativos (TORRES et al., 2010).

2.5.1.2 A cyclical evaluation model of information security maturity

Trabalho publicado pela revista *Information Management & Computer Security* em 2014. O artigo apresenta um modelo de avaliação cíclica da maturidade da segurança da informação baseado nos controles da norma ISO/IEC 27002.

A abordagem utilizada pelos autores para o desenvolvimento do modelo foi através de um conjunto de passos a serem seguidos para obter a avaliação periódica da maturidade e melhoria contínua dos controles de segurança. Os autores discorrem sobre as principais normas de gestão de segurança da informação como a ISO/IEC 27001 e 27002 de 2005 e a norma ISO/IEC 27005 de 2008. Após, apresentam os modelos de maturidade do COBIT e o O-ISM3.

Como resultado da pesquisa, é apresentado o modelo de avaliação cíclica de maturidade da segurança da informação proposto que oferece um método de avaliação periódica da maturidade e melhoria contínua dos controles da segurança da informação com base no levantamento dos riscos. O modelo proposto é baseado em 8 fases ou estágios cíclicos: 01 – Definição do escopo de avaliação; 02 – análise global dos riscos de SI; 03 – Seleção dos controles de SI; 04 – Planejamento da análise dos controles de SI; 05 – Análise e avaliação da maturidade dos controles de SI; 06 Consolidação dos planos de ação de SI; 07 – Acompanhamento dos planos de ação de SI; 08 – Fechamento, documentação e emissão de relatórios. Ao final do trabalho, foi realizado um estudo de caso, onde o modelo proposto foi aplicado. No estudo de caso foi possível constatar a aplicabilidade do modelo (RIGON et al., 2014).

2.5.1.3 An Assesment Model of Information Security Implementation Levels

Artigo publicado em 2011 na *International Conference on Electrical Engineering an Informatics* em Bandun, Indonesia. O trabalho apresenta um modelo para avaliação dos níveis de implementação da segurança da informação nas organizações. O modelo criado é composto de três níveis de maturidade que vão determinar os graus em que a segurança da informação está sendo gerida em uma organização.

A pesquisa utilizou-se da Revisão Sistemática da Literatura como instrumento para determinar os parametros de medição adequados. Os autores iniciam o trabalho discorrendo sobre a importancia da segurança da informação para as organizações, apontam também estudos anteriores dos principais fatores críticos que influenciam no sucesso da implementação da segurança da informação. No tópico Revisão da Literatura o trabalho cita as principais normas de segurança da informação e os modelos de maturidade existentes. No tópico seguinte é apresentado o modelo proposto, com três níveis de maturidade, que vai do Básico (Nível 1), passando pelo Intermediário (Nível 2) ao Avançado (Nível 3).

Ao final os autores sugerem o uso do modelo e exclarecem que ele não é conclusivo e completo, devendo ser validado e refinado ainda mais em investigações futuras (STAMBUL e RAZALI, 2011).

2.5.1.4 Analysis of the challenges faced in establishing and maintaining an information security management system on the Brazilian scene

Artigo publicado no *XI Brazilian Symposium on Information System*, Goiânia, Goiás em maio de 2015. A pesquisa em questão identificou e analisou os desafios enfrentados para o estabelecimento e manutenção de um Sistema de Gestão de Segurança da Informação (SGSI) no cenário brasileiro. O método utilizado no trabalho foi o estudo de casos múltiplos.

Os autores iniciam o trabalho citando a importância do uso de padrões e normas de segurança internacionalmente reconhecidas para a segurança de empresas e organizações voltadas principalmente para a norma ISO/IEC 27001, discorrem também sobre a falta de material cientifico sobre o tema da pesquisa. Nos tópicos seguintes são apresentadas a fundamentação teórica, justificativa para a pesquisa e os trabalhos relacionados.

Seis empresas de diferentes ramos de atividades foram estudadas no estudo de casos múltiplos. A coleta dos dados foi realizada através de um roteiro estruturado com entrevistas e perguntas abrangendo o ciclo PDCA aplicado a norma 27001. Por meio da entrevista e análise dos dados os autores alcançaram como resultados as seguintes hipóteses: falta de apoio da alta direção, falta de capacitação da equipe de segurança da informação, influência da cultura local, falhas na elaboração da análise de risco e resistência a mudança.

Ao final os autores concluem afirmando a relevância da pesquisa em questão e em como ela auxiliará os especialistas em segurança da informação com os principais desafios para estabelecer e manter um SGSI (FAZENDA e FAGUNDES, 2015).

2.5.1.5 Analytical hierarchy process approach for the metrics of information security management framework

Trabalho apresentado na *Sixth International Conference on Computational Intelligence, Communication Systems and Networks* em 2014. O estudo objetivou a identificação das métricas necessárias para o desenvolvimento de um framework de gestão de segurança da informação.

O trabalho é iniciado com uma introdução a respeito da importância da gestão da segurança da informação nas organizações e da sua busca pela excelência pelos gestores. Após, são descritos os trabalhos relacionados com a pesquisa e as métricas levantadas.

A metodologia utilizada pelos autores foi baseada na análise textual, utilizada para identificação das métricas. O processo envolveu a buscas em bases de dados, revistas, sites e motores de busca. As métricas levantadas na literatura foram agrupadas em seis categorias: Organizacional; Controle Interno; Ambiental; Políticas de Segurança; Gestão de Contingencia e; Gestão de Riscos. O método *Analytic Hierarchy Process* (AHP) foi utilizado para validação das métricas selecionadas.

Com os resultados obtidos através dos comparativos entre as métricas e suas categorias, os autores concluíram que a categoria de controles ambientais tem maior impacto na gestão da segurança do que as demais categorias, seguido pelas métricas organizacionais e de gestão de riscos.

Os autores concluem o trabalho com recomendações das práticas que devem ser seguidas

pelas organizações interessadas em segurança da informação, são elas: Buscar apoio da alta gestão; Conhecimento dos processos de negócio; Apresentação de relatórios periódicos de segurança para alta gestão; Documentação e publicação periódica de relatórios de segurança (MOETI e KELEMA, 2014).

2.5.1.6 Assesment of information security maturity: An exploration study of Malaysian public service organizations

Artigo publicado no *Journal of System and InformationTechnology* em 2012. O objetivo principal da pesquisa foi buscar e analisar os fatores básicos envolvidos com a gestão da segurança da informação nas organizações públicas da Malásia.

A metodologia utilizada baseou-se numa abordagem quantitativa, através da aplicação de um questionário realizado com 970 gestores de segurança de 722 agências governamentais. O estudo utilizou-se de uma análise empírica para identificar os antecedentes da maturidade da segurança da informação e esclarecer a relação entre a maturidade da segurança da informação e os fatores sociais e técnicos.

Os autores iniciam o trabalho abordando a importância da informação como sendo um dos principais ativos de uma organização. Na revisão da literatura são apresentados os principais modelos, de acordo com os pesquisadores, de avaliação de maturidade, sendo eles: COBIT, SSE-CMM e O-ISM3. O modelo escolhido para avaliação da maturidade foi o do COBIT, devido a sua brevidade e simplicidade na especificação das áreas de interesse. Posteriormente os autores relacionam as hipóteses criadas como fatores sociais e técnicos para a maturidade da segurança da informação, sendo eles: gerenciamento de riscos, estrutura organizacional, percepção individual, cultura de segurança da informação, barreiras sociais e barreiras técnicas. O trabalho é concluído demonstrando como os fatores sociais e técnicos combinados tem influência na maturidade da segurança da informação (DZAZALI e ZOLAIT, 2012).

2.5.1.7 Better information Security Management in Municipalities

Trabalho publicado na *IST – África Conference 2015.* O artigo utilizou-se de uma revisão

da literatura, análise de documentos, e argumentação para identificar os principais componentes de um sistema de gestão de segurança da informação nos municípios da África do Sul. Os métodos utilizados no estudo incluem uma revisão da literatura, a análise documental qualitativa e, a argumentação no sentido de uma solução inicial.

Os autores iniciam o trabalho alertando sobre a importância da tecnologia da informação e comunicação para prestação de serviços nas organizações, falam também da responsabilidade dos municípios na prestação de serviços aos cidadãos, dos quais a segurança da informação se torna um aspecto que requer muita atenção e gestão. O trabalho segue com boas referências a respeito de gestão da segurança da informação e boas práticas, focando na família das normas ISO/IEC 27000, COBIT 5 e *Corporate Governance of ICT Policy Framework* (CGICTFP).

Como resultados, são identificados oito componentes que contribuem para um Sistema de Gestão de Segurança da Informação eficaz nos municípios da África do Sul, são eles: Responsabilidade do Conselho Municipal; Leis de Tecnologia da Informação e Requisitos Regulamentados; Análise de Riscos de TI Municipal; Alinhamento Estratégico; Política de Segurança Municipal; Politicas Municipais de Apoio; Programa de Treinamento e Conscientização; Procedimentos de Segurança da Informação.

O trabalho é finalizado afirmando que os modelos de melhores práticas utilizados foram analisados para propor uma abordagem de melhoria da gestão de segurança da informação nos municípios estudados (LANGE, SOLMS e GERBER, 2015).

2.5.1.8 Framework de segurança da informação para medição do nível de maturidade das organizações

Dissertação de mestrado do Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação, defendida no ano de 2010 em Brasília, Distrito Federal.

O objetivo da pesquisa foi de propor um framework de segurança da informação para identificação do nível de maturidade atual das organizações, identificação do nível de maturidade exigido pelo negócio para cada um dos 10 domínios apresentados, e identificação dos controles necessários para atendimento destes níveis com a correta priorização. O trabalho buscou

responder a seguinte questão de pesquisa: “Como atingir os níveis de segurança da informação exigidos pelo negócio? “.

A metodologia utilizada no estudo foi o de uma pesquisa aplicada, pois envolveu uma aplicação prática dirigida à solução de um problema especifico, quantitativa, pois o *framework* possui métodos para identificar os níveis de maturidade, metodológica, devido aos procedimentos criados para identificação do nível de maturidade e de campo, devido aplicação de questionário a *checklist* para coleta de dados.

Como resultado final o framework foi desenvolvido e aplicado em uma organização para identificar as lacunas existentes entre o nível de maturidade exigido pelo negócio e o nível de maturidade atual (PARANHOS, 2010).

2.5.1.9 Factors influencing information security management in small and medium-sized enterprises: A case study from Turkey

Artigo publicado no *International Journal of Information Management* em 2010. O objetivo do trabalho foi examinar a segurança da informação em pequenas e médias empresas de Bursa, Turquia, e comparar os resultados com os dados de outras pesquisas semelhantes realizadas em diferentes países. O foco da pesquisa foi nas pequenas e médias empresas de Bursa na Turquia no ano de 2009. A coleta dos dados foi realizada através de questionários e contou com a participação de 97 empresas. A seleção das empresas foi realizada utilizando-se de um método de amostragem aleatória.

Após a coleta e análise dos dados, os autores constataram que quando a Gestão de Comunicações e Operações e a Política de Segurança melhoram, outros parâmetros de segurança, como o de Pessoal e Físico e Ambiental também melhoram.

Como resultado final, a pesquisa revelou que, no domínio segurança da informação, as empresas pesquisadas estão começando a se conscientizarem. Apesar das pressões econômicas, as organizações continuam investindo em segurança da informação. As normas internacionais de segurança estão ganhando mais aceitação. E o fator humano, continua a ser o elo mais fraco na segurança da informação (YILDIRIM et al., 2011).

2.5.1.10 Fatores Críticos de Sucesso em segurança da informação em um órgão da administração pública federal

Artigo publicado no II Simpósio Internacional de Gestão de Projetos (II Singep), em 2013. O trabalho teve como objetivo identificar os Fatores Críticos de Sucesso (FCS) para implantação de uma Política de Segurança da Informação (PSI) em um órgão da Administração Pública Federal.

A metodologia utilizada no trabalho baseou-se no método hipotético-dedutivo de Popper. A análise dos resultados obtidos com a pesquisa foi submetida ao teste Kolmogorov-Smirnov. A elaboração dos FCS foi baseada nos estudos de Rockart (1979) e nos prognósticos de Porter (1986). O universo da pesquisa foram os servidores públicos, usuários dos serviços de TI, dos níveis estratégico, tático e operacional, totalizando 265 servidores. A coleta dos dados foi através de um questionário estruturado, com objetivo de ordenar e validar os FCS.

Os autores fazem uma introdução ao tema segurança da informação, afirmando que a informação é um ativo cada vez mais importante para os negócios de uma organização. Discorrem sobre a família de normas da ISO/IEC 27000, para gestão da segurança da informação e apresentam a situação crítica da segurança da informação na administração pública federal, por meio do acordão 2.308/2010 TCU-Plenário, o qual revela baixos índices de gestão corporativa de segurança da informação.

No Referencial Teórico é conceituado Fatores Críticos de Sucesso, que segundo Rockart (1979, apud QUINTELLA e BRANCO 2013), são algumas áreas de atividade chave, cujo resultados favoráveis são absolutamente necessários para os gestores atingirem seus objetivos.

Após a coleta e interpretação dos dados da aplicação do questionário, obteve-se os seguintes FCS para elaboração da Política de Segurança da Informação no órgão estudado: Definição de papéis e responsabilidades; Motivação institucional; Qualificação prévia de um gestor de segurança da informação e; Profissionais especializados em segurança da informação (QUINTELLA E BRANCO, 2013).

2.5.1.11 GAIA-MLIS: A Maturity Model for information security

Trabalho apresentado na *SECURWARE 2014: The Eighth International Conference on*

Emerging Security Information, Systems and Technologies. O artigo teve como objetivo principal apresentar o modelo GAIA-MLIS para avaliação dos níveis de maturidade dos sistemas de gestão de segurança da informação das organizações e fornecer os dados-chave sobre como eles podem melhorar.

Para confecção do modelo foi realizado um estudo empírico com o objetivo de criar um modelo de avaliação de segurança da informação através das áreas hardware, software, equipe, instalações e informação, adaptadas das seções da norma ISO/IEC 27002.

O modelo proposto possui cinco níveis de maturidade, indo do nível 0 ao 4, avaliando 5 áreas distintas (hardware, software, instalações, pessoal e informação) e é baseado nas recomendações do COBIT 5 e das normas ISO/IEC 27001 e 27002.

Como forma de validar o modelo proposto foi aplicado um questionário com 30 perguntas, através das quais foram avaliadas três estruturas organizacionais que possibilitou a identificação dos pontos fortes e fracos nos processos ligados as cinco áreas.

Os autores concluem informando que o modelo GAIA-MLIS é capaz de indicar claramente as necessidades de cada área avaliada. Com os resultados obtidos, os gestores de segurança podem discutir as necessidades de investimento para todas as áreas avaliadas (COELHO et al., 2014).

2.5.1.12 Improving the quality of information security management system with ISO27000

Artigo publicado no *The TQM Journal* em 2011 no *Hope Street Centre*, Liverpool, Reino Unido. O trabalho teve como objetivo comparar as barreiras à adoção da série de normas ISO27000 com as normas ISO9000 e ISO14000 e supera-las, através de um processo, em cinco passos, desenvolvido pelo autor, denominado 5S2IS para pequenas e médias empresas (PME).

Este processo (5S2IS) foi construído sobre as fundações da ISO27001, ISO27002 e o Modelo de Maturidade de Capacidade (CMM) de Humphrey (1989).

A abordagem utilizada no processo mapeia o ciclo plan-do-check-act (PDCA) para o desenvolvimento em cinco estágios: Plan, Systemise, Monitor, Improve e Embed.

Como resultado final o autor desenvolveu uma abordagem que fornece um passo a passo e pode ser facilitada e mediada pela tecnologia, permitindo às PME proteger suas informações sem

precisar fazer uma mudança organizacional significativa e investimentos que não podem ser proporcionais aos riscos (GILLIES, 2011).

2.5.1.13 Information Security Culture Critical Success Factors

Trabalho apresentado na *12th International Conference on Information Technology – New Generations* em 2015. A pesquisa teve como objetivo principal examinar os fatores críticos de sucesso responsáveis pela cultura da segurança da informação nas organizações.

O autor utilizou uma análise da revisão da literatura na área de cultura de segurança da informação, a fim de compreender como criar um ambiente que apoia a adoção da cultura de segurança da informação.

Como resultado final o artigo em questão contribuiu para o conhecimento existente, fornecendo os principais fatores críticos necessários a existência da cultura de segurança da informação. Os principais fatores identificados na pesquisa foram: apoio da alta gestão, estabelecimento da política de segurança da informação eficaz, conscientização da segurança da informação, treinamento em segurança da informação, análise de riscos de segurança e avaliação, conformidade de segurança, políticas de conduta ética, e cultura da organização (ALNATHEER, 2015).

2.5.1.14 Effective Information Security Management: A critical success factors analysis

Tese de doutorado apresentada na *School of Graduate Studies* da *MCMaster University* de Hamilton, Ontario, em 2015. A pesquisa teve como objetivo principal, aplicar a abordagem dos fatores críticos de sucesso para a construção de um modelo teórico para investigar os principais fatores que contribuem para o sucesso da Gestão da Segurança da Informação (GSI).

A tese abordou três questões de pesquisa: Como medir o desempenho da GSI?; Quais são os fatores críticos que devem estar presentes para tornar a GSI eficaz?; e, Como esses fatores contribuem para o sucesso da GSI?

Segundo o autor, o estudo em questão contribui para o avanço da literatura de GSI propondo um modelo teórico para examinar os efeitos dos fatores críticos de sucesso

organizacional sobre o desempenho da GSI, validar empiricamente o modelo proposto, desenvolver e validar uma modelo de desempenho de GSI e revisar os mais influentes padrões de gerenciamento de segurança da informação e validar algumas diretrizes básicas do padrão.

Os resultados do trabalho demonstram que o gerenciamento bem-sucedido da segurança da informação pode ser alcançado através de controles de segurança da informação efetivamente desenvolvidos por meio do alinhamento do negócio, suporte organizacional, competências de TI e consciência organizacional dos riscos e controles de segurança (TU, 2015).

2.5.1.15 Information Security Maturity Model

Trabalho publicado no *International Journal of Computer Science and Security (IJCSS)* em 2011. A pesquisa tem como objetivo propor um modelo de maturidade de segurança da informação (ISMM) destinado a ser utilizado como uma ferramenta para avaliar a capacidade das organizações no cumprimento aos objetivos de segurança.

O autor identificou quatro domínios que afetam a segurança da informação em uma organização, sendo eles: a organização de governança, cultura organizacional, a arquitetura dos sistemas e o gerenciamento dos serviços. O modelo de maturidade proposto possui cinco níveis de conformidade, onde acredita-se que a organização melhore, com relação a segurança da informação, à medida que avança os níveis. Os níveis de conformidade são: Nenhuma Conformidade, Conformidade Inicial, Conformidade Básica, Conformidade Aceitável e Conformidade Total.

Ao final o autor informa que uma estrutura sistemática para realização de melhoria de *benchmarking* e desempenho foi desenvolvida e que o ISMM pode ser considerado um modelo de maturidade que implica em um sistema completo e de melhoria contínua (SALEH, 2011).

2.5.1.16 Information system security management (ISSM) success factor: retrospection from the scholars

Trabalho publicado na *11th European Conference on Information warfare and security* em 2012. O objetivo do estudo foi determinar, através de uma retrospectiva, os fatores mais influentes a respeito da implementação de um ISSM bem-sucedido em um negócio.

O autor informa que as três principais classes de fatores de sucesso no ISSM compreendem as características da tecnologia, estrutura organizacional e influencias ambientais.

Como resultado, a análise dos estudos anteriores mostrou que o sucesso de um ISSM é atribuído a três segmentos principais: Infraestrutura (infraestrutura de segurança e mecanismos de apoio), Estrutura Organizacional Física (tamanho e tipo do negócio), Estrutura Organizacional Lógica (apoio da alta administração, formalização e recursos) e Influencias Ambientais (governança, aplicação e estrutura de mercado) (NORMAN e YASIN, 2012).

2.5.1.17 ISO/IEC 27000, 27001 and 27002 for information security management

Artigo publicado no *Journal of Information Security* em abril de 2013. O trabalho apresentou as normas ISO 27000, 27001 e 27002 como padrões internacionalmente reconhecidos, e sua importância para o estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI).

O autor denomina estes padrões como a "linguagem comum de organizações em todo o mundo" para a segurança da informação. Todo o histórico e características das normas da família ISO 27000 são focadas na pesquisa com o intuito de demonstrar a sua importância para as organizações que desejam possuir seus processos de segurança da informação aceitos internacionalmente, através da certificação na ISO 27001.

Como resultado o autor deixa claro que um SGSI eficaz ajuda a reduzir os riscos e prevenir brechas de segurança, e essa eficácia pode ser alcançada através da adequação as normas 27000, 27001 e 27002 (DISTERER, 2013).

2.5.1.18 Maturity assessment and process improvement for information security management in small and medium enterprises

Artigo publicado no *Journal of Software: Evolution and Process* em julho de 2013. O trabalho propõe um método adaptado para pequenas e médias empresas para uma primeira avaliação de maturidade de segurança da informação e consequentemente melhorar os seus processos de conformidade.

O modelo foi desenvolvido para avaliar o nível de maturidade de segurança da informação e fornecer rapidamente uma visão geral da segurança da informação nas empresas. O método foi definido como um micro avaliação, sendo muito atraente para pequenas e médias empresas, devido ao fato de não dispender muitos recursos para sua execução.

Inicialmente estudos de caso foram realizados com pequenas e médias empresas de Luxemburgo para ajustes do modelo, após novos estudos de caso foram realizados com empresas maiores.

Os resultados da pesquisa mostram que o modelo proposto permite a introdução de conscientização de segurança nas pequenas e médias empresas. Os autores ainda informam que melhorias como a criação de uma plataforma em software irá fortalecer a base científica do método (CHOLEX e GIRARD, 2013).

2.5.1.19 Proposal to Structure the Information Security Management in a Scientific Research Environment

Trabalho apresentado no *7º CONTECSI – International Conference on Information System and Technology Management* em 2010, São Paulo, Brasil. A pesquisa teve como objetivo propor um estrutura de gestão de segurança da informação para uma instituição pública de pesquisa científica.

O autor buscou responder a seguinte questão de pesquisa: “ O que pode ser feito para potencializar a efetividade das normas e e procedimentos de segurança da informação em uma instituição pública de pesquisa científica da área nuclear no Brasil”?

A metodologia utilizada na pesquisa foi do tipo exploratório, e a coleta dos dados foi realizada nos tres níveis, Estratégico, Tático e Operacional.

Como resultado foi proposto um modelo de Gestão da Segurança da Informação. Constatou-se também que o principal requisito de segurança da informação no ambiente de pesquisa científica estudado é a integridade, seguido pela disponibilidade (ALEXANDRIA e QUONIAM, 2010).

2.5.1.20 Proposta de um Programa de Segurança da Informação para as Autarquias Federais

Artigo apresentado no Congresso InfoBrasil TI e Telecom em 2010. O trabalho teve como objetivo principal propor uma estrutura mínima e necessária, para o desenvolvimento de um Programa de Segurança da Informação que de apoio as autarquias federais, para o alcance dos objetivos de segurança da informação propostos pela Presidência da República.

No decorrer da pesquisa é apresentado a situação das autarquias federais, com relação a governança de TI, num levantamento realizado pela Secretaria de Fiscalização e Tecnologia da Informação (SEFTI), demonstrado também a situação preocupante da segurança da informação dos orgãos da administração pública federal. É levantado também o estado da arte em segurança da informação, demonstrando os principais conceitos relacionados à segurança da informação.

No último tópico do trabalho, é apresentado a proposta de desenvolvimento do Promogama de Segurança da Informação, baseado nas normas ABNT NBR ISO/IEC 27001:2006 e 27002:2005.

Como resultados esperados no desenvolvimento de um Programa de Segurança da Informação, seis itens foram específicados: Alinhamento Estratégico, Gerenciamento de Risco, Entrega de Valor, Gerenciamento de Recursos, Integração de Processos e Desempenho (JOHNSON e PINTO, 2010).

2.5.1.21 Towards a Taxonomy of Information Security Management Practices in Organizations

Trabalho apresentado na *25th Australasian Conference on Information Systems* em Auckland, Nova Zelândia em 2014. Este trabalho foi o primeiro de 4 estágios para desenvolvimento de uma taxonomia rigorosa, abrangente e empiricamente comprovada de

práticas de gestão de segurança da informação, fornecendo as organizações uma orientação abrangente.

Durante a pesquisa os autores demonstraram a importância da segurança da informação para as organizações através dos controles dos padrões já reconhecidos, como a família de normas ISO 27000.

Quanto a abordagem da pesquisa é utilizada uma taxonomia para classificação dos vários tipos de atividades de gestão de segurança da informação. A natureza da pesquisa foi exploratória e seguiu uma abordagem qualitativa. Este primeiro estágio consistiu em realizar uma revisão abrangente da literatura, buscando identificar o intervalo de práticas de gestão de segurança e sugerir possíveis maneiras de classificar a atividade de nível de gestão.

Como resultado os autores propuseram as seguintes áreas práticas de gestão de segurança: Política de Segurança; Gestão de Risco de Segurança; Resposta a Incidentes de Segurança; Treinamento, Educação e sensibilização em segurança; Gestão técnica e; Gestão de Contato intra-organização (ALSHAIKH, 2014).

2.5.2 Fatores Críticos de Sucesso na RSL

Durante a fase de leitura dos trabalhos selecionados na Revisão Sistemática da Literatura (RSL), vários fatores considerados críticos para o planejamento, implantação e manutenção da gestão da segurança da informação (GSI) foram citados. A aparição destes fatores, ocorreu de diversas formas diferentes, algumas vezes eram citados especificamente como fatores de sucesso para a gestão da segurança da informação, outras eram citados no decorrer do texto como um quesito essencial no processo de segurança da informação. Outro detalhe percebido durante a fase leitura, é que esses fatores foram citados utilizando diversos termos diferentes pelos autores, conforme Quadro 9.

Quadro 9. Fatores e Termos usados na identificação

Fator	Descrição	Termos usados nos trabalhos da RSL
Apoio da alta gestão	Compromisso e apoio da alta gestão	Comprometimento, Apoio, Suporte, Participação; Alta Gestão, Alta Gerência, Presidência, Direção, Alta Administração, Diretoria.
Treinamento e conscientização	Marketing eficaz de segurança para todos os gerentes e	Treinamento, Capacitação, Preparação; Conscientização, Sensibilização, Motivação.

	funcionários, através de educação e Treinamento em SI.	
Cultura de Segurança	Segurança da Informação consistente com a cultura organizacional	Cultura de Segurança; Comportamento de Segurança; Comportamento organizacional voltado a segurança da informação; Subcultura da cultura organizacional
Gestão de Riscos	Avaliação de Riscos para a compreensão dos requisitos de SI	Gestão, Gerenciamento, Análise, Estudo, Avaliação, Programa de Gestão, Sistema de Gestão; Riscos.
Política de Segurança	Implementação de uma política de segurança e sua divulgação na organização.	Política de Segurança; Politicas de Gestão de Segurança; Politica Corporativa de Segurança; Política de Segurança Organizacional.
Provisão de Recursos	Disponibilização de recursos para SI.	Provisão, Disponibilização, Fornecimento; Recursos Financeiros, Recursos Humanos, Recursos Tecnológicos.
Estrutura Organizacional	A SI é alcançada através da implementação de estruturas organizacionais próprias	Estrutura Organizacional de Gestão da Segurança da Informação; Gestão da Segurança da Informação Organizacional; Estratégia Organizacional; Estrutura de Segurança da informação agregada à cultura organizacional; Estrutura organizacional própria; Estrutura organizacional estratégica.
Alinhamento com os objetivos de negócio	Requisitos de segurança alinhados aos objetivos do negócio	Alinhamento, Direcionamento, Atendimento, Integração; Negócio, Objetivos de Negócio, Requisitos de Negócio, Estratégias do Negócio, Processo de Negócio.
Medição e avaliação da GSI	A efetividade dos procedimentos de segurança da informação deve ser constantemente avaliada	Medição, Monitoramento, Avaliação, Acompanhamento; dos controles da Gestão da Segurança
Papéis e Responsabilidades	Definição clara dos papéis e responsabilidades em SI	Papéis, Responsabilidades, Atribuições, Deveres; relacionados a segurança da informação
Competências da TI	Estabelecimento de um processo de gestão de incidentes de SI	Competência, Conhecimento, Capacidade, Habilidade; Equipe de TI
Gestão de Incidentes de SI	Competência da equipe de TI sobre SI	Gestão, Tratamento, Resposta; Incidentes de Segurança da Informação

Após a identificação dos fatores, buscou-se estipular um ranking, utilizando como critério de relevância a quantidade de artigos que os mencionaram como fatores essenciais para o sucesso da GSI. Ou seja, quanto mais bem colocado no ranking, mais trabalhos científicos citaram o referido fator. Estes fatores foram coletados e ordenados com base no número trabalhos em que foram citados na RSL, conforme Tabela 2.

Tabela 2. Ranking dos Fatores de Sucesso de GSI na RSL

Ranking	Fator	Trabalhos	Nº de Trabalhos com o fator
1º	Apoio da alta gestão	TU (2015), COELHO et al. (2014a), TORRES et al. (2010), STAMBUL e RAZALI (2011), FAZENDA e FAGUNDES (2015), MOETI e KELEMA (2014), ABNT (2005), YILDIRIM et al. (2011), QUINTELLA e BRANCO (2013), NORMAN e YASIN (2012), DISTERER (2013), ALEXANDRIA e QUONIAM (2010), JOHNSON e PINTO (2010), ALSHAIKH et al (2014), ALNATHEER (2015)	15
2º	Treinamento e conscientização	TU (2015), COELHO et al. (2014a), STAMBUL e RAZALI (2011), FAZENDA e FAGUNDES (2015), MOETI e KELEMA (2014), DZAZALI e ZOLAIT (2012), ABNT (2005), LANGE et al. (2015), YILDIRIM et al. (2011), QUINTELLA e BRANCO (2013), DISTERER (2013), ALEXANDRIA e QUONIAM (2010), ALSHAIKH et al (2014), ALNATHEER (2015)	14
3º	Cultura de Segurança da Informação	TU (2015), COELHO et al. (2014a), TORRES et al. (2010), STAMBUL e RAZALI (2011), FAZENDA e FAGUNDES (2015), MOETI e KELEMA (2014), DZAZALI e ZOLAIT (2012), LANGE et al. (2015), ABNT (2005), YILDIRIM et al. (2011), QUINTELLA e BRANCO (2013), JOHNSON e PINTO (2010), ALNATHEER (2015)	13
4º	Gestão de Riscos	TU (2015), COELHO et al. (2014), TORRES et al. (2010), STAMBUL e RAZALI (2011), FAZENDA e FAGUNDES (2015), MOETI e KELEMA (2014), DZAZALI e ZOLAIT (2012), LANGE et al. (2015), ABNT (2005), DISTERER (2013), ALEXANDRIA e QUONIAM (2010), ALSHAIKH et al (2014), ALNATHEER (2015)	13
5º	Política de Segurança da Informação	TU (2015), COELHO et al. (2014a), TORRES et al. (2010), STAMBUL e RAZALI (2011), MOETI e KELEMA (2014), LANGE et al. (2015), ABNT (2005), YILDIRIM et al. (2011), DISTERER (2013), ALEXANDRIA e QUONIAM (2010), ALSHAIKH et al (2014), ALNATHEER (2015)	12
6º	Provisão de Recursos	MOETI e KELEMA (2014), YILDIRIM et al. (2011), NORMAN e YASIN (2012), ALSHAIKH et al (2014), DISTERER (2013), TU (2015), JOHNSON e PINTO (2010), PARANHOS (2010), ALEXANDRIA e QUONIAM (2010), DZAZALI e ZOLAIT (2012)	10
7º	Papéis e Responsabilidades	PARANHOS (2010), TORRES (2010), STAMBUL e RAZALI (2011), LANGE et al. (2015), YILDIRIM et al. (2011), QUINTELLA e BRANCO (2013), DISTERER (2013), JOHNSON e PINTO (2010), TU (2015)	9
8º	Medição e avaliação da GSI	PARANHOS (2010), SALEH (2011), STAMBUL e RAZALI (2011), MOETI e KELEMA (2014), DISTERER (2013), RIGON et al., (2013), TU (2015), ALEXANDRIA e QUONIAM (2010)	7
9º	Estrutura	MOETI e KELEMA (2014), TU (2015), ALEXANDRIA e QUONIAM (2010), STAMBUL e RAZALI (2011), NORMAN	6

	organizacional	(2015), DZAZALI e ZOLAIT (2012),	
10º	Alinhamento com os objetivos de negócio	JOHNSON e PINTO (2010), PARANHOS (2010), STAMBUL e RAZALI (2011), DZAZALI e ZOLAIT (2012), SALEH (2011), TU (2015),	6
11º	Gestão de Incidentes de SI	ALSHAIKH et al (2014), PARANHOS (2010), ALEXANDRIA e QUONIAM (2010), DISTERER (2013), GILLIES (2011)	5
12º	Competências da TI	PARANHOS (2010), JOHNSON e PINTO (2010), MOETI e KELEMA (2014), TU (2015)	4

A partir da análise do Tabela 2, foi possível concluir que os fatores Apoio da Alta Gestão, Treinamento e Conscientização e Cultura de Segurança da Informação foram citados na maioria dos trabalhos selecionados na RSL, como sendo fatores de sucesso para a gestão da segurança da informação. Esses fatores estão relacionados diretamente ao fator humano das organizações. Tu (2015), afirma que a GSI é um processo dinâmico de tomada de deciões que envolve todos os componentes como infraestrutura organizacional, fatores humanos e práticas de segurança da informação. Para Mitnick e Simon (2003, apud Paranhos, 2010), "o fator humano é certamente o elo mais fraco da segurança". Corroborando com essa ideia, Dzazali e Zolait (2012) afirmam que o elemento humano representa a maior ameaça à segurança da informação de uma organização e este deve ser devidamente tratado. Ou seja, o processo de segurança da informação não abrange apenas a tecnologia, mas os fatores sociais.

Apesar dos fatores citados na Tabela 2 terem sido identificados nos trabalhos selecionados na RSL, eles não foram diretamente relacionados ao aprimoramento da maturidade da GSI, mas sim como fatores críticos para o sucesso da GSI de forma geral. O capítulo 5 deste trabalho buscou, nestes 12 fatores, encontrar o grau de importância que eles representam para o aprimoramento da maturidade da GSI.

2.6 Conclusão do capítulo

De maneira geral, este capítulo apresentou as informações relacionadas ao referencial teórico sobre a segurança da informação e gestão da segurança da informação (GSI) tendo como objetivo fundamentar todo o arcabouço teórico em torno da elevação da maturidade em GSI e identificação dos FCS que serviram de base para o resultado final desta pesquisa.

3 ESTUDO DE CAMPO

Este capítulo apresenta a coleta dos dados e a análise do estudo de campo realizado nas IFES. O estudo teve como objetivo fazer o levantamento e realizar um diagnóstico para identificar o nível de maturidade da gestão de segurança da informação das IFES estudadas. Posteriormente foi identificado os fatores críticos de sucesso para se alcançar cada um dos 5 níveis de maturidade dos quais as IFES necessitem se posicionar.

Este capítulo está subdividido nas seguintes seções:

- **Preparação do Estudo de Campo:** apresenta com detalhes como foi a preparação para a coleta dos dados;
- **Instrumento da Pesquisa:** apresenta a ferramenta utilizada para realização da avaliação de maturidade de GSI das IFES;
- **Descrição da população:** apresenta a população que foi definida para esta pesquisa;
- **Delimitação da amostra:** apresenta o método estatístico utilizado para definição da amostra para esta pesquisa.

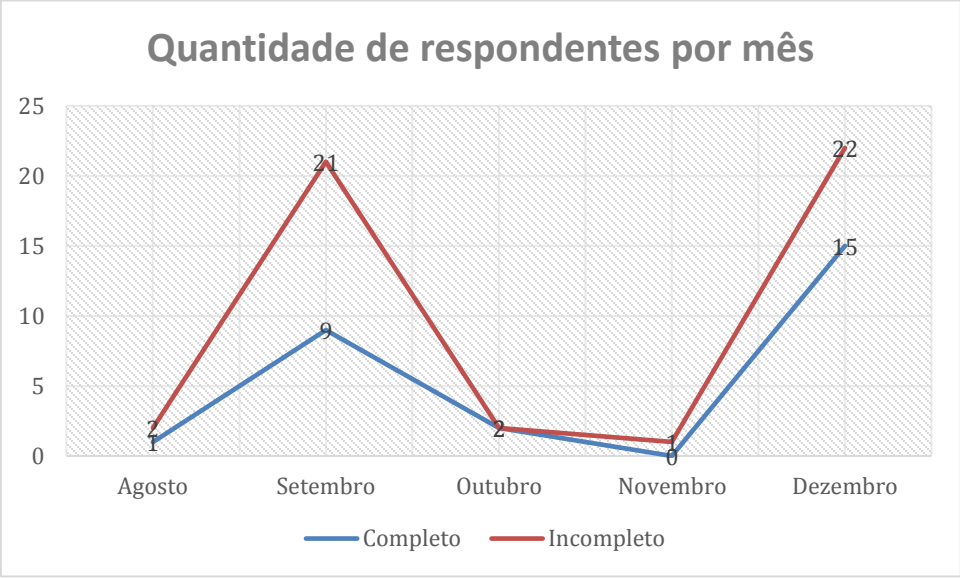
3.1 Preparação do Estudo de Campo

Após a definição da metodologia a ser aplicada, assim como as técnicas mais adequadas aos objetivos deste trabalho de pesquisa, iniciou-se o planejamento das ações para o seu desenvolvimento.

No dia 24 de agosto de 2016 foram contatados através de e-mail, sessenta e três (63) Universidades Federais e trinta e oito (38) Institutos Federais, dois (2) Centros Federais de Educação Tecnológica e um (1) Colégio Pedro II, totalizando 104 IFES, para que respondessem ao questionário de avaliação de maturidade de GSI. O e-mail continha os dados de apresentação do pesquisador, da pesquisa e o link para acesso ao questionário, além das orientações iniciais para o correto preenchimento.

Num primeiro momento somente 10 IFES responderam de forma completa o questionário e 23 começaram a responder, mas não completaram. Novamente em 26 de setembro de 2016, um novo e-mail foi enviado reiterando o e-mail anterior, solicitando mais uma vez a participação das IFES na pesquisa. Entre esse e-mail e o período final de disponibilidade do questionário (dezembro), diversas ligações foram feitas as Diretorias de TI das IFES, solicitando a participação na pesquisa. Desta vez, até o mês de dezembro foi possível obter mais 17 respostas completas e 25 respostas incompletas. No total obteve-se 27 respostas completas e 48 incompletas, conforme Gráfico 1.

Gráfico 1. Quantidade de respondentes por mês



O questionário ficou disponível para preenchimento no período entre 24/08/2016 a 30/12/2016, o qual foi necessário para obter o número de IFES respondentes.

3.2 Instrumento da Pesquisa

A *Information Security Program Assesment Tool* (Ferramenta de Avaliação de Programa de Segurança da Informação) faz parte da Iniciativa de Segurança Cibernética EDUCAUSE e foi criada por voluntários que fazem parte do HEISC - *Higher Education Information Security Council* (Conselho de Segurança da Informação do Ensino Superior). Essa Iniciativa de Segurança Cibernética auxilia as instituições de ensino superior com a melhoria na governança da segurança da informação, conformidade, proteção de dados e programas de privacidade. HEISC é

um esforço voluntário aberto a todos os profissionais de segurança da informação da educação, privacidade e outras áreas de TI.

De acordo com EDUCAUSE (2015), essa "ferramenta" foi criada para avaliar a maturidade dos programas de segurança da informação do Ensino Superior, utilizando a norma ISO/IEC 27002:2013 (Código de Prática para Controles de Segurança da Informação). Ela foi projetada para o uso por uma instituição como um todo, apesar de um setor dentro de uma instituição também pode usá-la, salvo disposto em contrário. Deve ser preenchida pelo diretor de tecnologia da informação, diretor de segurança da informação ou cargo equivalente.

A ferramenta de avaliação de maturidade do HEISC foi criada para ser utilizada anualmente, ou com a frequência que a instituição sentir a necessidade de avaliar e controlar a maturidade dos programas de gestão de segurança da informação.

A norma utilizada para definir a maturidade é a ISO/IEC 21827:2008 (Information technology – Security techniques – System Security Engineering – Capability Maturity Model (SSE-CMM)), que avalia os níveis numa escala de 0 a 5, sendo 5 o nível mais alto de maturidade (EDUCAUSE, 2015). Cada seção da ISO 27002:2013 será avaliada, alcançando uma média, que proporcionará a identificação do nível de maturidade.

A *Information Security Program Assesment Tool* foi a ferramenta escolhida e utilizada neste trabalho de pesquisa para identificação do nível de maturidade de GSI das IFES. Esta escolha se deu pelo fato dessa "ferramenta" ter sido desenvolvida especificamente para avaliar a maturidade dos programas de segurança da informação de Instituições de Ensino Superior e pelo fato de ser baseada em normas de renome e internacionalmente reconhecidas como a ISO/IEC 21827:2008 e a ISO/IEC 27002:2013. O resultado da aplicação desta "ferramenta" pode ser visto no Capítulo 4 deste trabalho.

A ferramenta foi estudada e baixada do site da Biblioteca EDUCAUSE em formato XLSM (Excel), e posteriormente traduzida e disponibilizada por meio eletrônico, através do software LimeSurvey, para as Diretorias de Tecnologia da Informação das IFES. O questionário é composto por um total de 101 perguntas e, em média, levou cerca de 30 minutos para que os respondentes completassem a ferramenta. O questionário completo pode ser visto no ANEXO I. .

Com essa ferramenta é possível alcançar a mesma classificação de maturidade em outros modelos como o CMMI, NIST, COBIT, ou outro que possua os mesmos 0 a 5 níveis de maturidade em sua estrutura (EDUCAUSE, 2015).

Para que a avaliação da maturidade seja realizada adequadamente, cada pergunta deve ser respondida, selecionando o nível adequado de maturidade de 0 a 5. Cada seção da ISO 27002:2013 será avaliada, alcançando uma média, que proporcionará a identificação do nível de maturidade. A classificação das questões pode ser melhor observada na Quadro 10.

Quadro 10. Classificação do questionário

Norma ISO	Questões	Exemplo de Questão
Gestão de Riscos (ISO 27005:2011)	1 a 3	A sua instituição tem um programa de gestão de riscos?
Política de Segurança da Informação (Seção 5 da 27002:2013)	4 a 6	A sua instituição tem uma política de segurança da informação aprovada pela administração?
Organização da Segurança da Informação (Seção 6 da 27002:2013)	7 a 13	A responsabilidade está claramente atribuída a todas as áreas da arquitetura da segurança da informação?
Segurança de Recursos Humanos (Seção 7 da 27002:2013)	14 a 18	A sua instituição realiza formação especializada baseada em funções?
Gestão de Ativos (Seção 8 da 27002:2013)	19 a 20	A sua instituição realiza a classificação das informações?
Controle de Acesso (Seção 9 da 27002:2013)	21 a 35	A sua instituição tem uma política de controle de acesso para autorização e revogação de direitos de acesso?
Criptografia (Seção 10 da 27002:2013)	36 a 38	A sua instituição utiliza métodos de criptografia apropriados para proteger dados confidenciais em trânsito?
Segurança Física e de Ambiente (Seção 11 da 27002:2013)	39 a 44	O centro de dados de sua instituição possui controle de acesso físico?
Segurança nas Operações (Seção 12 da 27002:2013)	45 a 64	O processo de backup dos dados está consistente com os requisitos de disponibilidade da sua instituição?
Segurança nas Comunicações (Seção 13 da 27002:2013)	65 a 70	A sua instituição exige confidencialidade ou acordos de confidencialidade para empregados ou terceiros?
Aquisição, Desenvolvimento e Manutenção de Sistemas (Seção 14 da 27002:2013)	71 a 84	A sua instituição tem um processo para validade a segurança dos produtos de software e serviços adquiridos?
Relacionamento com Fornecedores (Seção 15 da 27002:2013)	85 a 90	A sua instituição possui requisitos de segurança nos contratos com entidades externas, antes de conceder acesso aos ativos de informação?
Gestão de Incidentes de Segurança da Informação (Seção 16 da	91 a 92	Possui procedimentos de tratamento de incidentes para informar e responder a eventos de segurança em todo o ciclo de vida do

27002:2013)		incidente, incluindo a definição de papéis e responsabilidades?
Aspectos de Segurança da Informação na Gestão de Continuidade dos Negócios (Seção 17 da 27002:2013)	93	A sua instituição tem um plano documentado continuidade de negócios de tecnologia da informação que é baseado em uma análise de impacto nos negócios, é testado periodicamente, e tem sido analisado e aprovado por altos funcionários ou do conselho de administração?
Conformidade (Seção 18 da 27002:2013)	94 a 101	A sua instituição tem uma política de proteção de dados aplicável que abrange informações de identificação pessoal (PII)?

Fonte: adaptado de EDUCAUSE (2015)

Abaixo está um resumo do foco da Gestão de Riscos (ISO/IEC 27005) e de cada seção da norma 27002 de 2013 usado na ferramenta (EDUCAUSE, 2015):

- Gestão de Riscos (ISO 27005): avaliar como a instituição realiza a gestão dos riscos de segurança da informação.
- Políticas de Segurança da Informação (ISO 5): avaliar como uma instituição manifesta a sua intenção no que diz respeito à segurança da informação.
- Organização da Segurança da Informação (ISO 6): avaliar como uma instituição gere a sua segurança da informação em toda a empresa, incluindo a forma como a liderança institucional compromete o seu apoio e fornece orientação geral.
- Segurança em Recursos Humanos (ISO 7): avaliar as salvaguardas e os processos de uma instituição para assegurar que todos os funcionários são qualificados para e compreender os seus papéis e responsabilidades de suas funções de trabalho e que o acesso é removido uma vez que o vínculo é encerrado.
- Gestão de Ativos (ISO 8): avaliar programa de gerenciamento de ativos de uma instituição. Será que são incluídas maneiras de identificar, rastrear, classificar e atribuir a propriedade dos ativos mais importantes para garantir que eles sejam devidamente protegidos?
- Controle de Acesso (ISO 9): avaliar o uso de uma instituição de recursos administrativos, físicos, técnicos ou de segurança para gerenciar como os usuários e sistemas se comunicam e interagem com outros recursos de informação.
- Criptografia (ISO 10): avaliar as políticas da instituição sobre o uso de criptografia (criptografia) e gerenciamento de chaves.

- Segurança Física e do Ambiente (ISO 11): avaliar as etapas de uma instituição tomadas para proteger os sistemas, edifícios e infraestruturas de apoio relacionada contra ameaças associadas ao seu ambiente físico.
- Segurança nas Operações (ISO 12): avaliar as políticas de uma instituição formalizadas, procedimentos e controles, que auxiliam na proteção de dados e do sistema.
- Segurança nas Comunicações (ISO 13): avaliar as políticas de uma instituição formalizadas, procedimentos e controles, que auxiliam na gestão da rede e operação.
- Aquisição, Desenvolvimento e Manutenção de Sistemas (ISO 14): avaliar se uma instituição tem requisitos de segurança estabelecidos como parte integrante do desenvolvimento ou implementação de um sistema de informação.
- Relacionamento com Fornecedores (ISO 15): avaliar como uma instituição interage com terceiros para proteger adequadamente os recursos de informação e tecnologia que terceiros tenham acesso, processar e gerenciar.
- Informações sobre Gerenciamento de Incidentes de Segurança da Informação (ISO 16): avaliar programa de gerenciamento de incidentes de segurança da informação de uma instituição. Um programa eficaz irá garantir pessoal são treinados e equipados para detectar, informar e responder a eventos adversos.
- Aspectos de Segurança da Informação na Gestão da Continuidade do Negócio (ISO 17): avaliar a gestão de continuidade de negócios de uma instituição. A instituição madura tem um método de gestão, a organização para o desenvolvimento de procedimentos para assegurar a continuidade das operações em circunstâncias extraordinárias, incluindo a manutenção de medidas para garantir a privacidade e segurança dos seus recursos de informação.
- Conformidade (ISO 18): avaliar a conformidade dos processos de segurança da informação com as exigências legais e contratuais.

3.3 Descrição da população

A população foco desta pesquisa foram as Diretorias de Tecnologia da Informação, mais

especificamente os diretores, gestores de segurança e servidores da área de TI que estejam ligados com a gestão da segurança da informação das Instituições Federais de Ensino Superior.

As instituições pesquisadas neste trabalho, tratam-se de Universidades Federais e de Institutos Federais. A Lei 9.394, de 29 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional, define em seu Art. 52:

> Universidades – são instituições pluridisciplinares de formação dos quadros profissionais de nível superior, de pesquisa, de extensão e de domínio e cultivo do saber humano, que se caracterizam por:
>
> I - produção intelectual institucionalizada mediante o estudo sistemático dos temas e problemas mais relevantes, tanto do ponto de vista científico e cultural, quanto regional e nacional;

A Lei nº 11.892, de 29 de dezembro de 2008, que institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências, define em seu Art. 2º:

> Institutos Federais - são 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.

Além de universidades e institutos federais, estão incluídos na população 2 centros federais de educação tecnológica e 1 Colégio Pedro II. Totalizando um total de 104 Instituições Federais de Ensino Superior.

3.4 Delimitação da Amostra

A delimitação da amostra para esse estudo utilizou o tipo de amostra probabilista casual simples. Kauark (2010), afirma que "neste tipo de amostra cada elemento da população tem oportunidade igual de ser incluído".

Gil (2009, apud Teixeira Filho, 2010) informa que os quatro elementos que determinam o tamanho da amostra são: a amplitude do universo, podendo ser definida como finita (quando não excede a 100.000 elementos) ou infinita (quando excede a 100.000 elementos); o nível de confiança que refere-se à área da curva "normal" definida a partir dos desvios-padrão em relação

à sua média (1 desvio padrão corresponde a 68,8% de nível de confiança, 2 corresponde a 95,5% e 3 corresponde a 99,7%); o erro máximo permitido que é expresso em termos percentuais e; a percentagem com que o fenômeno se verifica.

Este estudo considerou o cálculo da Amostra finita, pois a quantidade de IFES (104) é inferior a 100.000 elementos. Desta forma, foi adotado a fórmula para o cálculo de amostras para populações finitas, conforme Figura 7.

Figura 7. Fórmula de cálculo para Amostra Finita

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

Fonte: adaptado de Gil (2008)

Onde:

- n = tamanho da amostra;
- σ^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);
- e^2 = erro máximo permitido.

Considerando os resultados apurados no Índice de Governança de TI de 2014 (iGovTI2014), obteve-se os seguintes percentuais quanto ao número de instituições que adotam integralmente as práticas de Gestão de Riscos de TI nos órgãos da Administração Pública Federal (APF) (BRASIL, 2014):

- 10%: identificam os riscos de TI dos processos críticos de negócio;
- 9%: avaliam os riscos de TI dos processos críticos de negócio;
- 6%: tratam os riscos de TI dos processos críticos de negócio;
- 9%: executam um processo de gestão de riscos de TI;
- 8%: o processo de riscos de TI está formalmente instituído.

Tirando a média desses valores, obteve-se uma estimativa percentual de 8,4% dos órgãos da APF que adotam integralmente as práticas de Gestão de Riscos de TI. Torres et al. (2010) e ABNT (2013), afirmam que a Gestão de Riscos de TI, é o primeiro passo na definição dos

requisitos para a Gestão da Segurança da Informação, direcionando as ações apropriadas. Dessa forma, ficou estabelecido, para efeitos desta pesquisa, que o percentual com o qual o fenômeno se verifica foi ajustado para 8,4%, logo p é igual a 8,4. Com isso identificamos que q é igual a 100 – 8,4, ou seja 91,6.

Com relação ao nível de confiança, foi estabelecido 1 desvio padrão correspondente a 68,0% e um erro máximo de 5,0%. Aplicando-se a formula encontrou-se o seguinte resultado, conforme Figura 8.

Figura 8. Calculo para Amostra Finita

$$n = \frac{1^2 . 8{,}4 . 91{,}6 . 104}{5^2 (104 - 1) + 1^2 . 8{,}4 . 91{,}6} = \frac{80021{,}76}{3344{,}44} = 23{,}93$$

Fonte: adaptado de Gil (2008)

Com base no resultado apresentado pelo cálculo da fórmula (Figura 9), observou-se a necessidade de um quantitativo mínimo de 23,93 respondentes em uma população de 104 IFES. Esse número foi arredondado para 24 respondentes. O número de respostas recebidas durante a fase de coleta foi de 27 instituições, ou seja, acima do quantitativo mínimo estabelecido no cálculo da amostra finita.

3.5 Seleção e organização dos dados

Gil (2010), afirma que conforme os dados da pesquisa são agrupados, existe a necessidade de examina-los para verificar se estão completos, claros, coerentes e precisos. Durante a fase de recebimento das respostas do questionário aplicado as IFES, percebeu-se que muitos respondentes não completavam o questionário, resultando em respostas incompletas. Estes não foram considerados como respondentes válidos para a pesquisa durante a fase de resultados do diagnóstico de maturidade.

Com relação a participação das instituições, um total de 75 respostas foram registradas na base de dados do questionário eletrônico (LimeSurvey). Porém, após a finalização do período de

preenchimento do questionário, 48 dessas respostas foram desconsideradas por estarem incompletas ou em duplicidade. Desta forma, 27 respostas foram consideradas válidas para a participação na etapa de resultados. Destas, estão incluídos institutos federais e universidades federais, conforme Tabela 3.

Tabela 3. Quantidade de respondentes

IFES	**Recebimento das Respostas**		
	Completas	**Incompletas**	**Total**
Institutos Federais	16	15	**31**
Universidades Federais	11	5	**16**
Sem Identificação	0	28	**28**
Total	**27**	**48**	**75**

Dessa forma, as informações que foram tabuladas e apresentadas em análise exploratória são referentes as 27 respostas completas, representando um quantitativo acima dos 100% necessário para a amostra mínima de 24, conforme calculado na delimitação da amostra (Figura 8). Por meio da Tabela 3, é possível verificar que a maior representatividade nesta pesquisa foi de institutos federais, com 16 instituições, enquanto que universidades federais ouve um quantitativo de 11 instituições. Isso se deve ao fato deste pesquisador ter um contato mais próximo de institutos federais do que com universidades.

No próximo capítulo são apresentados os resultados da análise e o diagnóstico de maturidade das instituições pesquisadas.

3.6 Conclusão do capítulo

O presente capítulo buscou apresentar todos os dados referente ao estudo de campo realizado nas IFES, caracterizando o campo de pesquisa, as técnicas utilizadas para alcance do público alvo, o instrumento utilizado para avaliação e a seleção e organização dos dados. O número total de participantes na pesquisa foram 75, destes apenas 27 respostas foram de fato utilizadas para a análise dos dados. O resultado do cálculo amostral foi de 24, logo o número de respostas completas (27) atendeu satisfatoriamente para o resultado da pesquisa.

4 RESULTADOS DO DIAGNÓSTICO DE MATURIDADE

Os dados obtidos por meio do estudo de campo foram analisados a partir da aplicação do questionário nas IFES. Ao final da coleta, foi apresentado um resultado com o quantitativo de 27 respostas completas e satisfatórias, já definidas anteriormente na seção 3.4 (Delimitação da Amostra), com os níveis de maturidade da gestão da segurança da informação (GSI).

O método de percentagem foi utilizado para análise dos resultados dessa pesquisa. Este método serve para dar forma numérica as características qualitativas e reduzem as distribuições por frequência a uma base comum, simplificando a comparação (MARKONI e LAKATOS, 2011).

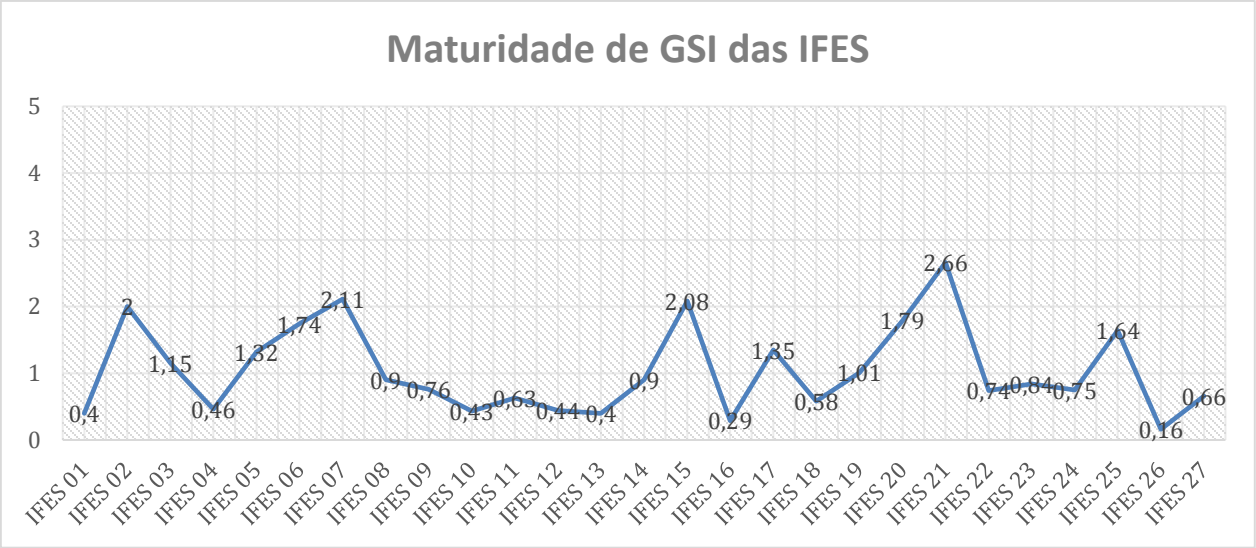
O questionário aplicado buscou levantar informações necessárias para identificar o nível de maturidade em GSI nas instituições pesquisadas. Este capítulo está dividido nas seguintes seções:

- **Resultados do Diagnóstico de Maturidade de Geral:** apresentação de uma análise geral do nível de maturidade de GSI das IFES estudadas.
- **Resultados do Diagnóstico de Maturidade por Domínio:** apresentação da análise dos resultados e diagnóstico de maturidade das IFES por domínio da 27002.

4.1 Resultados do Diagnóstico de Maturidade Geral

Esta seção tem por objetivo apresentar os resultados do levantamento e a identificação da maturidade da GSI das IFES pesquisadas. Para fins desta pesquisa, as instituições foram identificadas com uma numeração, para garantir a sua confidencialidade e melhor representação dos resultados, tais como: IFES 01, IFES 02... IFES 27. Essa numeração foi estabelecida com base na organização por ordem alfabética dos nomes das IFES. O Gráfico 2, apresenta o resultado acerca do levantamento de maturidade nas IFES pesquisadas.

Gráfico 2. Maturidade de GSI das IFES



O que se percebe é um baixo índice de maturidade de gestão da segurança da informação por parte das IFES, de modo que o maior nível de maturidade alcançado foi de 2,66, ou seja, das 27 instituições pesquisadas nenhuma foi identificada nos níveis de maturidade 3, 4 ou 5. Outra conclusão preocupante é que grande parte das IFES pesquisadas não chegou nem ao nível de maturidade 1, no qual as práticas de GSI são realizadas informalmente, sem documentação ou planejamento. Este resultado corrobora com Alexandria e Quoniam (2010), que afirmam que as instituições públicas, apesar da regulamentação existente, não sofrem maiores pressões dos órgãos superiores para proverem a proteção de suas informações e que estas instituições ainda tem um longo caminho a percorrer para atingir bons níveis de maturidade em relação a segurança da informação.

Por meio da classificação, foi possível identificar as IFES melhores colocadas quanto a maturidade de GSI, desta forma observou-se que apenas 4 IFES alcançou o nível de maturidade 2 e 16 IFES não chegaram ao nível de maturidade 1, ficando no nível 0, conforme Tabela 4.

Tabela 4. Classificação das IFES quanto a maturidade

Classificação	IFES	Maturidade Média
1	IFES 21	**2,66**
2	IFES 07	**2,11**
3	IFES 15	**2,08**
4	IFES 02	**2,00**
5	IFES 20	**1,79**
6	IFES 06	**1,74**
7	IFES 25	**1,64**
8	IFES 17	**1,35**

9	IFES 05	**1,32**
10	IFES 03	**1,15**
11	IFES 19	**1,01**
12	IFES 08	**0,90**
13	IFES 14	**0,90**
14	IFES 23	**0,84**
15	IFES 09	**0,76**
16	IFES 24	**0,75**
17	IFES 22	**0,74**
18	IFES 27	**0,66**
19	IFES 11	**0,63**
20	IFES 18	**0,58**
21	IFES 04	**0,46**
22	IFES 12	**0,44**
23	IFES 10	**0,43**
24	IFES 01	**0,40**
25	IFES 13	**0,40**
26	IFES 16	**0,29**
27	IFES 26	**0,16**

Alguns fatores ambientais organizacionais podem ter influencia com o resultado de maturidade obtido pelas IFES. Estes fatores vão desde a cultura da instituição, estrutura organizacional, infraestrutura e tempo de instituição. Percebeu-se que as instituições com um tempo de existência considerável e com uma estrutura organizacional específica para a segurança da informação, ou seja, as instituições que possuem setores e cargos específicos para tratar da segurança da informação, foram as mais bem colocadas na classificação. Outra característica importante é que das 5 IFES melhores colocadas, 3 são do Centro-Oeste do Brasil, levando a crer numa certa evolução nesta região quanto a segurança da informação. Quanto as IFES com os índices de maturidade mais baixos, são instituições (em sua maioria) que não possuem uma estrutura organizacional específica para a segurança da informação. Identificou-se que das 5 IFES com menor nível de maturidade, 3 são da região Norte.

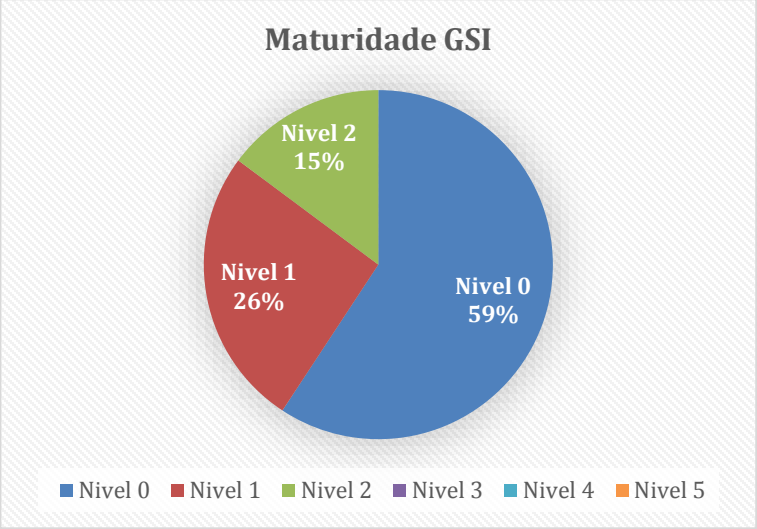
Para este diagnóstico foram considerados os níveis de maturidade inteiros, não fracionados, ou seja, se uma instituição foi identificada no nível de maturidade médio de 1,8, ela será incluída na análise como parte das instituições que estão no nível de maturidade 1. Se outra instituição foi identificada com o nível de maturidade médio de 0,7, ela será contabilizada com as instituições que estão no nível de maturidade 0, e assim sucessivamente.

Os resultados encontrados após coleta dos dados demonstram que as instituições ainda têm muito a evoluir com relação a gestão da segurança da informação. A maioria das IFES

pesquisadas foram identificadas no nível de maturidade 0 (59%), no qual poucos ou nenhum procedimento de segurança da informação estão sendo realizados, conforme Gráfico 3.

As IFES com melhor índice de maturidade foram identificadas no nível 2, com um total de 15%. Neste nível as práticas base para elaboração de uma GSI eficaz são planejados e gerenciados. Nenhuma das instituições pesquisadas foram identificadas nos níveis de maturidade 3, 4 ou 5, revelando um quadro preocupante na gestão da segurança da informação das Instituições Federais de Ensino Superior.

Gráfico 3. Maturidade de GSI geral



A situação crítica apresentada no gráfico 3, fortalece o que já foi demonstrado nos levantamentos realizados pelos iGovTI de anos anteriores, já citados no Item 1.1 desta pesquisa. A exemplo, o Acordão 3117/2014 TCU-Plenário, que concluiu que o nível de adoção das práticas de Gestão Corporativa de Segurança da Informação está muito distante do esperado, revelando lacunas na coordenação e na normatização da GSI, expondo a administração pública federal a diversos riscos, como indisponibilidade de serviços e perda da integridade das informações (BRASIL, 2014). O mesmo documento afirma 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 controles voltados à proteção das informações.

4.2 Resultados do Diagnóstico de Maturidade por Domínio

Esta seção apresenta um diagnóstico dos principais pontos de Gestão de Segurança da Informação das IFES pesquisadas. Para isso, apresenta-se uma análise holística dos resultados, dispostos nos quadros e figuras gerados a partir das respostas dos questionários. A análise apresentada a seguir, será da Gestão de Riscos (ISO 27005) e de cada uma das seções (domínios) da ISO 27002:2013, utilizadas na ferramenta de avaliação de maturidade.

Assim como o diagnóstico anterior, neste diagnóstico foram considerados os níveis de maturidade inteiros, não fracionados, ou seja, se uma instituição foi avaliada com nível de maturidade médio de 1,8 no domínio Política de Segurança, ela será incluída na análise como parte das instituições que estão no nível de maturidade 1. Se no domínio Gestão de Ativos, essa mesma instituição foi avaliada com o nível de maturidade médio de 0,7, ela será contabilizada com as instituições que estão no nível de maturidade 0 neste domínio, e assim sucessivamente.

4.2.1 Gestão de Riscos de Segurança da Informação

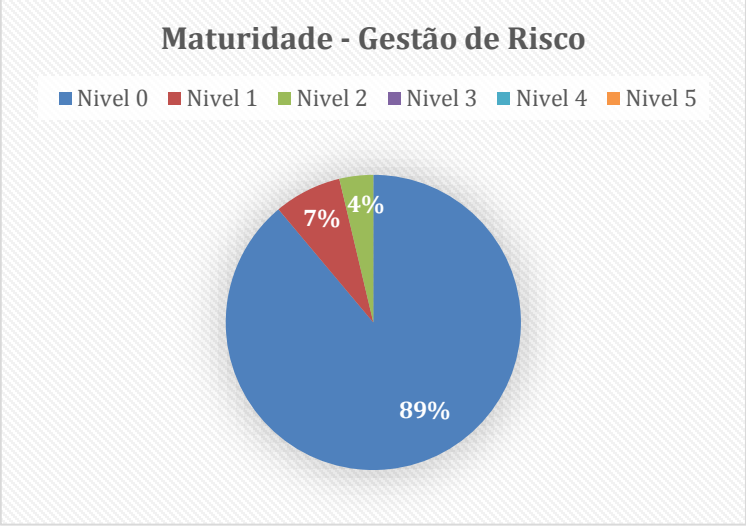
Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da Gestão de Riscos de Segurança da Informação das IFES pesquisadas. A norma NBR ISO/IEC 27002 deixa claro que uma das principais fontes dos requisitos de segurança de uma organização é a avaliação de riscos, levando em conta os objetivos e as estratégias globais do negócio da organização (ABNT, 2013b).

Para que uma gestão de riscos de segurança da informação possa ser realizada de maneira eficaz, diversas normas e procedimentos estão disponíveis para as organizações, dentre elas destacam-se:

- ABNT NBR ISO/IEC 27005: norma internacional que fornece diretrizes sobre a gestão de riscos de segurança da informação;
- NC 04/IN01/DSIC/GSI/PR: estabelece diretrizes para o processo de Gestão de Riscos da Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta (BRASIL, 2013).

Quando avaliadas (questões 1 a 3) sobre os procedimentos de gestão de riscos de segurança da informação, o Gráfico 4 demonstra que a maioria das IFES pesquisadas (89%) estão no nível de maturidade 0 (Não Realiza) neste domínio. Assim, é possível constatar que a maioria das IFES não possuem um processo de Gestão de Riscos de Segurança da Informação ou o processo existente não está bem estruturado.

Gráfico 4. Maturidade Gestão de Riscos



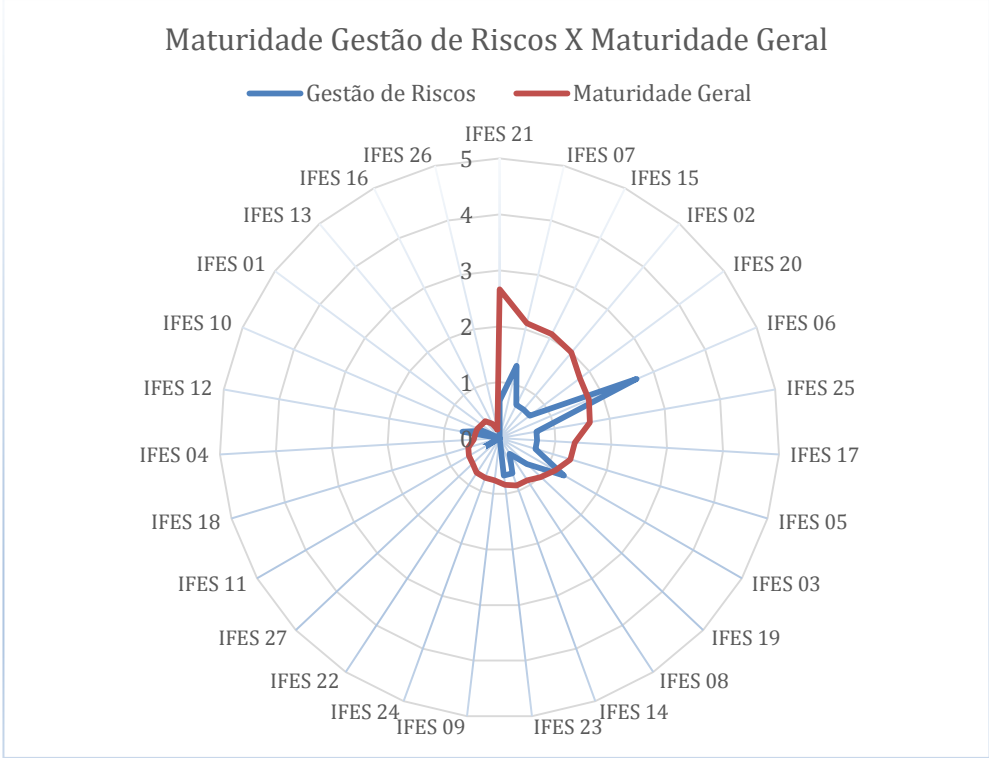
No nível de maturidade 1 (Realiza Informalmente) foram identificadas 7% e no nível de maturidade 2 (Planejado), 4%. Desta forma, observou-se que algumas instituições iniciaram o processo de gestão de riscos, mas ainda estão na fase inicial e/ou de planejamento.

Nenhuma das instituições pesquisadas foram identificadas nos níveis de maturidade 3 (Bem Definido), 4 (Controlado) ou 5 (Melhoria contínua). Este fato evidencia o quadro crítico em que se encontram as IFES no domínio Gestão de Riscos de Segurança da informação. Este resultado corrobora com o levantamento realizado pelo TCU em 2014 nos órgãos da APF, no qual identificou-se que 21% (9% parcialmente e 12% integralmente) realizam um processo gestão de riscos e apenas 14% (6% parcialmente e 8% integralmente) o formalizaram (BRASIL, 2014). É através da avaliação de riscos que são identificadas as ameaças aos ativos, suas vulnerabilidades, as probabilidades de ocorrência e impacto aos negócios (ABNT, 2013).

O Gráfico 5 apresenta um quadro comparativo entre a maturidade no domínio Gestão de Riscos de Segurança da Informação e a maturidade geral obtidas pelas instituições pesquisadas.

Nele, observou-se uma grande distância entre os itens comparados, ou seja, o processo de gestão de riscos de segurança da informação está sendo pouco ou nada trabalhado em comparação a maturidade geral obtidas pelas IFES. Somente as IFES 06 e 03 obtiveram suas maturidades no domínio Gestão de Riscos (2,67 e 1,33), maior que sua maturidade geral (1,74 e 1,15). As normas 27001, 27002 e 27005, deixam claro que o primeiro passo para gerir a segurança da informação é através da gestão de riscos (ABNT, 2013a; ABNT, 2013b; ABNT, 2011).

Gráfico 5. Comparativo Maturidade Gestão de Riscos X Maturidade Geral



Esse resultado ajuda a justificar o baixo índice de maturidade geral que se encontram as IFES estudadas nesta pesquisa. Torres et al. (2010), explica que os resultados das análises de risco ajudam a direcionar e estabelecer as ações apropriadas e as prioridades gerenciais dos riscos de segurança da informação. Ou seja, sem uma análise concreta dos riscos de segurança da informação todo o processo de gestão de segurança da informação é afetado.

Johnson e Pinto (2010), em seu trabalho “Proposta de um Programa de Segurança da Informação para as Autarquias Federais”, afirma que a habilidade em identificar adequadamente os riscos da informação e dos ativos de propriedade intelectual requer a cooperação de colaboradores de toda a organização.

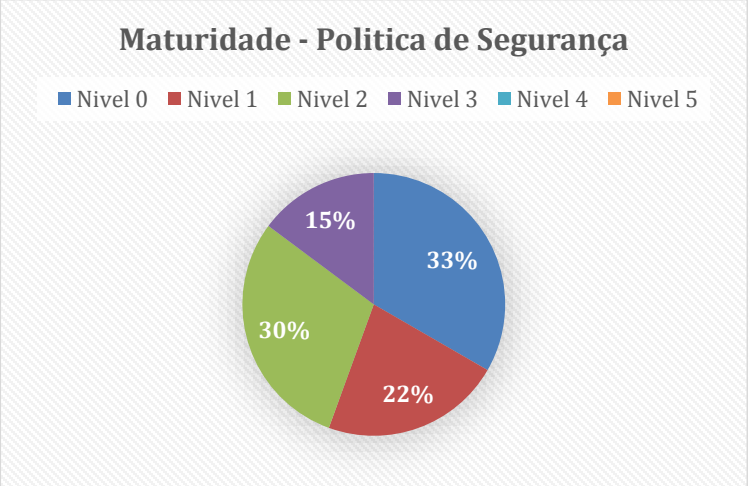
4.2.2 Política de Segurança da Informação

Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 5 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Nesta seção são tratados aspectos relativos a política de segurança da informação (PSI) e seus requisitos, apresentando como deve ser desenvolvido, mantido e atualizado o documento da política. Ela é composta por duas categorias principais (ABNT, 2013b; COELHO et al, 2014a):

- Políticas para segurança da informação – descreve o que convém que o documento da política deva conter e a importância de sua divulgação a organização.
- Análise crítica das políticas para segurança da informação – apresenta como deve ser realizada a análise crítica pela direção da organização em intervalos planejados, ou quando ocorrerem mudanças significativas.

Quando avaliadas (questões 4 a 6) na seção PSI e seus objetivos, a maior parcela das IFES pesquisadas (33%) ainda está no nível de maturidade 0. O que significa que essas instituições ainda não possuem uma PSI instituída, ou ela não está devidamente implementada e não há um planejamento para sua elaboração, conforme Gráfico 6.

Gráfico 6. Maturidade Política de Segurança



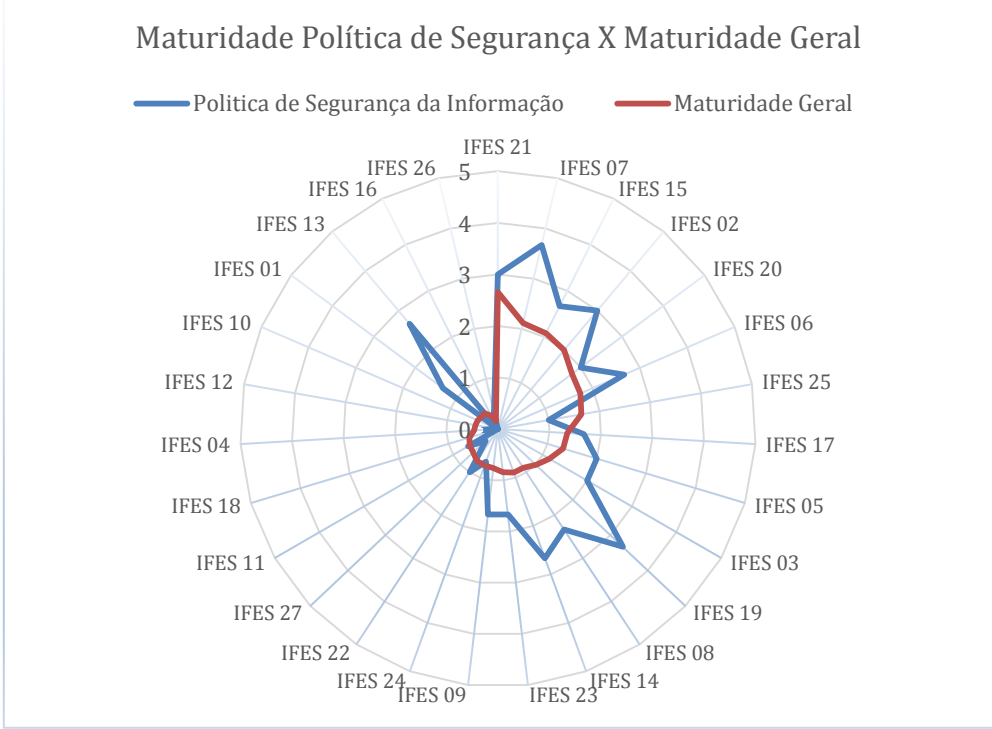
Esse resultado corrobora com o trabalho de Rios (2016), no qual a maior parte das IFES consultadas na pesquisa (57%) informaram não possuir PSI. O mesmo autor constatou também que a carência dos fatores Apoio da Alta Gestão, Treinamento em Segurança da Informação e

Comprometimento da Equipe Responsável são críticos para a elaboração da PSI, segundo os respondentes.

Trabalhos como Tu (2015), Coelho et al. (2014), Torres et al. (2010), Stambul e Razali (2011), Moeti e Kelema (2014), Lange et al. (2015), Yildirim et al. (2011), Disterer (2013) e Alexandria e Quoniam (2010), afirmam que a Política de Segurança da Informação (PSI) é um Fator Crítico de Sucesso (FCS) para uma efetiva Gestão de Segurança da Informação numa organização.

Quando comparados os resultados da maturidade da PSI com a maturidade geral, o Gráfico 7 deixa evidente que a política de segurança é uma área que está com uma boa evolução, quando comparada as outras, visto que grande parte das IFES pesquisadas obtiveram a maturidade da PSI acima de sua maturidade geral. O fato de 30% das instituições já estarem no nível de maturidade 2 e 15% no nível 3, perfazendo um total de 45%, evidencia que as IFES já estão começando a voltar sua atenção a elaboração de uma PSI mais eficaz. Apenas as IFES 10, 12, 16 e 18 obtiveram nível de maturidade 0 no domínio Política de Segurança.

Gráfico 7. Comparativo Maturidade PSI X Maturidade Geral



Estes dados se confirmam através dos resultados apresentados pelo iGovTI2014, no qual revelou que 68% das instituições pesquisadas declararam adotar a prática da PSI, contra apenas 44% no levantamento anterior (IGovTI2012), ou seja, uma evolução de 24 pontos percentuais (Brasil, 2014). Entretanto, esses resultados ainda estão muito distantes do esperado pelos órgãos reguladores.

Buscando a solução para a falta do estabelecimento e adoção da PSI nos órgãos da Administração Pública Federal (APF), vários autores propuseram em seus trabalhos de pesquisa ações para este problema. Rios (2016), definiu um guia para implementação e revisão da PSI em Instituições Federais de Ensino Superior, baseado nas melhores práticas recomendadas pelo COBIT 5, ITIL v3 e ISO/IEC 27002:2013. Quintela e Branco (2013), identificaram os fatores críticos de sucesso para a implantação da PSI em um órgão da APF. A própria Norma Complementar 03/IN01/DSIC/GSIPR estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da PSI nos órgãos e entidades da APF, direta e indireta (BRASIL, 2009). Contudo, os níveis de maturidade de PSI das IFES ainda estão muito baixos, conforme apresentado nos Gráficos 5 e 6.

4.2.3 Organização da Segurança da Informação

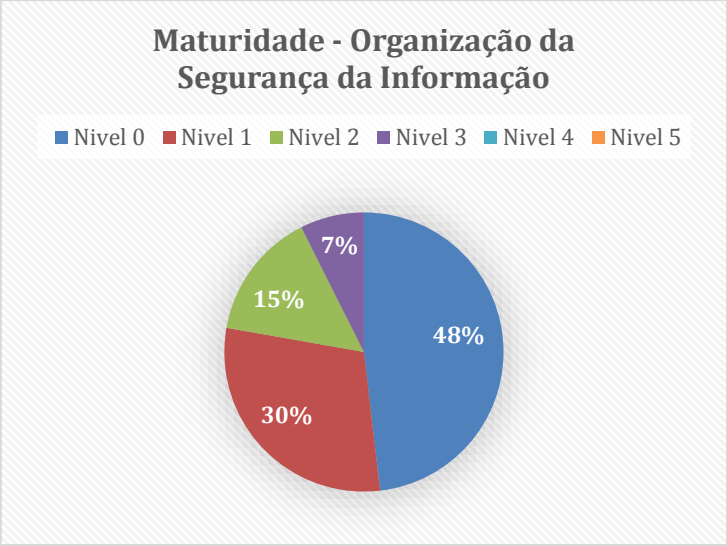
Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 6 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Nesta seção são apresentados os controles para estruturar o gerenciamento da segurança da informação dentro da organização, além dos controles para que se possa manter a segurança dos recursos que processam as informações disponibilizados através de dispositivos móveis ou trabalho remoto. Ela está dividida em duas categorias principais (ABNT, 2013b; COELHO et al., 2014a):

- Organização interna – esta categoria possui cinco controles que devem ser implementados na organização e tratam da estruturação da segurança, seus processos de autorização, confidencialidade, definição de papéis e responsabilidades, contatos com autoridades e grupos especiais.

- Dispositivos móveis e trabalho remoto – trata dos controles essenciais para a gerencia da segurança da informação no trabalho remoto e na utilização de dispositivos móveis.

Quando questionadas (questões 7 a 13) a respeito de controles da referida seção, observou-se que a maioria das IFES pesquisadas (48%) foram classificadas no nível de maturidade 0, ou seja, estas instituições não realizam a maioria dos controles relacionados a definição de papéis e responsabilidades pela segurança da informação, segregação de funções, contato com autoridades, entre outros controles definidos na seção 6 da norma 27002, conforme Gráfico 8.

Gráfico 8. Maturidade Organização da Segurança da Informação



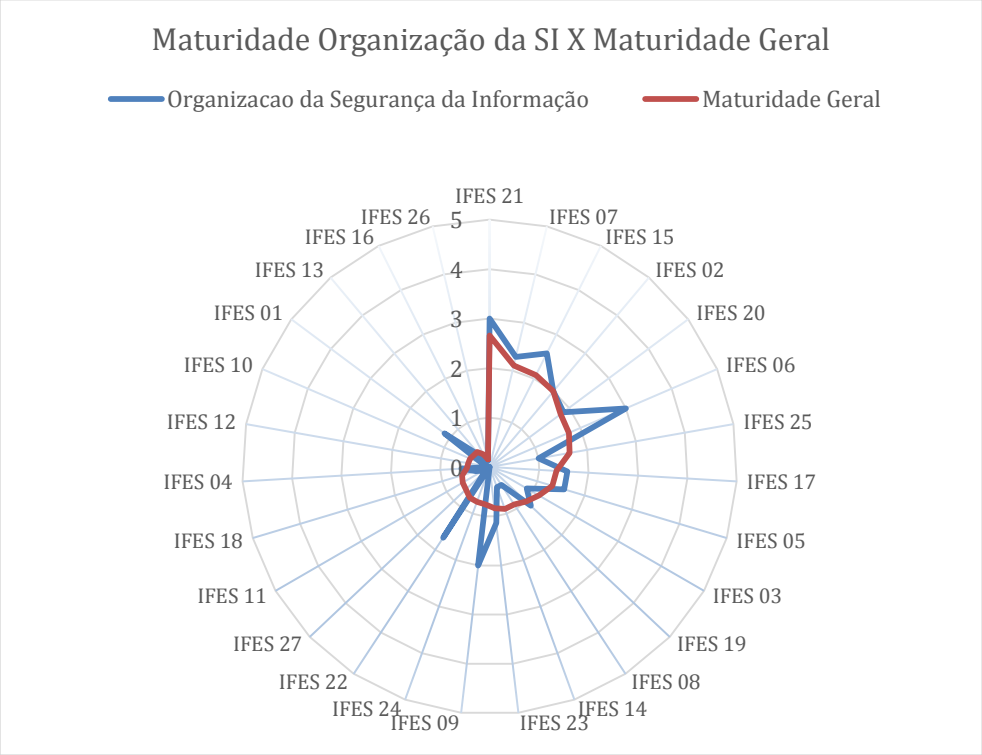
Cerca de 30% das IFES foram identificadas no nível de maturidade 1, ou seja, estas instituições realizam os controles de segurança da referida seção de forma aleatória e sem planejamento, registro ou documentação. No nível de maturidade 2, os controles são planejados e gerenciados, todos os procedimentos executados são verificados com relação ao seu desempenho. Neste nível foram identificadas 15% das IFES. No nível de maturidade 3, 7% das IFES foram identificadas. Neste nível, os processos relacionados aos controles são executados de acordo com um planejamento já definido, gerenciado e aprovado pela organização. Nenhuma das IFES pesquisadas foram identificadas nos níveis de maturidade 4 e 5.

Dentre os controles da seção Organização da Segurança da Informação (OSI) da ISO/IEC 27002, pode-se destacar a definição de papéis de responsabilidade. Torres et al. (2010), afirma

que os papéis de responsabilidade pela segurança da informação de funcionários, fornecedores e terceiros envolvidos devem ser documentados e que esta responsabilidade deve ser estabelecida antes mesmo da contratação. A norma ABNT NBR ISO/IEC 27002, afirma que a segregação de funções é um método para reduzir o risco do mau uso, acidental ou deliberado, dos ativos de uma organização (ABNT, 2013).

O Gráfico 9 compara os níveis de maturidade alcançados no domínio Organização da Segurança da Informação (OSI) com a Maturidade Geral obtida pelos IFES participantes da pesquisa.

Gráfico 9. Comparativo Maturidade Organização da SI X Maturidade Geral



O que se observou foi que mais de 50% das IFES (14) obtiveram o nível de maturidade no domínio OSI acima ou igual a maturidade geral. Isto quer dizer que, quando comparado com as outras áreas avaliadas, este domínio está com o nível mais elevado. Entretanto, isso não garante que seja o nível ideal. Essa definição do nível adequado de maturidade dos processos de segurança da informação deve ser feita pela própria instituição, ou empresa de consultoria especializada. As IFES que obtiveram o maior nível de maturidade neste domínio (3,0) foram as IFES 21 e 06, e as que obtiveram os menores (0,0) foram as IFES 12 e 24.

Um dos fatores de sucesso para a GSI de qualquer organização é uma definição clara dos papéis e responsabilidades relacionadas à segurança da informação. As responsabilidades pela proteção de cada ativo, pela execução dos processos de segurança e pelas atividades de gerenciamento dos riscos devem ser devidamente definidas (ABNT, 2013b). Esta definição visa garantir que os processos e atividades relacionadas à segurança da informação estão sendo executadas corretamente.

4.2.4 Segurança em Recursos Humanos

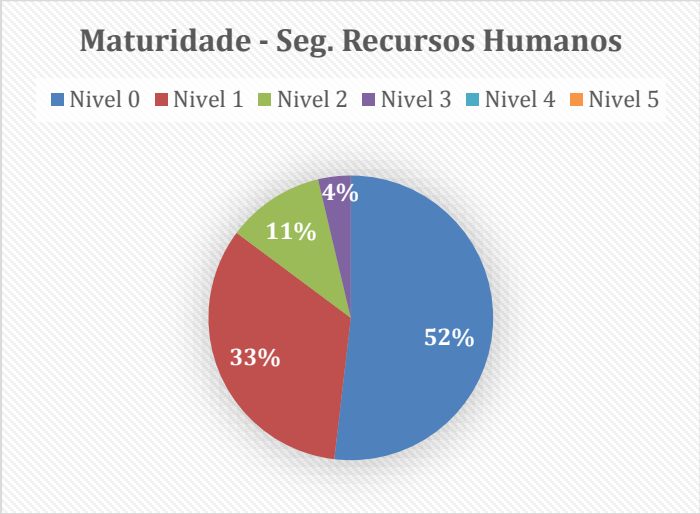
Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 7 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. De acordo Coelho et al. (2014a) e ABNT (2013b) a referida seção trata dos controles de segurança da informação durante o ciclo de vida da prestação de serviços pelos profissionais na organização. Essa seção está dividida em três categorias:

- Antes da contratação – assegura que os funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais foram estabelecidos.
- Durante a contratação – garante que os funcionários e partes externas estejam conscientes e cumpram as suas responsabilidades pela segurança da informação, através de capacitações em segurança da informação e aplicação de processo disciplinar em caso de violação das políticas de segurança da informação.
- Encerramento e mudança da contratação – garante a proteção dos interesses da organização como parte do processo de mudança ou enceramento de contrato, através de atividades como devolução de ativos e alteração ou remoção de direitos de acesso.

Quando avaliadas (questões 14 a 18) a respeito dos controles da seção 7, o Gráfico 10 demonstra mais uma vez que a maioria das IFES pesquisadas (52%) estão no nível mais baixo de maturidade, seguidas respectivamente pelos níveis 1, 2 e 3. Nenhuma das instituições pesquisadas alcançaram os níveis de maturidade 4 e 5. Este cenário deixa evidente que, na maioria das IFES

pesquisadas, os procedimentos para a garantia da segurança da informação não estão sendo devidamente realizados durante o ciclo de vida de prestação de serviços dos funcionários.

Gráfico 10. Maturidade Segurança nos Recursos Humanos



Segundo Disterer (2013) e ABNT (2013), todos os empregados, contratados e terceiros, usuários dos ativos de informação, devem estar cientes das ameaças a segurança, de suas responsabilidades e do apoio as políticas de segurança de sua organização. Grande parte dos incidentes de segurança são causados pela falta de conscientização dos funcionários, levando ao mau uso ou má interpretação da tecnologia ou dos procedimentos (ALSHAIKH et al., 2014).

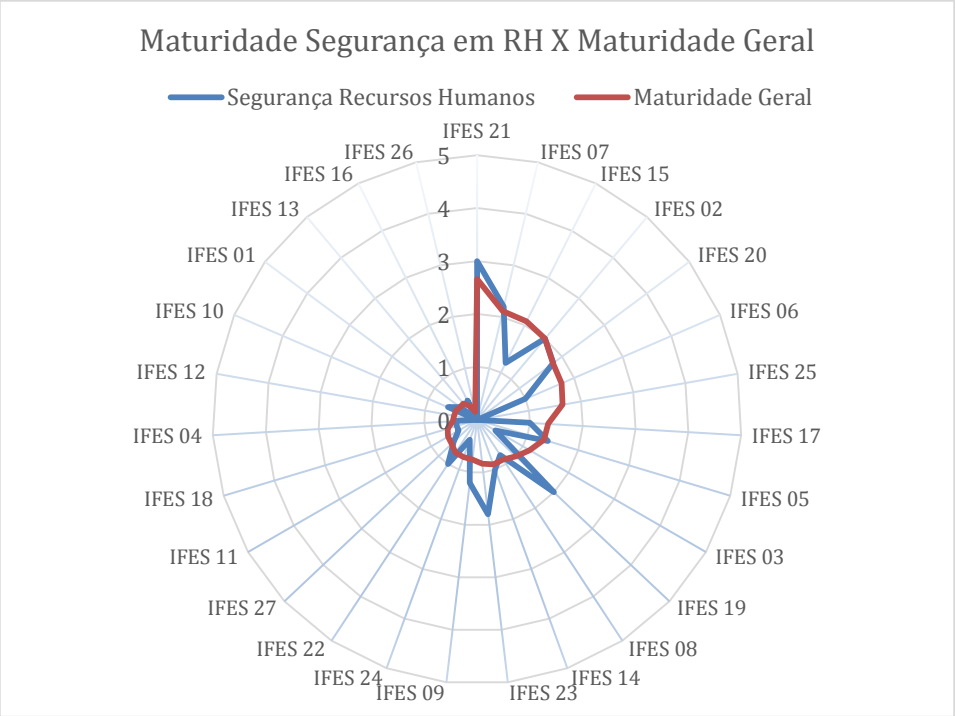
Para que se possa garantir a participação de todos os colaboradores e terceiros nas iniciativas de segurança da informação o Apoio da Alta Gestão torna-se extremamente importante. A norma NBR ISO/IEC 27002 em sua seção 7 traz a seguinte orientação:

> Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização (ABNT, 2013b).

Treinamento e conscientização em segurança da informação é também um dos fatores críticos para o sucesso da gestão da segurança, principalmente em relação ao fator humano. Todos os colaboradores da organização e terceiros devem receber treinamento apropriado com atualizações regulares das políticas e procedimentos organizacionais, específicos a sua função (ABNT, 2013b).

Quando comparados, os níveis de maturidade da Segurança em Recursos Humanos (SRH) com a maturidade Geral, obtidos pelas IFES respondentes, o que se pode verificar é que grande parte dessas instituições (14) estão com o nível de maturidade em SRH abaixo do seu nível de maturidade geral, conforme Gráfico 11.

Gráfico 11. Comparativo Maturidade Segurança RH X Maturidade Geral



Este resultado é preocupante, pois os controles de segurança da informação voltados ao fator humano não estão sendo devidamente empregados. A IFES 21 obteve o maior nível de maturidade neste domínio (3), enquanto que as IFES com menor nível de maturidade (0) foram as IFES 12, 13, 25 e 26.

TU (2015), em sua tese de doutorado "*Effective Information Security Management: A Critical Success Factors Analysis",* afirma que os fatores humanos podem ser mais importantes do que os controles de segurança para o sucesso da GSI de uma organização. Entretanto se os processos de gestão segurança da informação voltados aos recursos humanos das IFES não estiverem bem definidos, controlados e não forem constantemente avaliados e melhorados este sucesso não pode ser alcançado.

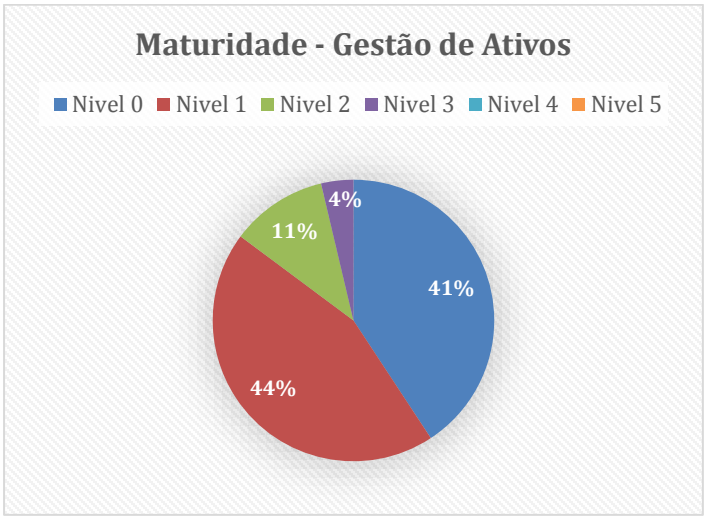
4.2.5 Gestão de Ativos

Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 8 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Esta seção trata dos controles de segurança da informação relacionados aos ativos da organização. Ela está dividida em três categorias (ABNT, 2013b; COELHO et al., 2014a):

- Responsabilidade pelos ativos – apresenta os controles que estão relacionados com a proteção dos ativos da organização e de definição das reponsabilidades.
- Classificação das informações – define os controles para a classificação da informação, atribuindo a elas um nível de segurança de acordo com sua importância para a organização.
- Tratamento de mídias – define os controles adequados para o gerenciamento das diversas mídias, relacionando-os com o esquema de classificação adotado.

Quando avaliadas (questões 19 e 20) quanto aos controles da seção 8, o Gráfico 12 demonstra que a maior parcela das IFES pesquisadas (44%) está no nível de maturidade 1. Neste nível, os processos de GSI voltados a gestão dos ativos da instituição são realizados de maneira informal, ou seja, não há um planejamento ou documentação dos procedimentos realizados, eles são realizados de forma reativa e são dependentes de habilidades e conhecimentos individuais.

Gráfico 12. Maturidade Gestão de Ativos



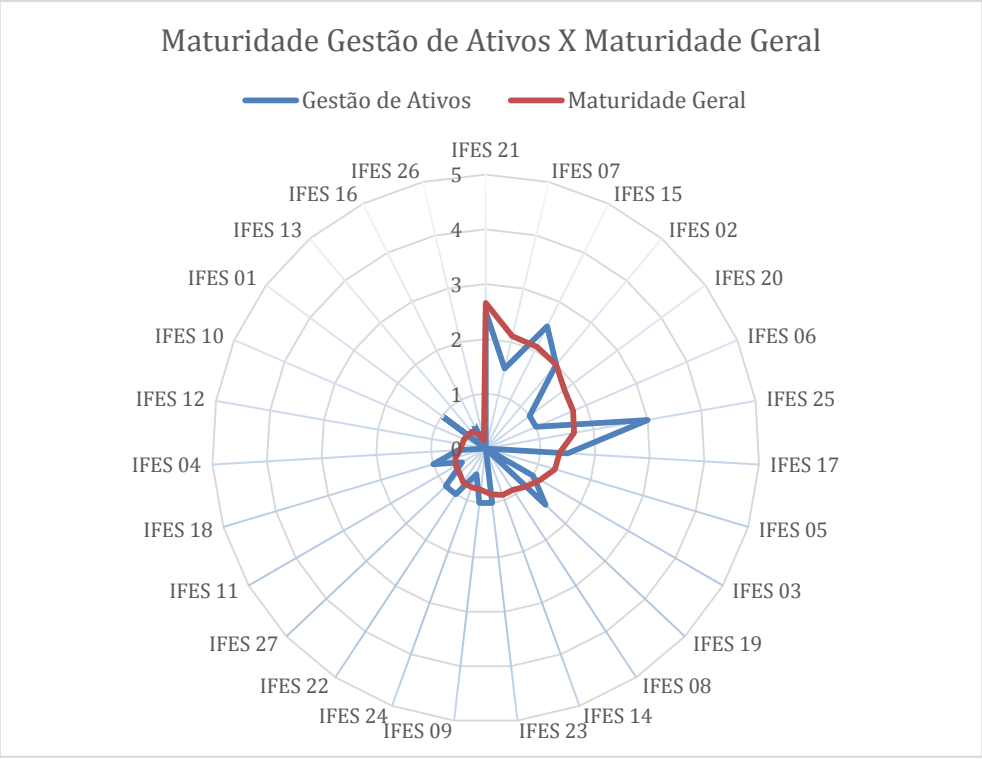
A segunda maior parcela de IFES identificadas na pesquisa (41%) está no nível de maturidade 0, seguidos de 11% no nível 2 e 4% no nível 3. Nenhuma das IFES pesquisadas foram identificadas nos níveis de maturidade 4 ou 5. Pode-se concluir que, no domínio Gestão de Ativos, cerca de 85% das instituições pesquisadas, quando executam os controles de segurança voltados a proteção dos ativos, são desestruturados e informais, sem documentação ou planejamento.

Torres (2010), afirma que a informação, os processos de apoio, os sistemas e as redes de dados são ativos essenciais as organizações, sejam elas públicas ou privadas. A norma 27002 em sua seção 8, deixa claro os objetivos: (i) "Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos"; (ii) "Assegurar que a informação receba um nível adequado de proteção, de acordo com a sua importância para a organização"; (iii) "Prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias" (ABNT, 2013). Entretanto, o baixo índice de maturidade apresentado indica que esses objetivos não estão sendo realizados adequadamente.

Para que se possa garantir a proteção adequada aos ativos de informação, estes devem ser devidamente identificados, bem como seus proprietários. Dessa forma, é possível atribuir a esses proprietários a responsabilidade pela manutenção da segurança desses ativos (TORRES, 2010). O mesmo autor afirma que para reduzir o risco de furto, fraude e mau uso dos ativos, os papéis e responsabilidades de segurança da informação de todos os colaboradores (internos ou externos) devem ser documentados de acordo com as políticas estabelecidas.

O Gráfico 13 representa a situação da maturidade no domínio Gestão de Ativos em comparação a maturidade geral obtidas pelas IFES participantes da pesquisa. O que se percebe é que 52% das instituições foram identificadas com nível de maturidade, no domínio Gestão de Ativos, abaixo do seu nível de maturidade geral, o restante das instituições (48%) obteve níveis acima ou iguais. Este resultado evidencia a criticidade e a necessidade de aprimoramento da maturidade no processo de gestão de ativos das IFES pesquisadas. Entretanto, para que isso seja possível é necessário que todos processos sejam estruturados e documentados, monitorados e melhorados de forma iterativa. As IFES 05, 08, 10, 12, 13, 14 e 26 ficaram no nível de maturidade 0 neste domínio. Apenas a IFES 25 obteve a maturidade 3.

Gráfico 13. Comparativo Maturidade Gestão de Ativos X Maturidade Geral



Alexandria e Quoniam (2010), afirma que quando as medidas de segurança em vigor são insuficientes para dar a proteção necessária que a instituição precisa é necessário que se tenha uma postura mais planejada e estruturada, a fim de assegurar que os ativos de informação, que dão suporte as atividades críticas, não venham a comprometer seus objetivos e sua imagem diante de seus parceiros e sociedade.

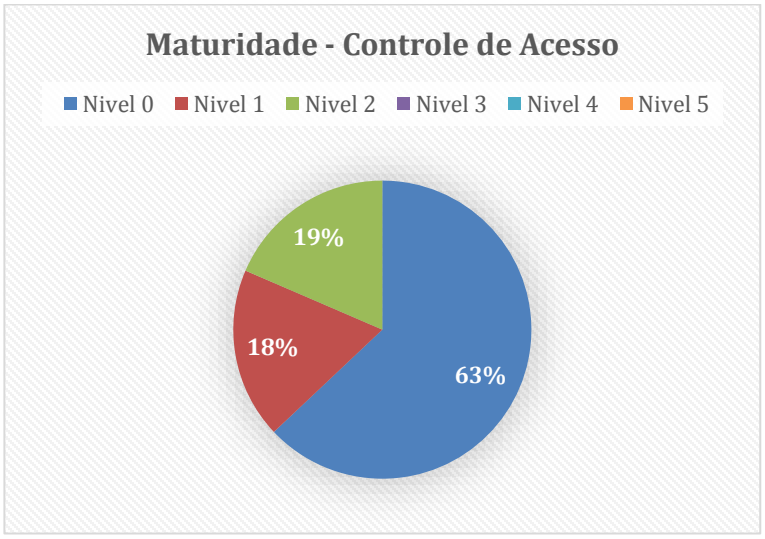
4.2.6 Controle de Acesso

Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 9 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. A referida seção trata dos controles de acesso lógico, diferente da seção “Segurança física e do ambiente”, e nela são considerados os aspectos relacionados a privilégios de acesso, acesso a rede, senhas e outros controles, divididos em quatro categorias (ABNT, 2013b; COELHO et al., 2014a):

- Requisitos do negócio para controle de acesso – define os controles de forma a limitar o acesso à informação e aos recursos computacionais.
- Gerenciamento de acesso do usuário – assegura acesso ao usuário autorizado e previne o acesso não autorizado a sistemas e serviços.
- Responsabilidade dos usuários – torna os usuários responsáveis pela proteção das informações sob sua responsabilidade, a exemplo as informações de autenticação.
- Controle de acesso ao sistema e à aplicação – Previne o acesso não autorizados aos sistemas e aplicações.

Quando questionadas (questões 21 a 35) a respeito dos controles da seção 9, o Gráfico 14 demonstra que 63% das IFES pesquisadas foram identificadas no nível de maturidade 0 (Não Realiza), 18% foram identificadas no nível 1 (Realiza Informalmente) e 19% no nível 2 (Planejado).

Gráfico 14. Maturidade Controle de Acesso

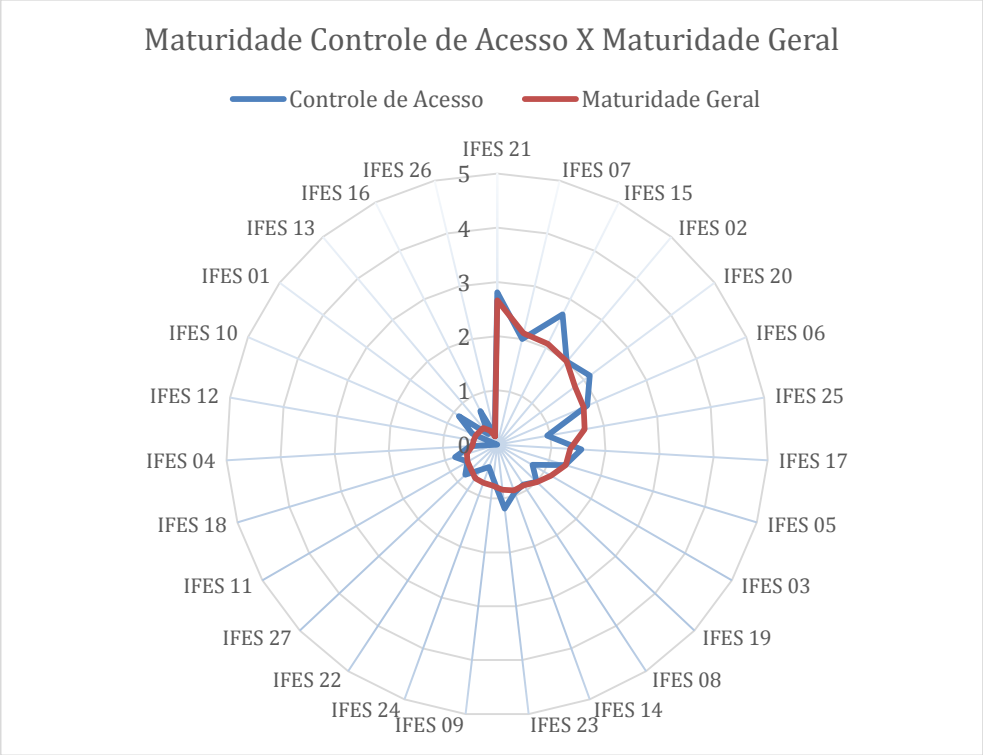


Esse resultado deixa evidente que o princípio da confidencialidade pode ser afetado, pois nenhumas das instituições pesquisadas foram identificadas nos níveis de maturidade 3 (Bem Definido), 4 (Controlado) ou 5 (Melhoria Contínua). De acordo com Paranhos (2010), as regras de controle de acesso devem levar em consideração as políticas para autorização e disseminação da informação. O mesmo autor afirma que um controle de acesso efetivo impossibilita que

pessoas não autorizadas tenham acesso as informações institucionais e gerem prejuízos que afetem a integridade ou a disponibilidade do ativo ou da informação.

Um comparativo entre a maturidade no domínio Controle de Acesso e a maturidade geral, obtidas pelas instituições pesquisadas, revelou que os controles da referida seção estão bem parelhos a maturidade geral, conforme Gráfico 15. Contudo, isso não significa que os procedimentos de controle de acesso estejam sendo bem empregados nas instituições, mas que comparando com as outras áreas esta não está com a maturidade tão baixa. A instituição com maior nível de maturidade neste domínio foi a IFES 21 com maturidade média de 2,81. Já àquela com menor nível foi a IFES 12 com maturidade 0.

Gráfico 15. Comparativo Maturidade Controle de Acesso X Maturidade Geral



Torres et al. (2010), em seu artigo “A Gestão da Segurança da Informação e Seu Alinhamento Estratégico na Organização”, afirma que o acesso a informação, seus recursos de processamento e os processos críticos de negócio devem ser controlados e criteriosamente autorizados para uso. Dessa forma, percebe-se a necessidade de melhoria dos processos relacionados ao controle de acesso das IFES e consequentemente o aprimoramento da maturidade de GSI.

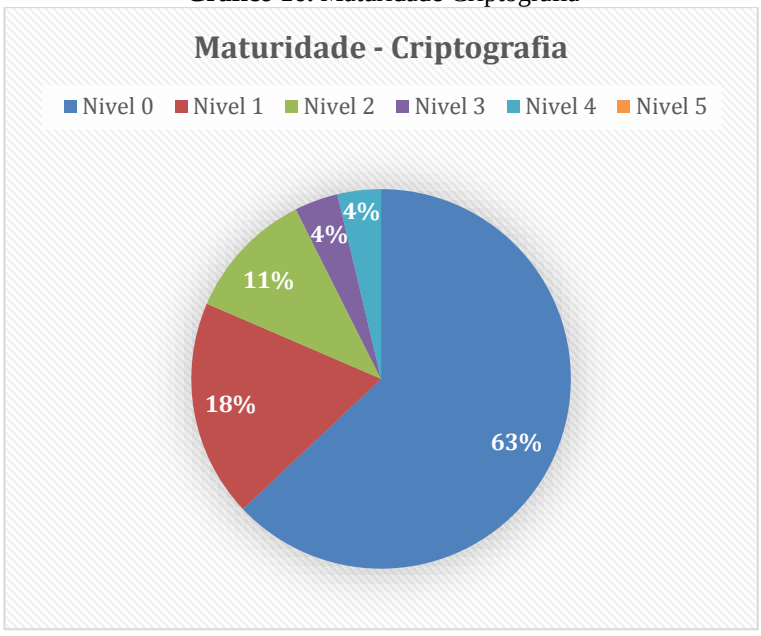
4.2.7 Criptografia

Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 10 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Esta seção trata dos controles relacionados ao uso da criptografia no uso dos sistemas e serviços de TI. A referida seção possui a seguinte categoria (ABNT, 2013b; COELHO et al., 2014a):

- Controles criptográficos – assegura o uso da criptografia de forma efetiva para garantia da confidencialidade, autenticidade e integridade da informação.

As questões 36 a 38, buscaram identificar o nível de maturidade das IFES pesquisadas quanto ao uso da criptografia. No Gráfico 16 é possível verificar que a situação das IFES neste domínio não é diferente das seções anteriores analisadas nesta pesquisa, pois a maioria das instituições pesquisadas, totalizando 81%, foram identificadas nos níveis mais baixos de maturidade (0 Não realiza e 1 Realiza informalmente).

Gráfico 16. Maturidade Criptografia

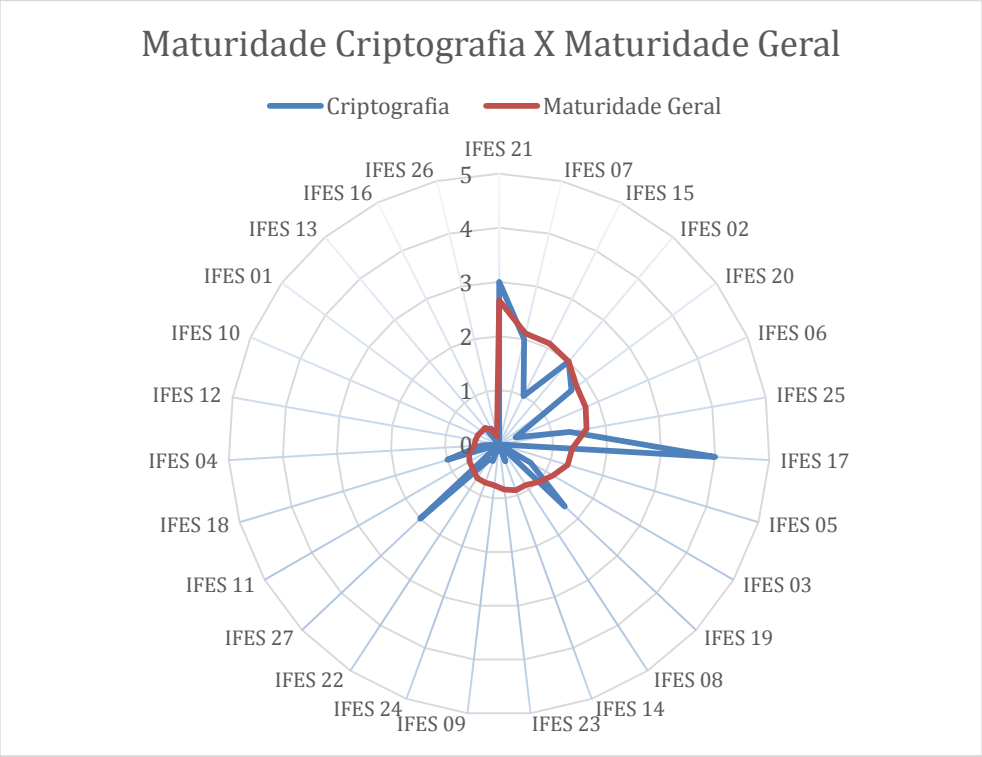


Cerca de 11% das instituições foram identificadas no nível de maturidade 2 (Planejado), 4% foram no nível 3 (Bem Definido) e 4% no nível 4 (Controlado). Nenhuma instituição foi identificada no nível 5 (Melhoria Contínua). Esse resultado evidencia que os procedimentos para uso de criptografia não estão sendo realizados na grande maioria das IFES.

De acordo com Sêmola (2013), a criptografia é a uma ciência que estuda os princípios, meios e métodos para proteger a confidencialidade das informações através da codificação ou processo de cifração. O uso de uma solução de criptografia deve fazer parte de um processo mais amplo de avaliação de riscos e seleção de controles. Essa avaliação pode ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle convém ser aplicado e para qual proposito e processos de negócio (ABNT, 2013).

A maior parcela das instituições pesquisadas ficou com o nível de maturidade no domínio criptografia bem abaixo do seu nível de maturidade geral, quando comparados através do Gráfico 17. Este resultado evidencia e confirma a carência em que estas instituições estão quanto aos procedimentos de controles criptográficos. Algumas IFES obtiveram bons níveis de maturidade neste domínio, como a IFES 17 e 21, com os níveis 4 e 3 respectivamente. Contudo a maior parcela ficou no nível 0.

Gráfico 17. Comparativo Maturidade Criptografia X Maturidade Geral



Segundo Silva (2009), um dos requisitos para se obter um ambiente informacional seguro é através do uso da criptografia e a assinatura digital. Essa mesma autora afirma que a

criptografia é usada como mecanismo de apoio ao controle de acesso para reforçar o sigilo de informações.

Um dos documentos que orientam sobre o uso de recursos criptográficos para segurança da informação é a Norma Complementar 09/IN01/DSIC/GSIPR, tem como objetivo normatizar o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da Administração Pública Federal, direta e indireta (BRASIL, 2014).

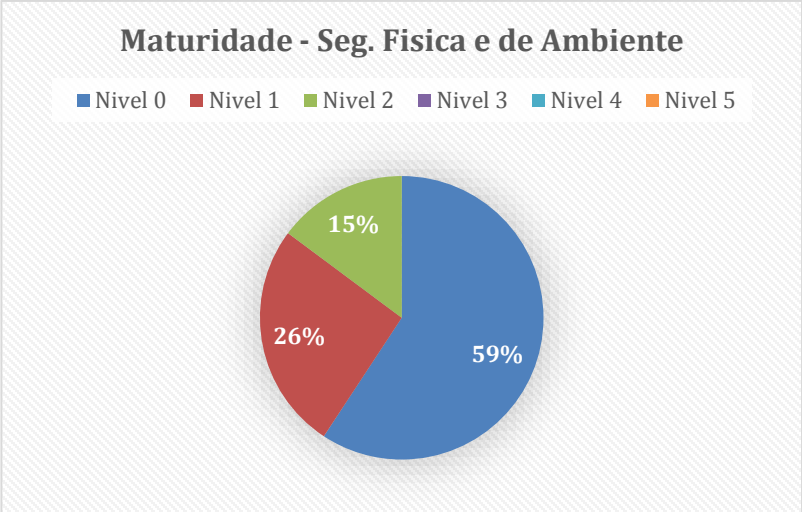
4.2.8 Segurança Física e de Ambiente

Esta seção tem por objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 11 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Como o próprio nome já diz, trata dos objetivos e controles relacionados aos critérios de segurança física dos ativos e do ambiente onde estes estão dispostos. Esta seção está dividida em duas categorias (ABNT, 2013b; COELHO et al., 2014a):

- Áreas seguras – trata dos critérios de segurança de acesso físico às instalações da organização. Os controles mais comuns nessa categoria vão desde segurança de perímetro, áreas internas e externas, áreas seguras, de acesso público a áreas de entrega de materiais.
- Equipamentos – trata dos critérios de segurança voltados para a proteção física dos ativos e de sua disponibilidade. Esta categoria possui controles para instalação de equipamentos, parte elétrica, refrigeração do ambiente, manutenção, reutilização e alienação dos ativos.

Após a coleta dos dados referentes a identificação de maturidade dos controles da seção 11 da norma 27002, o Gráfico 18 pode ser desenvolvido. Neste domínio, foi verificado que 59% das IFES pesquisadas estão no nível de maturidade 0. Estas instituições não possuem, ou são insuficientes, os procedimentos que tratam do controle de acesso físico aos ambientes que mantem os recursos de processamento das informações.

Gráfico 18. Maturidade Segurança Física e de Ambiente



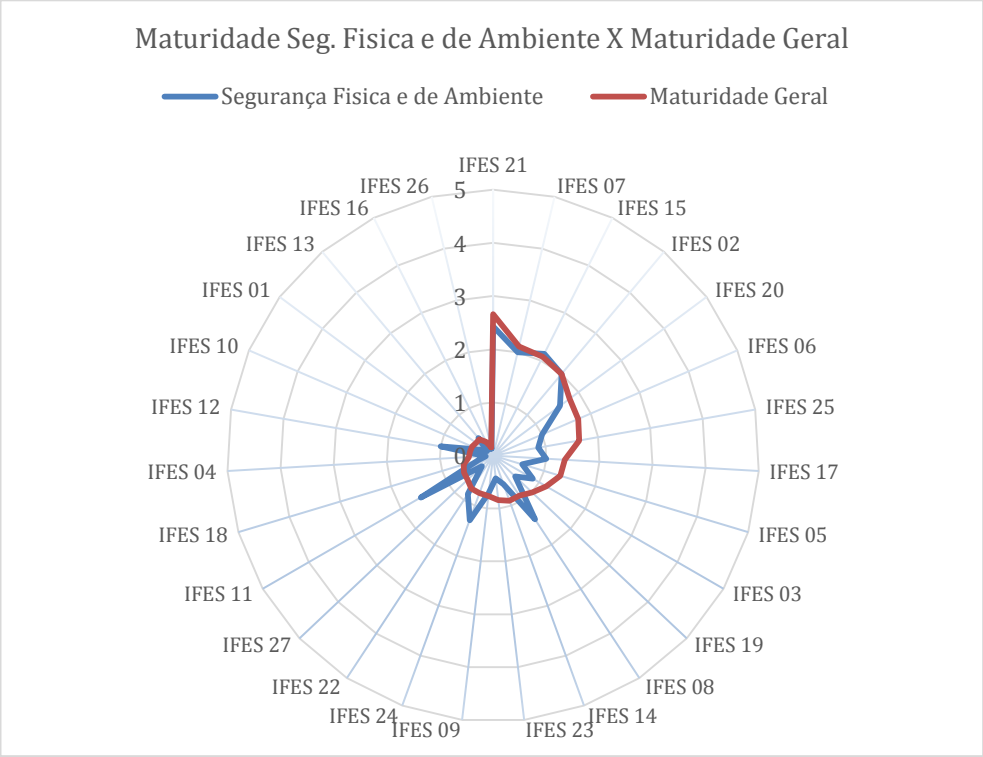
Verificou-se também que 26% das IFES foram identificadas no nível de maturidade 1 (Realiza informalmente). Neste nível os procedimentos de controles de acesso físico e demais controles da seção 11, são geralmente executados e dependem do conhecimento individual de um ou outro colaborador, não há documentação e padronização do processo. No nível de maturidade 2 (Planejado), 15% das IFES foram identificadas. Neste nível os processos de segurança aplicados aos controles de acesso físico e ambientais são planejados e gerenciados. Já é possível avaliar o desempenho e resultado dos processos. Nos níveis de maturidade 3, 4 e 5 não foram identificadas nenhuma das IFES pesquisadas.

Os controles de segurança física e ambiental são responsáveis por evitar perdas, danos, furto ou roubo, ou o comprometimento de ativos e interrupção das operações da organização (ABNT, 2013). De acordo com Torres et al. (2010), o acesso físico controlado aos ativos computacionais previne danos e interferências nas informações institucionais. Os mesmos autores ainda afirmam que os equipamentos que processam as informações devem ser mantidos em áreas seguras, com delimitação de perímetro e controle de acesso. Entretanto, os resultados apontados no Gráfico 18 apresentam um resultado preocupante no domínio segurança física e de ambiente.

Um comparativo entre a maturidade no domínio Segurança Física e de Ambiente (SFA) e a maturidade geral, obtidas pelas instituições respondentes, revelou que os níveis de maturidade no domínio SFA estão bem abaixo da maturidade geral, conforme Gráfico 19. Com isso, é possível constatar que os controles desse domínio não estão sendo empregados adequadamente

nas IFES. Como exemplo observa-se a IFES 25 com a maturidade no domínio Segurança Física e de Ambiente de 0,86 e a maturidade geral com 1,64.

Gráfico 19. Comparativo Maturidade Segurança Física e de Amb. X Maturidade Geral



Alexandria e Quoniam (2010), afirma que além da segurança lógica uma boa infraestrutura física do ambiente que abriga os sistemas de informações da organização, condições adequadas de temperatura e umidade, fornecimento ininterrupto de energia, uma rede confiável de dados, entre outros fatores, também é responsável por uma boa gestão da segurança da informação. Ou seja, a segurança da informação deve ser pensada em todos os aspectos, não somente o lógico (sistemas), mas também o físico e o humano.

4.2.9 Segurança nas Operações

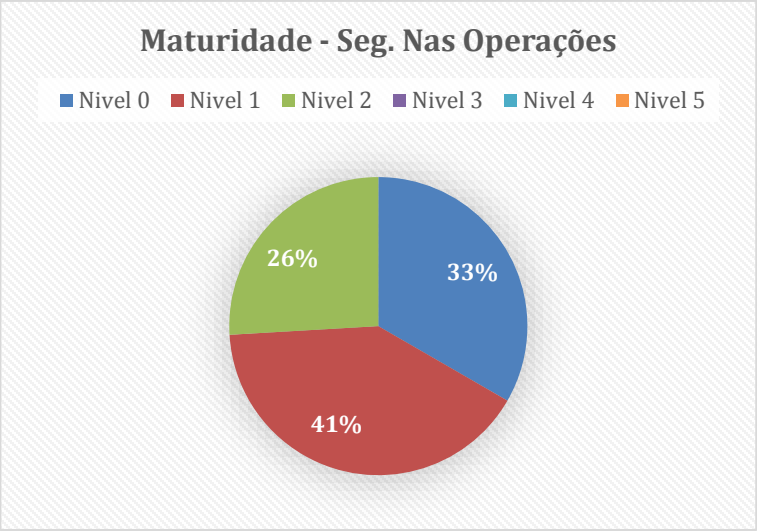
A presente seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 12 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Esta seção trata dos critérios de segurança da informação voltados às operações diárias dos serviços de TI, buscando atender a maioria das vulnerabilidades relacionadas aos aspectos

operacionais. Esta seção possui sete categorias de controle (ABNT, 2013b; COELHO et al., 2014a):

- Responsabilidades e procedimentos operacionais – trata dos controles que buscam garantir a operação segura e correta dos recursos de processamento da informação.
- Proteção contra códigos maliciosos – assegura que as informações e os recursos computacionais estão devidamente protegido, mantendo um nível de segurança adequado.
- Cópias de segurança – trata da proteção contra a perda acidental ou intencional dos dados, garantindo assim uma cópia de segurança para eventual recuperação dos dados.
- Registros e monitoramento – trata do monitoramento e registro das atividades realizadas nos sistemas computacionais, gerando evidencias para eventuais auditorias.
- Controle de software operacional – trata dos procedimentos para controle da instalação de softwares, com o objetivo de manter a integridade e disponibilidade dos sistemas operacionais.
- Gestão de vulnerabilidades técnicas – trata dos procedimentos para prevenção da exploração das vulnerabilidades técnicas.
- Considerações quanto à auditoria de sistema de informação – tem como objetivo minimizar o impacto das atividades de auditoria nos sistemas operacionais.

Quando questionadas (questões 45 a 64) a respeito dos controles da referida seção, é possível constatar, por meio do Gráfico 20, que uma maior parcela das IFES pesquisadas (41%) executa os procedimentos mínimos de segurança durante suas atividades operacionais, colocando-as no nível de maturidade 1 (Realiza Informalmente). Estas instituições possuem um consenso de que a segurança da informação deve ser considerada durante a realização das atividades, porém não são estruturadas ou documentadas.

Gráfico 20. Maturidade Segurança nas Operações

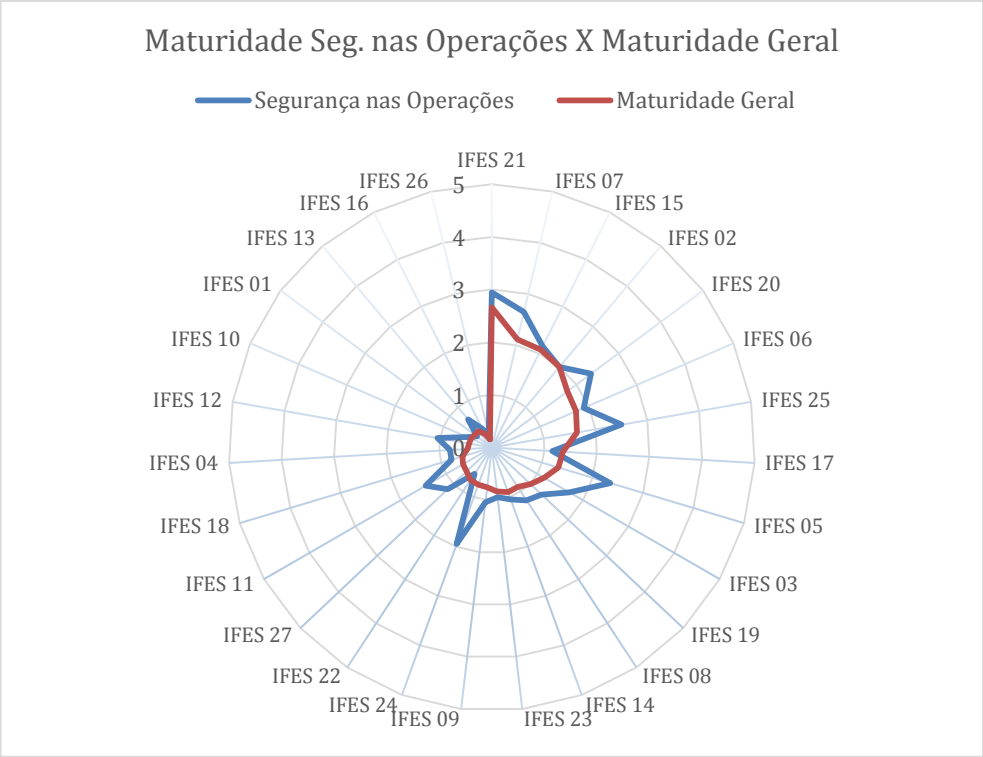


Cerca de 33% das IFES pesquisadas foram identificadas no nível de maturidade 0. Estas instituições não realizam os controles de segurança da informação ou eles são insuficientes para garantir a segurança nas atividades operacionais. No nível de maturidade 2 foram identificadas 26% das IFES pesquisadas. Estas possuem os processos de segurança planejados e documentados. O desempenho destes processos pode ser avaliado e medido. Nenhuma das IFES pesquisadas foram identificadas nos níveis de maturidade 3, 4 ou 5. Este é mais um resultado preocupante constatado nesta pesquisa.

Todos os procedimentos operacionais devem ser documentados e disponibilizados aos usuários que necessitem deles. Umas das causas mais comuns de falhas de segurança, é a operacionalização incorreta ou desconhecimento por parte dos usuários no uso dos sistemas (ABNT, 2013).

Quando comparados os resultados da análise de maturidade no domínio Segurança nas Operações com a maturidade geral, percebeu-se um certo avanço em relação as outras, pois poucas áreas tiveram sua maturidade acima da maturidade geral, conforme Gráfico 21. Tomando como exemplo a IFES 05 que obteve a maturidade de 2,35 neste domínio e 1,32 na maturidade geral. Esse resultado indica que essa área está evoluindo mais do que outras, estando abaixo apenas da Politica de Segurança. Contudo, o fato de nenhuma das instituições pesquisadas terem sido identificadas nos níveis de maturidade 3, 4 e 5, revelam uma situação preocupante com relação a segurança da informação nas operações.

Gráfico 21. Comparativo Maturidade Segurança nas Operações X Maturidade Geral



Alguns fatores considerados críticos para o sucesso da gestão da segurança da informação como a Cultura da Segurança da Informação e Treinamento e conscientização estão diretamente relacionados a segurança das operações das instituições. Autores como Tu (2015), afirmam que a cultura pode orientar como colaboradores pensam, agem e sentem, e, dessa forma, influencia-los durante as operações da instituição, fazendo com que instintivamente executem suas atividades com segurança. Alexandria e Quoniam (2010), enfatiza que é necessário manter um programa de treinamento contínuo, para que os colaboradores tenham consciência dos riscos a que as informações estão expostas e para que as práticas de segurança sejam internalizadas e produzam os efeitos esperados. Entretanto, para se atingir níveis de maturidade adequados não adianta apenas treinar e conscientizar os funcionários, mas planejar e documentar todos os procedimentos operacionais considerando neste processo os aspectos da segurança da informação.

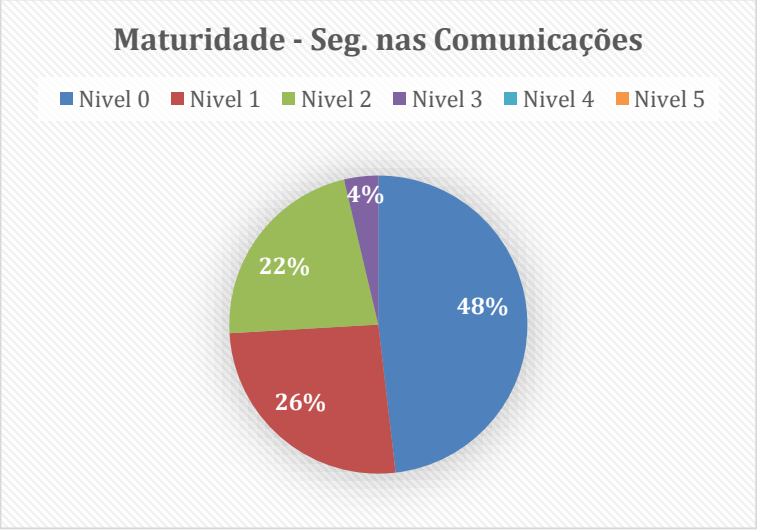
4.2.10 Segurança nas Comunicações

Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 13 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Trata dos controles necessários para a segurança dos equipamentos e dos recursos de redes. Esta seção possui duas categorias (ABNT, 2013b; COELHO et al., 2014a):

- Gerenciamento da segurança em redes – tem como objetivo proteger as informações em tráfego na rede de computadores e os equipamentos que compõem a infraestrutura.
- Transferência de informação – procura manter a segurança na troca de informações internas e externas.

O Gráfico 22 apresenta os resultados acerca da maturidade obtida pelas IFES participantes da pesquisa quanto aos procedimentos de segurança nas comunicações entre os ativos de rede (questões 65 a 70). Observou-se que a maior parcela das IFES pesquisadas (48%), não executam ou são insuficientes os controles de segurança no domínio Segurança nas Comunicações, colocando-as no nível de maturidade 0.

Gráfico 22. Maturidade Segurança nas Comunicações

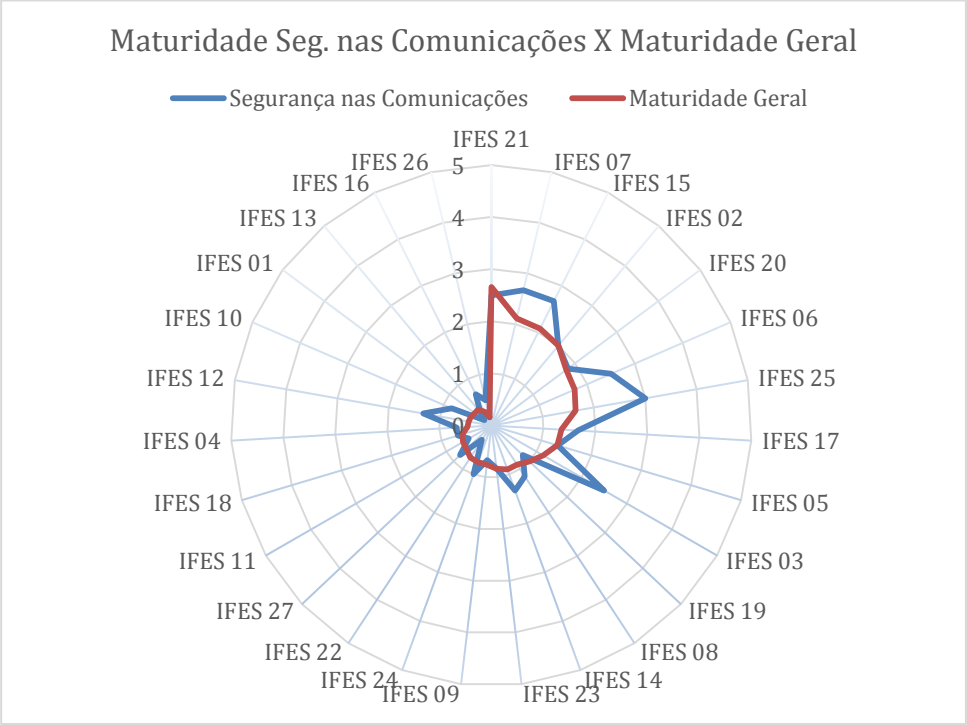


Cerca de 26% das instituições realizam os procedimentos de segurança, porém de maneira informal e desordenada, sem qualquer padronização ou documentação, colocando-as no nível de

maturidade 1. No nível de maturidade 2, 22% das instituições possuem um planejamento e documentação do processo, de modo que este já pode ser corretamente gerenciado. Somente 4% das IFES estão no nível de maturidade 3, onde os processos são bem definidos, utilizando versões aprovadas e adaptadas de processos padrões da instituição. Nenhuma das instituições foi identificada nos níveis de maturidade 4 e 5. A norma 27002, em sua seção 13, afirma que as redes devem ser gerenciadas e controladas, mecanismos de segurança devem ser incluídos em qualquer acordo de serviços de rede (ABNT, 2013).

O Gráfico 23 compara os resultados da análise de maturidade no domínio Segurança nas Comunicações com a maturidade geral. É possível verificar que neste domínio, quando comparado aos outros, obteve-se um nível de maturidade mais elevado, indicando uma evolução sobre as demais áreas. Muitas instituições estão como a IFES 25, com a maturidade no domínio Segurança nas Comunicações (3,0) maior que sua maturidade geral (1,64). Entretanto, a grande parcela de instituições no nível 0 (48%) revela uma situação preocupante neste domínio.

Gráfico 23. Comparativo Maturidade Segurança nas Comunicações X Maturidade Geral



A seção 13 da norma 27002 tem como objetivos: (i) “garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam” e; (ii) “manter a

segurança da informação transferida dentro da organização e com quaisquer entidades externas". Os controles desta seção podem ser realizados em conjunto com a norma ISO/IEC 27033 e suas 6 partes. Paranhos (2010) e Disterer (2013), afirmam que a norma ISO/IEC 27033 é uma norma estritamente técnica, específica para a segurança de rede. Inclusive esta norma é referenciada na ISO/IEC 27002.

4.2.11 Aquisição, Desenvolvimento e Manutenção de Sistemas

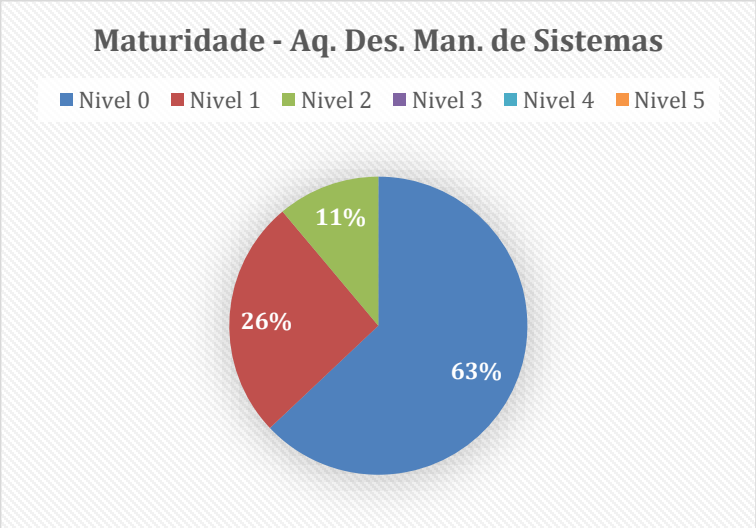
Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 14 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. A referida seção busca o desenvolvimento da segurança da informação nos sistemas da organização, do estabelecimento de critérios de segurança relativos as atividades de aquisição, desenvolvimento e manutenção de softwares. Esta seção possui três categorias de segurança (ABNT, 2013b; COELHO et al., 2014a):

- Requisitos de segurança de sistemas de informação – objetiva garantir que a segurança da informação faça parte de todo o ciclo de vida dos sistemas de informações da organização, incluindo também os requisitos para sistemas de informações que fornecem serviços sobre as redes públicas.
- Segurança em processos de desenvolvimento e de suporte – trata dos critérios relacionados a segurança nos processos de desenvolvimento e suporte dos sistemas.
- Dados para teste – trata dos critérios de segurança para os dados usados em teste.

Quando avaliadas (questões 71 a 84) a respeito dos controles de segurança da informação nos processos de aquisição, desenvolvimento e manutenção de sistemas, o Gráfico 24 apresenta o resultado da maturidade da GSI das IFES pesquisadas. Percebe-se que a maior parcela das instituições foi identificada no nível de maturidade 0 (63%), ou seja, estas instituições não realizam ou realizam parcialmente os procedimentos de segurança da informação dos processos que integram o ciclo de vida dos sistemas de informações (incluindo também sistemas fornecidos por terceiros). Cerca de 26% das IFES possuem um consenso sobre a necessidade da segurança

da informação nos processos de aquisição, desenvolvimento e manutenção dos sistemas, porém os procedimentos são realizados aleatoriamente, há pouca ou nenhuma documentação e os processos não são gerenciados e monitorados, estas instituições estão no nível de maturidade 1.

Gráfico 24. Maturidade Aquisição, Desenvolvimento e Manutenção de Sistemas



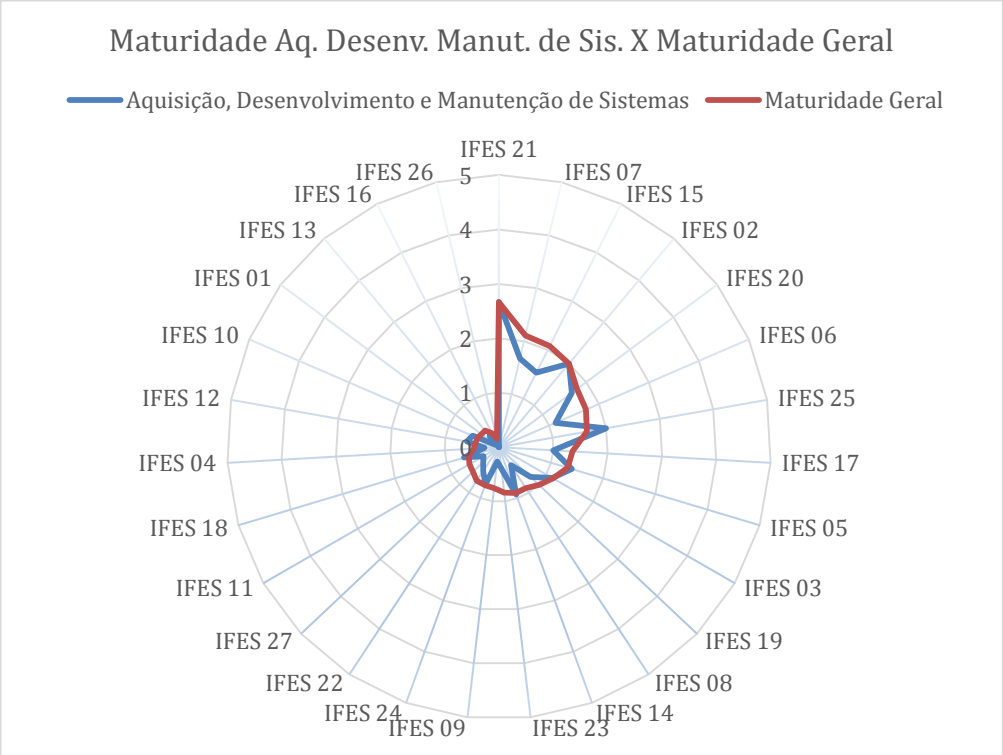
Apenas 11% das instituições pesquisadas foram identificadas no nível de maturidade 2. Nestas instituições já existe um planejamento com relação aos procedimentos de segurança da informação nos processos que envolvem os sistemas de informações. Estes processos são gerenciados e documentados pela equipe responsável.

Nos níveis de maturidade 3, 4 e 5 não foram identificadas nenhuma das instituições pesquisadas. Este é mais um resultado preocupante, pois isso demonstra que 100% da IFES consultadas na pesquisa, ainda não possuem seus processos Bem Definidos, Controlados ou em Melhoria Contínua.

De acordo com Torres (2010), proteger a integridade dos sistemas de software e da informação por ele manipulados também deve fazer parte da política de gestão de segurança da informação, o acesso aos códigos-fonte dos sistemas de informação deve ser estritamente controlado e restrito apenas à equipe de desenvolvimento a fim de que sejam evitadas mudanças não autorizadas. Os riscos de segurança também são causados por vulnerabilidades dos sistemas de informação, logo estas devem ser devidamente tratadas (DISTERER, 2013).

Um comparativo entre a maturidade no domínio Aquisição, Desenvolvimento e Manutenção de Sistemas (ADMS) e a maturidade geral, obtidas pelas instituições respondentes, revelou que os níveis de maturidade neste domínio estão bem abaixo da maturidade geral, conforme Gráfico 25. Uma grande parcela das instituições está como a IFES 06, com a maturidade no domínio ADMS (1,13) abaixo de sua maturidade geral (1,74). Com este resultado, somado a parcela de 63% das instituições identificadas no nível de maturidade 0, é possível constatar que os controles da referida seção não estão sendo empregados adequadamente nas IFES.

Gráfico 25. Comparativo Maturidade Aq., Desen. e Manut. de Sis. X Maturidade Geral



A experiência tem mostrado que no processo de desenvolvimento de software, os desenvolvedores buscam garantir a entrega de um produto funcional e sem falhas, entretanto não se preocupam tanto com a questão da segurança. Diversas normas e modelos estão disponíveis com boas práticas para o desenvolvimento de software seguro, dentre elas pode-se destacar a Norma Complementar nº 16/IN01/DSIC/GSIPR, estabelece diretrizes de segurança da informação e comunicações para a obtenção de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta (BRASIL, 2012). Outra norma que se destaca é a

ISO/IEC 15408 (2005, apud NUNES e BELCHIOR, 2006), que afirma que o desenvolvimento seguro de software envolve a segurança tanto do ambiente de desenvolvimento quanto do produto final desenvolvido. Nunes e Belchior (2006), ainda explicam que a necessidade de segurança deve ser tratada em todo o ciclo de vida de desenvolvimento de sistemas, passando pela fase de análise de requisitos, especificação funcional, projetos de alto e baixo nível, implementação final e seu ambiente de produção.

4.2.12 Relacionamento com Fornecedores

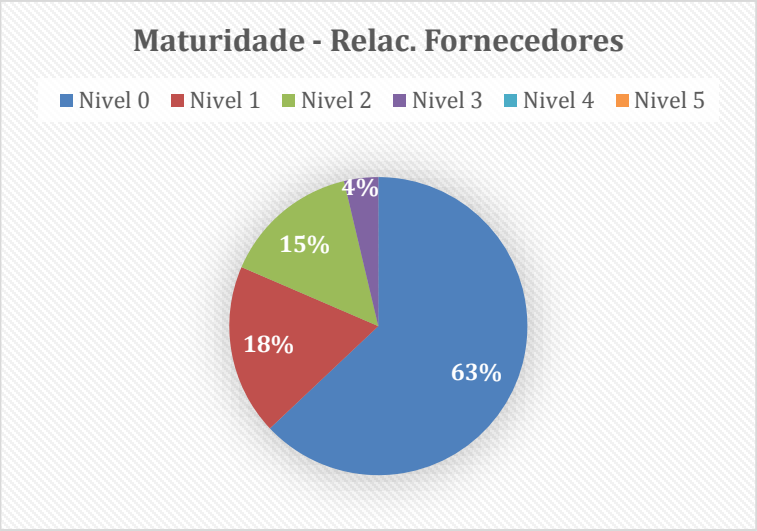
Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 15 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. A referida seção trata dos procedimentos de segurança da informação nos relacionamentos com os fornecedores. Esta seção possui duas categorias (ABNT, 2013b; COELHO et al., 2014a):

- Segurança da informação na cadeia de suprimento – objetiva a proteção da informação e dos ativos acessados por fornecedores.
- Gerenciamento de entrega do serviço do fornecedor – tem como objetivo manter o nível de segurança e de entrega de serviços dos fornecedores da forma como foi acordado.

Norman e Yasin (2015), afirmam que o uso de sistemas de informação não está mais vinculado somente a organização, mas se espalhou externamente para clientes e fornecedores. Ou seja, todo os processos de gestão de segurança da informação devem ser repensados de modo que incluam todos os participantes envolvidos, tanto internos quanto externos.

Quando questionadas (questões 85 a 90) a respeito dos controles de segurança da informação nos relacionamentos com fornecedores é possível constatar, através do Gráfico 26, que 63% das IFES pesquisadas não realizam os procedimentos controle de segurança da informação, ou estes são insuficientes, nos processos que envolvem fornecedores que tenham algum contato com os ativos de TI da instituição. Estas instituições foram identificadas no nível de maturidade 1.

Gráfico 26. Maturidade Relacionamento com Fornecedores



Ainda no Gráfico 26, é possível observar que 18% das instituições realizam os procedimentos de segurança da referida seção, entretanto eles são executados informalmente, sem gerencia ou controle. No nível de maturidade 2 foram identificadas 15% das IFES, que corresponde àquelas que já possuem um planejamento e documentação dos procedimentos de segurança nos processos com fornecedores. No nível de maturidade 3, somente 4% das instituições foram identificadas. Estas possuem seus procedimentos de segurança bem definidos, o que significa que os processos foram planejados, gerenciados e aprovados utilizando um processo padrão de toda a empresa (SSE-CMM, 2003). Nenhuma das IFES pesquisadas foram identificadas nos níveis de maturidade 4 e 5.

O fato de 63% das instituições pesquisadas estarem no nível de maturidade 0 e 18% no nível 1, perfazendo um total de 81%, revela uma situação crítica também no domínio de Segurança no Relacionamento com Fornecedores. A norma ABNT NBR ISO/IEC 27002, em sua seção 15 orienta:

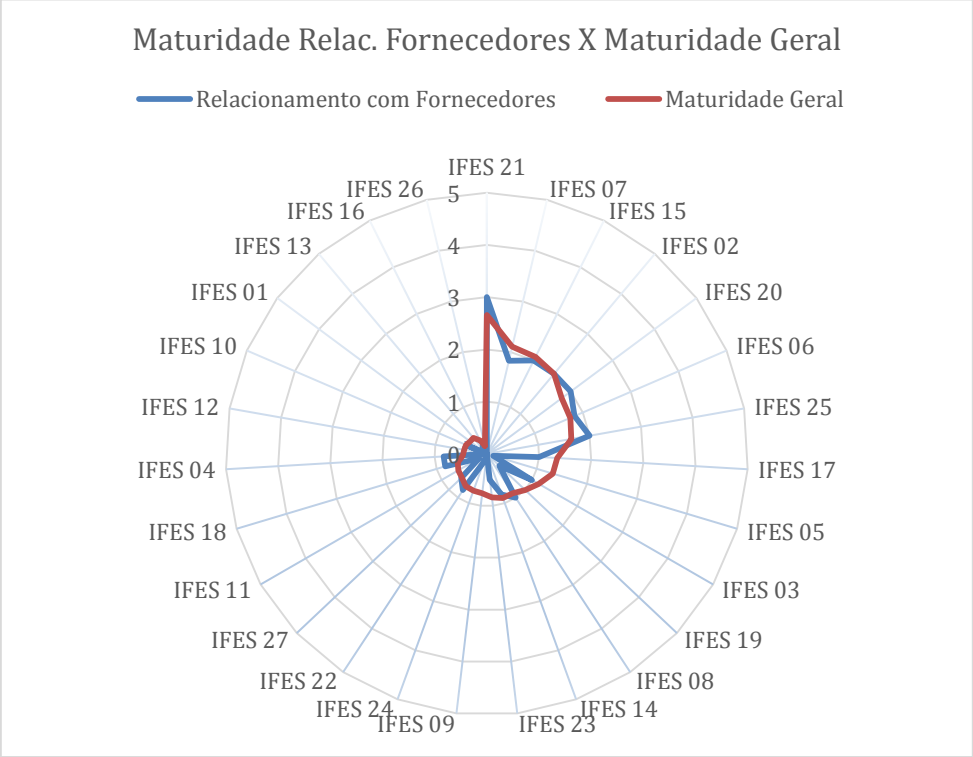
> Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização (ABNT, 2013b, p. 90).

Disterer (2013), afirma que as diretrizes fundamentais para garantir a segurança da informação devem ser definidas e especificadas sob a forma de políticas, definição de papéis e responsabilidades e, em particular, os deveres de manter a confidencialidade e as regras para

comunicações com partes externas como clientes e fornecedores. Contudo, os resultados apresentados no Gráfico 26 revelam que essas diretrizes não estão sendo cumpridas adequadamente.

Através de um comparativo, percebeu-se que os níveis de maturidade no domínio Relacionamento com Fornecedores ficaram bem abaixo dos níveis de maturidade geral, na maior parcela das IFES pesquisadas, conforme Gráfico 27. Com esse resultado, revelou-se mais um domínio com maturidade baixa no cenário das IFES. A exemplo a IFES 05 com a maturidade de apenas 0,13 no domínio Relacionamento com Fornecedores e 1,32 na maturidade geral.

Gráfico 27. Comparativo Maturidade Relac. Fornecedores X Maturidade Geral



Para que este cenário seja revertido, Torres et al. (2010) recomenda que a implementação dos controles de segurança da informação deve ser realizada numa arquitetura *Top-Down*, atingindo desde a mais alta direção, passando por todos os funcionários e abrangendo clientes, fornecedores e demais envolvidos. Os controles apontados na seção 15 da Norma ISO/IEC 27002, são ótimas referencias. Disterer (2013), faz menção, além da Norma 27002 para a gestão da segurança da informação, como também a Norma ISO/IEC 27036 para a segurança da informação no relacionamento com fornecedores. A própria Instrução Normativa 04 de 11 de

setembro de 2014, que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal, trabalha os aspectos de segurança da informação.

4.2.13 Gestão de Incidentes de Segurança da Informação

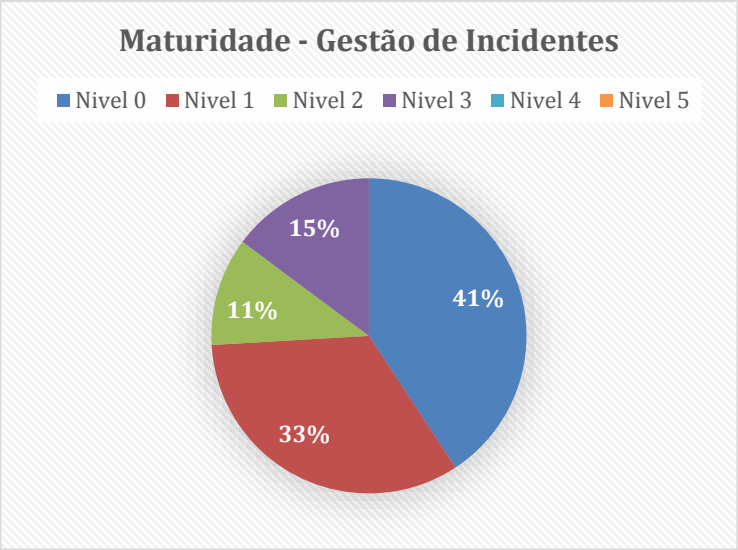
Esta seção tem por objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 16 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Esta seção foca nos processos de notificação de eventos de segurança, responsabilidades e coleta de evidências. Ela possui uma categoria (ABNT, 2013; COELHO et al., 2014):

- Gestão de incidentes de segurança da informação e melhorias – tem como objetivo assegurar que vulnerabilidades e eventos de segurança sejam comunicados e que incidentes de segurança possam ser gerenciados de forma efetiva.

As IFES foram questionadas (questões 91 e 92) quanto aos processos de gestão de incidentes de segurança da informação realizados, ou não, em suas instituições. Com isso foi possível obter o Gráfico 28, com os índices de maturidade de GSI neste domínio.

Cerca de 41% das IFES não realizam procedimentos de gestão de incidentes, ou eles são insuficientes, colocando-as no nível de maturidade 0. No nível de maturidade 1, foram identificadas 33% das instituições. Estas iniciaram o uso dos procedimentos de gestão de incidentes, entretanto eles são informais e executados eventualmente sem gerencia, controle ou documentação. Nos níveis de maturidade 2 e 3, foram identificadas respectivamente 11%, que corresponde as IFES que possuem seus processos de gestão de incidentes planejados e 15%, que correspondem as IFES que estão com os processos bem definidos. Nenhuma das instituições foram identificadas nos níveis de maturidade 4 e 5.

Gráfico 28. Maturidade Gestão de Incidentes



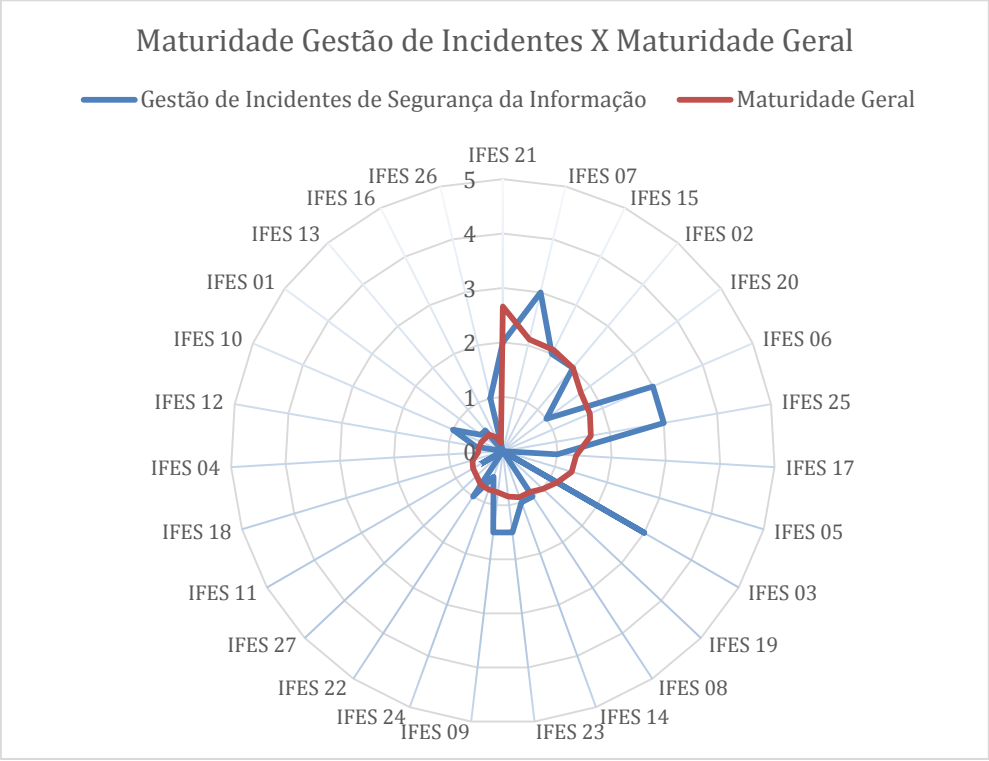
Alshaikh et al. (2014), afirma que independente dos controles de segurança da informação implementados nas organizações, os incidentes de segurança sempre vão acontecer. Assim como qualquer outro controle de segurança da informação os incidentes de segurança devem ser documentados, analisados e avaliados para possíveis melhorias ou verificações essenciais (DISTERER, 2013).

Muitos autores afirmam que a Gestão de Incidentes de Segurança da Informação é um fator crítico para o sucesso da gestão da segurança da informação, autores como: Tu (2015), Coelho et al. (2014), Torres et al. (2010), Stambul e Razali (2011), Fazenda e Fagundes (2015), Moeti e Kelema (2014), Dzazali e Zolait (2012), Lange et al. (2015), ABNT (2005), Disterer (2013), Alexandria e Quoniam (2010), Alshaikh et al. (2014). Desta forma, fica evidente que a gestão de incidentes é de extrema importância para a gestão de segurança das organizações, reduzindo os impactos das ameaças e mantendo a continuidade do negócio.

Comparados os resultados da análise de maturidade no domínio Gestão de Incidentes com a maturidade geral, obtidas pelas instituições participantes, percebeu-se um certo avanço, quando comparados a outros domínios, pois poucos tiveram sua maturidade acima da maturidade geral, conforme Gráfico 29. Esse resultado indica que o processo de Gestão de Incidentes está mais maduro que muitos outros, como pode ser observado na IFES 03, com nível de maturidade 3 neste domínio e 1,15 em sua maturidade geral. Contudo, o fato de 74% das instituições terem

sido identificadas nos níveis de maturidade mais baixos (níveis 0 e 1), revelou que este domínio ainda tem muito a evoluir.

Gráfico 29. Comparativo Maturidade Gestão de Incidentes X Maturidade Geral



Incidentes de segurança vão ocorrer, cedo ou tarde, e quando ocorrerem, procedimentos de recuperação estabelecidos nas políticas de gestão da segurança da informação devem ser implementados em tempo hábil (TORRES et al., 2010). Os mesmos autores afirmam que todos, incluindo funcionários, fornecedores e terceiros devem estar cientes dos procedimentos de recuperação. Alexandria e Quoniam (2010), afirma que um mecanismo importante para a gestão de incidentes de segurança é a criação e manutenção de um grupo de tratamento de incidentes, conhecido como Time de Resposta a Incidentes de Segurança, responsável por receber, analisar e responder a notificações e atividades relacionadas aos incidentes de segurança da informação.

Visando a gestão de incidentes de segurança da informação nos órgãos e entidades da administração pública federal, 3 normas complementares a Instrução Normativa 01 de 13 de junho de 2008 foram criadas. A primeira é a Norma Complementar 05/IN01/DSIC/GSIPR que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da APF. A segunda é a Norma Complementar

08/IN01/DSIC/GSIPR que estabelece as diretrizes para o gerenciamento de incidentes em redes computacionais nos órgãos e entidades da APF. A terceira é a Norma Complementar 21/IN01/DSIC/GSIPR que estabelece as diretrizes para o registro de eventos, coleta e preservação de evidencias de incidentes de segurança em redes nos órgãos e entidades da APF, direta e indireta.

4.2.14 Aspectos da SI na Gestão da Continuidade dos Negócios

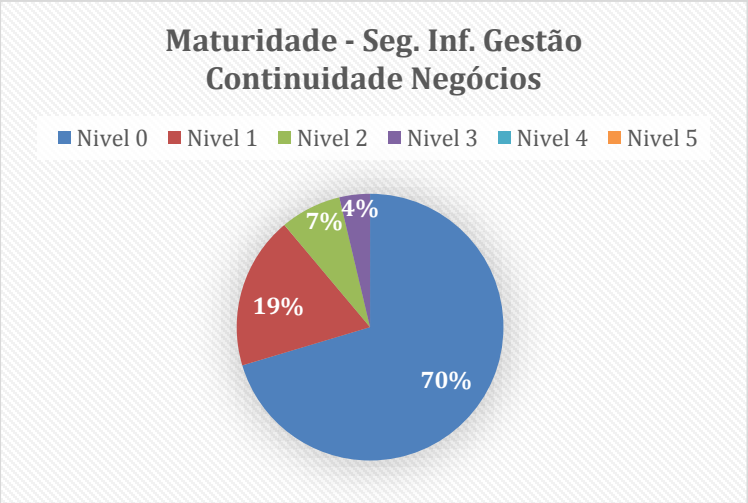
Esta seção tem por objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 17 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. A referida seção trabalha com os aspectos de continuidade em caso de falhas ou desastres e possui duas categorias (ABNT, 2013b; COELHO et al., 2014a):

- Continuidade da segurança da informação – objetiva não permitir a interrupção das atividades voltadas ao negócio, através da proteção dos processos críticos contra efeitos de falhas ou desastres significativos. Com isso, é possível garantir uma retomada dos serviços em tempo hábil.
- Redundâncias – tem por objetivo manter a disponibilidade dos serviços que suportam o negócio, assegurando o acesso quando necessário.

A continuidade da gestão da segurança da informação precisa ser considerada nos planos de gestão da continuidade dos negócios de uma organização, bem como garantir a disponibilidade dos recursos que processam essas informações através de procedimentos de redundância (ABNT, 2013).

Quando avaliadas (questão 93) a respeito dos controles de segurança da informação na gestão da continuidade dos negócios, o Gráfico 30 demonstra mais um resultado preocupante quanto ao tratamento da segurança da informação. A maioria das instituições pesquisadas foram identificadas nos níveis de maturidade 0 e 1, com 70% e 19% do total respectivamente. No nível de maturidade 2, foram identificadas 7% das IFES pesquisadas e no nível de maturidade 3, foram identificadas 4%.

Gráfico 30. Maturidade SI na Gestão da Continuidade do Negócio

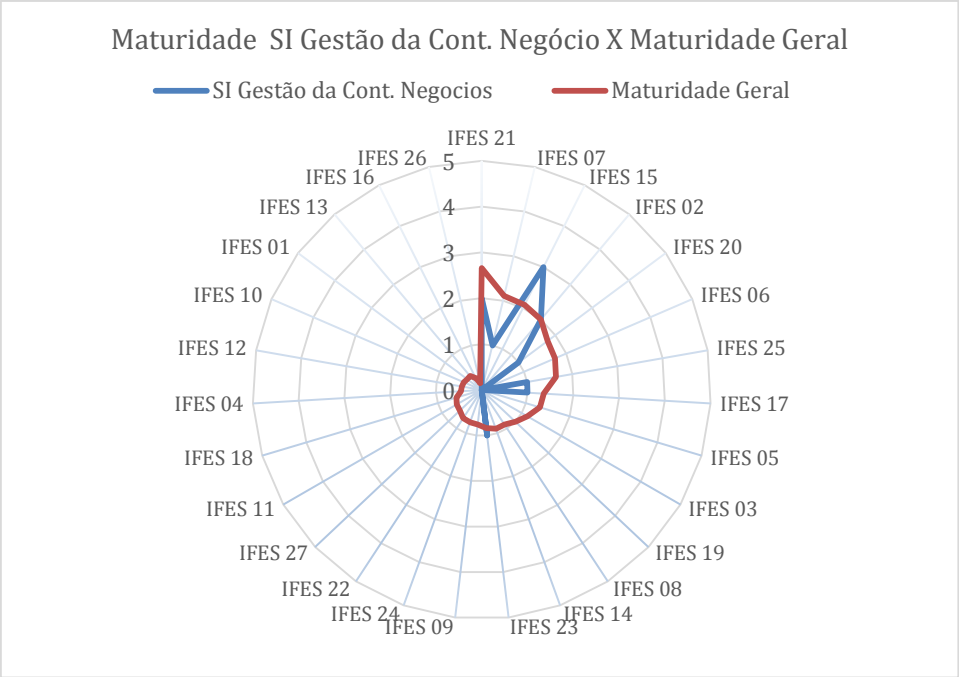


Neste aspecto, o resultado de maturidade apresentado no Gráfico 30 se aproxima com o levantamento realizado pelo IGovTI2014. No levantamento apenas 27% dos órgãos da APF analisados declararam dispor de políticas de cópias de segurança dos dados institucionais de forma integral, outras 27% adotam a pratica de forma parcial. Nesse mesmo levantamento, apenas 27% dos órgãos declararam dispor de uma política de gestão da continuidade dos negócios.

O objetivo da gestão da continuidade dos negócios, segundo Disterer (2013), é combater as interrupções das atividades empresariais e proteger os processos críticos de negócio dos efeitos das grandes falhas dos sistemas de informação ou catástrofes e assegurar a sua retomada a tempo. Alshaikh et al. (2014), afirma que um gerenciamento de incidentes apropriado e eficaz auxilia na redução do impacto das ameaças e na manutenção da continuidade dos negócios.

Um comparativo entre a maturidade no domínio Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio e a maturidade geral, obtidas pelas instituições respondentes, revelou que os níveis de maturidade neste domínio estão muito abaixo da maturidade geral, conforme apresentado no Gráfico 31. Este resultado, somado aos 70% das instituições identificadas no nível de maturidade 0, revelou um cenário preocupante, podendo afetar negativamente o princípio da disponibilidade. A IFES 07 com o nível de maturidade 1 neste domínio e 2,11 de maturidade geral, é um bom exemplo desse cenário.

Gráfico 31. Comparativo Maturidade SI na Gestão da Cont. Negócio X Maturidade Geral



Paranhos (2010), afirma que um plano de continuidade de negócios bem implementado prevê ações para o funcionamento da empresa nos momentos de indisponibilidade dos ativos e das pessoas dos processos críticos ao negócio. Este plano deve atender também aos requisitos para a continuidade da gestão da segurança da informação, durante uma crise ou desastre (ABNT, 2013b).

Buscando garantir a continuidade da gestão da segurança da informação nos planos de gestão da continuidade dos negócios, foi criada a Norma Complementar 05/IN01/DSIC/GSIPR que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da APF.

4.2.15 Conformidade

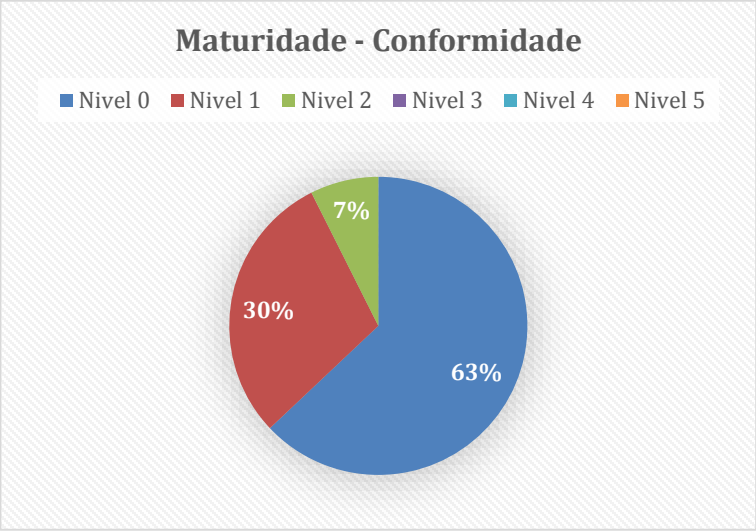
Esta seção tem como objetivo apresentar os resultados dos níveis de maturidade identificados acerca da seção 18 da norma ABNT NBR ISO/IEC 27002, das IFES pesquisadas. Esta seção define os requisitos de segurança da informação em conformidade com toda e

qualquer legislação vigente e está dividida em duas categorias de segurança (ABNT, 2013; COELHO et al., 2014):

- Conformidade com requisitos legais e contratuais – objetiva evitar qualquer violação de lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de qualquer requisito de segurança da informação.
- Análise crítica da segurança da informação – tem como objetivo assegurar que a gestão da segurança da informação esteja implementada e operacionalizada dentro das políticas e procedimentos determinados pela organização.

O Gráfico 32 apresenta o resultado obtido acerca dos questionamentos (questões 94 a 101) feitos as IFES no domínio Conformidade. Cerca de 93% das IFES questionadas não chegaram no nível de maturidade 2.

Gráfico 32. Maturidade da Conformidade



Este é mais um resultado preocupante, pois toda a estrutura da GSI deve ser elaborada estando em total sincronia com as obrigações legais, estatutárias, regulamentares ou contratuais, além é claro das normas internas da própria organização. Entretanto, apenas 7% das instituições pesquisadas possuem essas práticas planejadas e documentadas.

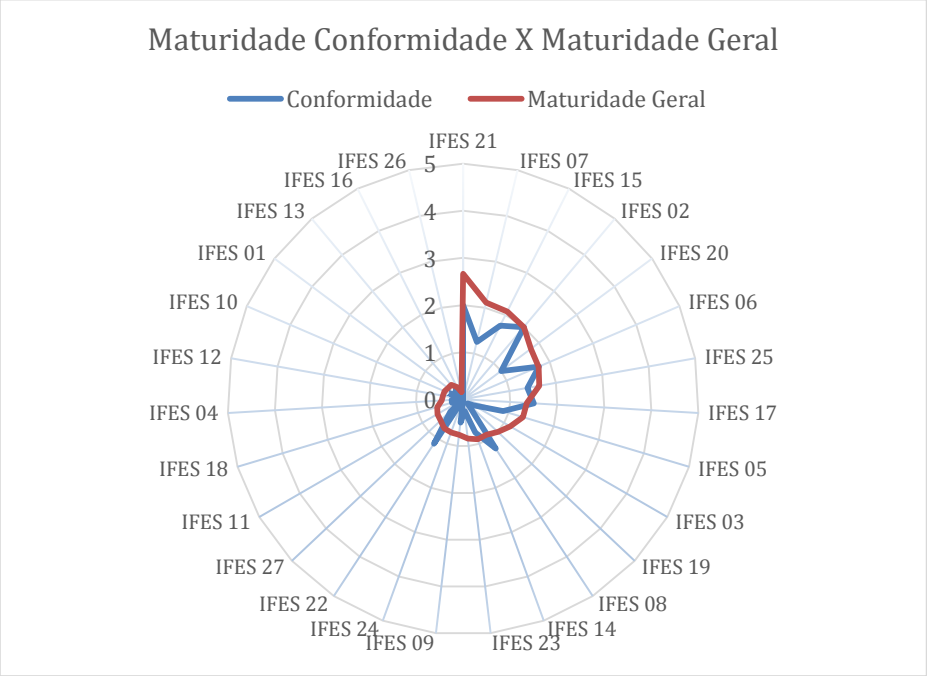
A norma ABNT NBR ISO/IEC 27002 trata a conformidade com as políticas e procedimentos de segurança da informação da seguinte forma:

> Convém que os gestores analisem criticamente, a intervalos regulares, a

> conformidade dos procedimentos e do processamento da informação, dentro das áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação (ABNT, 2013b, p. 96).

Quando comparadas, a maturidade do domínio Conformidade com a maturidade geral, obtidas pelas instituições respondentes, observou-se que os níveis de maturidade neste domínio estão muito abaixo da maturidade geral, conforme apresentado no Gráfico 33. Este resultado deixa evidente que a conformidade entre os procedimentos de segurança da informação realizados pelas IFES e as normas internas e legislação vigente não estão sendo tratadas adequadamente. As IFES 07 e 20 são bons exemplos dessa situação, com 1,25 e 1,0 de maturidade no domínio Conformidade e maturidade geral de 2,11 e 1,79, respectivamente.

Gráfico 33. Comparativo Maturidade da Conformidade X Maturidade Geral



Disterer (2013), afirma que para o cumprimento dos requisitos de conformidade, medidas adequadas devem ser implementadas, em especial os direitos de autoria e de exploração, os requisitos para segurança e proteção de dados, de modo que sejam regulados e assegurados de forma verificável.

Os resultados apresentados e analisados nos Gráficos 31 e 32, trazem à tona a importância em se definir os fatores responsáveis pelo aprimoramento dos níveis de maturidade em GSI.

Dessa forma, atendendo-se a esses fatores considerados críticos para aprimoramento da gestão da segurança da informação, será possível obter índices de maturidade adequados.

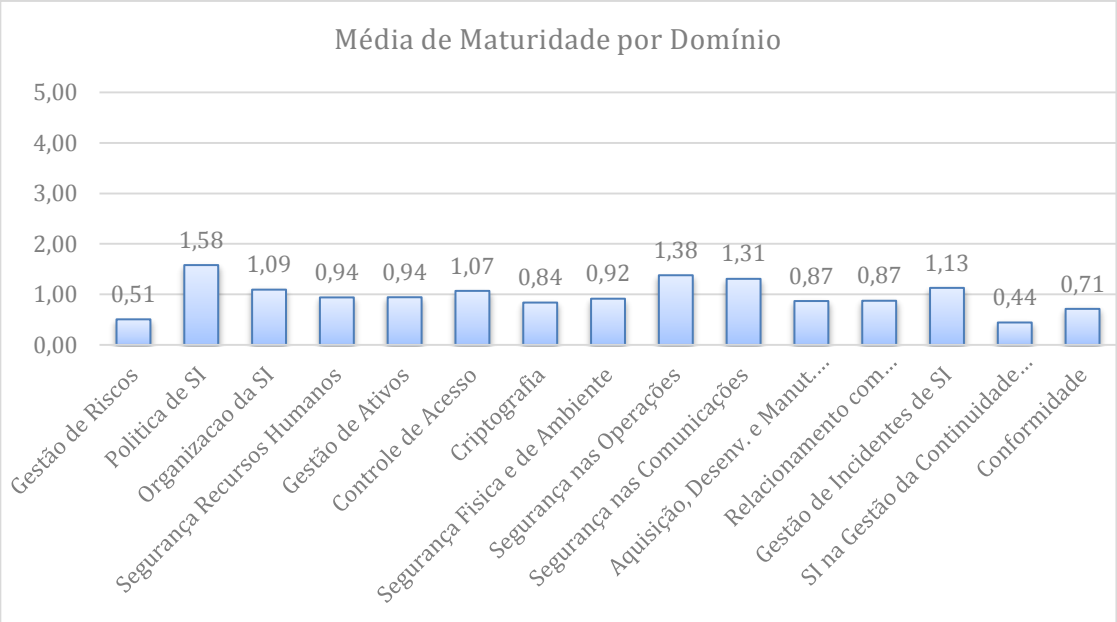
4.2.16 Consolidação dos Resultados do Diagnóstico de Maturidade

Após a realização do diagnóstico de maturidade de Gestão de Segurança da Informação (GSI) nas Instituições Federais de Ensino Superior (IFES), foi possível observar a amplitude das áreas abordadas pela norma NBR ISO/IEC 27002:2013 e a complexidade em planejar, implementar e gerir os controles de segurança da informação.

Através dos resultados obtidos por meio do diagnóstico de maturidade, constatou-se uma situação variada quanto a maturidade alcançada entre os domínios de segurança avaliados na pesquisa, ou seja, as IFES participantes alcançaram melhores níveis de maturidade em alguns domínios e piores em outros. Contudo, Semôla (2014), em seu livro "Gestão da Segurança da Informação: Uma visão executiva", explica que numa avaliação deste tipo, essa situação está presente na maioria das organizações e isso acontece devido a ausência de um diagnóstico abrangente e capaz de integrar o levantamento de ameaças, impactos, vulnerabilidades física, tecnológica e humana, associando-as às reais necessidades do negócio.

O Gráfico 34 apresenta uma média dos níveis de maturidade obtidos pelas instituições participantes da pesquisa em cada domínio. Verificou-se que os domínios que alcançaram os maiores níveis de maturidade na pesquisa foram: Política de Segurança da Informação; Segurança nas Operações e; Segurança nas Comunicações. Contudo, o fato desses domínios terem alcançado os maiores níveis de maturidade não garante que seus controles de segurança estejam sendo executados adequadamente, pois a maior parte das instituições foram identificadas nos níveis de maturidade 0 e 1.

Gráfico 34. Média da Maturidade por Domínio



Em contrapartida os domínios que alcançaram os piores níveis de maturidade nesta pesquisa foram: Gestão de Riscos; Aspectos de Segurança da Informação na Gestão da Continuidade dos Negócios e; Conformidade. Esse resultado revela que uma atenção maior deve ser dada a esses domínios, pois estão relacionados a aspectos importantes como análise de riscos, continuidade do negócio e garantia da conformidade com a legislação local e normas da organização.

Um destaque maior pode ser dado ao domínio Gestão de Riscos de Segurança da Informação, pois é através dele que os requisitos de segurança da informação são identificados e validados. Sêmola (2014), afirma que sem uma análise de riscos as ações de segurança tornam-se desorientadas, mal priorizadas, redundantes, muitas vezes, e, assim pecam por não oferecer o retorno esperado e medido pelo nível de segurança da organização.

4.3 Conclusão do capítulo

Este capítulo buscou apresentar o resultado do diagnóstico de maturidade da gestão da segurança da informação das IFES pesquisadas. O diagnóstico foi realizado em duas etapas: (1) diagnóstico de maturidade geral das IFES; (2) diagnóstico de maturidade por domínio.

Os dados coletados durante o estudo de campo foram inseridos na ferramenta de avaliação de maturidade possibilitando a identificação da situação quanto a maturidade da gestão da segurança da informação das IFES pesquisadas. O resultado moutrou-se preocupante, pois a maior parcela das IFEs pesquisadas foram avaliadas no nível mais baixo de maturidade (nível 0). Nenhuma das IFES pesquisadas foram identificadas nos níveis de maturidade 3, 4 e 5. No nível de maturidade mais alto alcançado pelas instituições (nível 2), apenas 4 IFES foram identificadas.

Quanto a avaliação por domínio, percebeu-se que os domínios que alcançaram os maiores níveis de maturidade na pesquisa foram: Política de Segurança da Informação; Segurança nas Operações e; Segurança nas Comunicações. Em contrapartida os domínios de menor maturidade foram: Gestão de Riscos; Aspectos de Segurança da Informação na Gestão da Continuidade dos Negócios e; Conformidade.

Os resultados apresentados possibilitam as IFES identificarem quais domínios estão mais críticos e quais estão com maior maturidade, podendo focar seus esforços naqueles que realmente importam.

5 FATORES CRÍTICOS PARA APRIMORAR A MATURIDADE DA GSI

Este capítulo apresenta como foi realizado a classificação de importância dos Fatores Críticos de Sucesso (FCS) para aprimorar a maturidade de GSI, encontrados nos estudos da Revisão Sistemática, capítulo 2, item 2.5.2 (p.68). Após a realização do diagnóstico de maturidade, as 27 IFES participantes deste estudo foram classificadas em ordem decrescente de acordo com o nível de maturidade, conforme já apresentado no capítulo 4, item 4.1, Tabela 4 (p. 83).

Após classificar todas as IFES, foi possível identificar as 5 instituições que se destacaram quanto ao nível de maturidade. Essas IFES foram contatadas por meio eletrônico (e-mail) no intuito de responder um questionário que definiu o grau de importância dos FCS para o aprimoramento da maturidade de GSI. Este capítulo está estruturado nas seguintes seções:

- **Grau de importância dos FCS:** apresenta os procedimentos utilizados para a coleta dos dados e o método utilizado para definição do grau de importância dos FCS;
- **Consolidação dos FCS**: apresenta o resultado final, com a priorização dos FCS para o aprimoramento da maturidade da gestão da segurança da informação.

5.1 Grau de importância dos FCS

Para identificação do grau de importância dos FCS um questionário foi utilizado como instrumento para coleta dos dados. Este questionário foi disponibilizado em meio eletrônico através da ferramenta Google Forms. As questões foram elaboradas utilizando a escala Likert com 5 pontos. Dzazali e Zolait (2012), informam que a escala Likert é amplamente utilizada para medição de atitudes, crenças e opiniões.

Quando questionados, os respondentes informaram sua opinião quanto ao grau de importância dos 12 FCS (Item 2.5.2, p.68) para os níveis de maturidade 1 ao 5 de GSI. Neste caso, não foi considerado o nível de maturidade 0, pois neste nível não há processos de segurança estabelecidos, logo não há necessidade de inclui-lo no questionário.

As opções de respostas foram de Sem Importância a Muito Importante, sendo que a cada opção foi atribuído um valor (ponto), conforme Tabela 5.

Tabela 5. Grau de importância do fator

Sem Importância	Pouco importante	Indiferente	Importante	Muito importante
1	**2**	**3**	**4**	**5**

Fonte: adaptado de Oliveira (2016)

A tabulação dos dados coletados do questionário foi realizada utilizando-se o calculo da média ponderada, conforme trabalho de Oliveira (2016). Multiplicou-se as pontuações das respostas (PR) com a quantidade de respondentes (QR), somando-a e, posteriormente, dividindo-se o resultado pelo número de respondentes (NR), o que conferiu o grau de importância do fator (GIF), conforme Figura 9.

Figura 9. Fórmula do grau de importância do fator

$$GIF = \frac{\sum PRxQR}{NR}$$

Fonte: adaptado de Oliveira (2016)

Considerando que, conforme o nível de maturidade aumenta, a maturidade e a complexidade dos processos de segurança também aumentam, foi atribuído um peso para cada nível de maturidade, de modo que o grau de importância dado aos fatores pelos respondentes obtivesse um peso diferente em cada nível de maturidade, conforme tabela 6.

Tabela 6. Peso dos níveis de maturidade

Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
1	**2**	**3**	**4**	**5**

Desta forma, o grau de importância geral do fator (GIGF) foi alcançado através da soma da pontuação média do grau de importância do fator (GIF) multiplicado pelo peso do nível de maturidade (PN), dividida pela somatória dos pesos dos níveis (SPN), conforme Figura 10.

Figura 10. Fórmula do grau de importância geral do fator

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}}$$

Fonte: adaptado de Oliveira (2016)

Estabelecidas as fórmulas foi possível identificar o grau de importância dos FCS para os níveis de maturidade 1 ao 5 (calculo detalhado no APÊNDICE B. CÁLCULO DO GRAU DE IMPORTÂNCIA DOS FATORES), e posteriormente o grau de importância geral de cada FCS para o aprimoramento da maturidade de GSI, demonstrados nos tópicos a seguir.

5.1.1 Grau de importância do FCS Treinamento e Conscientização

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Treinamento e Conscientização**, foi possível a elaboração da Tabela 7.

Tabela 7. Grau de Importância do FCS Treinamento e Conscientização

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Treinamento e Conscientização	Nível 1	4,4
	Nível 2	4,8
	Nível 3	5,0
	Nível 4	4,6
	Nível 5	5,0

Com esse resultado foi possível estabelecer o grau de importância geral do fator (GIGF), produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}6\text{x}1)+(5{,}0\text{x}2)+(4{,}8\text{x}3)+(5{,}0\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}93$$

O fator Treinamento e Conscientização obteve um GIGF de 4,93 pontos, o que o coloca em primeiro lugar quando comparados aos demais fatores avaliados. Este resultado evidencia a importância que o referido fator tem para o aprimoramento da maturidade de GSI, pois é através

de uma estratégia de treinamento e conscientização bem estruturada que todos os colaboradores de uma instituição passam a enxergar a segurança da informação como essencial para o negócio.

Grande parte das instituições ainda acredita que a segurança da informação é uma área que deve ser conhecida e dominada apenas pelo pessoal de TI, contudo, estudos recentes demonstram que não é bem assim: Fazenda e Fagundes (2015), Moeti e Kelema (2014), Dzazali e Zolait (2012), Lange et al. (2015), Yildirim et al. (2011), Quintella e Branco (2013), Disterer (2013), Alexandria e Quoniam (2010), Alshaikh et al. (2014). A segurança da informação deve ser compreendida por todos os colaboradores de uma organização, em todos os níveis, não somente pela equipe de TI.

Muitos dos incidentes de segurança são causados pela falta de conscientização e treinamento dos funcionários, levando ao mau uso dos recursos de informação ou má interpretação de tecnologia ou dos procedimentos (ALSHAIKH et al., 2014). Para que isso seja evitado, os funcionários e a gerencia deve ter um certo nível de compreensão dos riscos de segurança para os ativos de informação da organização.

Von Solms (1999, apud TU, 2015), afirma que a consciência da segurança da informação precisa ser reconhecida pela alta gestão, não somente pela equipe de TI. Alexandria e Quoniam (2010), em seu trabalho: "Proposta para a Estruturação da Gestão da Segurança da Informação em um Ambiente de Pesquisa Científica", afirmam que:

> Para se conscientizar um usuário dos riscos a que as informações estão expostas é necessário manter um sistema de treinamento contínuo, para que as práticas de segurança sejam internalizadas e produzam os efeitos esperados.

As pessoas são elementos cruciais na manutenção da segurança da informação, pois de nada adianta possuir as práticas e procedimentos bem estruturados e documentados de GSI, se aqueles que manipulam as informações não tiverem uma consciência da segurança da informação.

5.1.2 Grau de importância do FCS Gestão de Riscos

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Gestão de Riscos**, foi possível a elaboração da Tabela 8.

Tabela 8. Grau de Importância do FCS Gestão de riscos

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Gestão de Riscos	Nível 1	4,2
	Nível 2	4,8
	Nível 3	4,8
	Nível 4	5,0
	Nível 5	5,0

Após a obtenção do GIF para o fator Gestão de Riscos, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importância do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}2\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(5{,}0\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}88$$

O FCS Gestão de Riscos, foi considerado um dos mais importantes para o aprimoramento da maturidade de GSI, obtendo um GIGF de 4,88 pontos, ficando em segundo lugar, logo abaixo do fator Treinamento e Conscientização.

É por meio da análise de riscos que os ativos da organização considerados na GSI são identificados e, a partir deles, as políticas de segurança da informação e toda uma cadeia de processos de segurança serão elaboradas (FAZENDA e FAGUNDES, 2015).

Torres et al. (2010), afirma que a identificação dos requisitos de segurança da informação de uma instituição é realizada através de uma análise sistemática dos riscos da segurança da informação. Os mesmos autores ainda informam que os investimentos com controles de segurança precisam ser ponderados conforme os danos causados aos negócios gerados pelos potenciais incidentes de segurança.

Com a análise dos riscos bem executada, é possível direcionar e estabelecer as ações necessárias e as prioridades gerenciais dos riscos da Segurança da Informação, na implementação de controles para proteção contra esses riscos. Isso pode ser alcançado estabelecendo-se um programa de gestão de riscos de segurança da informação utilizando como base a norma ABNT NBR ISO/IEC 27005.

5.1.3 Grau de importância do FCS Cultura de Segurança da Informação

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Cultura de Segurança da Informação**, foi possível a elaboração da Tabela 9.

Tabela 9. Grau de Importância do FCS Cultura de Segurança da Informação

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Cultura de Segurança da Informação	Nível 1	4,4
	Nível 2	4,8
	Nível 3	4,8
	Nível 4	4,8
	Nível 5	5,0

Com esse resultado é possível estabelecer o grau de importância geral do fator (GIGF) em análise, produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}4\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}84$$

A Cultura de Segurança da Informação é a forma como as pessoas se comportam em relação a segurança da informação na organização (Hu et al., 2012; apud Tu, 2015). Este fator ficou com um GIGF de 4,84 pontos, colocando-o entre os 5 FCS com maior grau de importância para o aprimoramento da maturidade de GSI. Este fator está intimamente ligado ao fator Treinamento e conscientização, pois somente através de estratégias de conscientização efetivas se consegue estabelecer uma cultura de segurança.

Dhilon e Backhouse (2001, apud Dzazali e Zolait, 2012), afirmam que a cultura de segurança da informação pode ser definida como a suposição sobre qual o tipo de comportamento de segurança da informação é aceito e incentivado a fim de incorporar características de segurança na maneira como as coisas são feitas em uma organização.

Fazenda e Fagundes (2015), afirmam que grande parte dos usuários dos ativos de informação ainda mantem a ideia de que a segurança da informação serve apenas para a

“proteção do computador”. Ou seja, muitas instituições ainda mantem a cultura de que as situações devem ser tratadas e resolvidas de forma rápida, sem considerar os aspectos da segurança da informação.

De acordo com a Instrução Normativa GSI Nº 1, promover a cultura da segurança da informação, é um dos papéis atribuídos ao Gestor de Segurança da Informação e Comunicações na APF (BRASIL, 2008). Tu et al. (2014, apud Alshaikh et al., 2014), afirma que este gestor deve manter a comunicação com toda a organização (incluindo a alta gerência) para garantir que os requisitos de negócios, direções de gerenciamento e procedimentos sejam considerados com relação à segurança da informação. Com estes canais de atendimento bem estabelecidos e mantidos, a segurança da informação terá um reconhecimento dentro da organização e dessa forma será vista como um elemento importante, cultivando assim uma cultura de segurança da informação na instituição (ALSHAIKH et al., 2014).

Adquirindo uma cultura de segurança, cada funcionário dentro da instituição reconhecerá a importância da segurança da informação para a instituição e atuará em conformidade com ela, resultando na efetividade dos procedimentos e aprimoramento da maturidade da GSI.

5.1.4 Grau de importância do FCS Apoio da Alta Gestão

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 a 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Apoio da Alta Gestão**, foi possível a elaboração da Tabela 10.

Tabela 10. Grau de Importância do FCS Apoio da alta gestão

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Apoio da Alta Gestão	Nível 1	4,2
	Nível 2	4,8
	Nível 3	5,0
	Nível 4	4,6
	Nível 5	5,0

Calculado o GIF do fator Apoio da Alta Gestão, foi possível realizar o calculo do grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}4\text{x}1)+(4{,}8\text{x}2)+(5{,}0\text{x}3)+(4{,}6\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}83$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,83 pontos. Este resultado coloca o Apoio da Alta Gestão, entre os 5 FCS com maior GIGF, apontado pelos respondentes. Acima deste ficaram os FCS Treinamento e Conscientização, Gestão de Riscos e Cultura de Segurança da Informação. Ou seja, o Apoio da Alta Gestão é um fator que deve ser priorizado para que se possa alcançar bons níveis de maturidade de GSI.

Durante a fase de leitura da revisão sistemática, esse fator foi citado em 15 trabalhos, conforme Item 2.4.2, Quadro 8. Kayworth e Whitten (2010, apud TU, 2015), afirma que o comprometimento da alta gestão traz o enfoque necessário para que a segurança da informação seja considerada importante em toda a organização, incluindo o financiamento, alocação de recursos humanos e financeiros e a promoção da cultura da segurança da informação em todos os níveis gerencias. Torres et al. (2010), afirmam que para a obtenção da segurança da informação de forma eficaz, o apoio da gestão deve ser constante e presente. O mesmo autor afirma que a implantação deve acontecer de cima para baixo (arquitetura Top-Down), atingindo todos os níveis da organização, desde a mais alta direção, passando por todos os funcionários e clientes, fornecedores e *stakeholders*[3].

Stambul e Razali (2011), em seu trabalho "*An Assessment Modelo f Information Security Implementation Levels",* afirma que:

> Para garantir a segurança da informação, a alta gestão deve dar o apoio necessário, garantindo que todos na organização conheçam seu papéis e responsabilidades, fornecendo treinamento e programas de conscientização.

[3] Pessoa ou grupo que tem interesse nos resultados de uma organização.

A falta de comprometimento e apoio da alta gestão é refletida através do não provimento de recursos para realização de programas que buscam expandir a cultura de segurança da informação dentro das organizações, baixo envolvimento nas ações de GSI com o intuito de demonstrar aos colaboradores que a segurança da informação é uma preocupação oriunda do negócio da organização, falta de analises críticas da GSI para garantir a melhoria contínua nos processos e alinhamento aos objetivos da organização (FAZENDA e FAGUNDES, 2015). Com isso fica evidente que o apoio da alta gestão é um dos principais fatores críticos para o sucesso da GSI, pois praticamente todos os demais fatores possuem uma relação direta com ele.

5.1.5 Grau de importância do FCS Alinhamento com o negócio

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Alinhamento com o negócio**, foi possível a elaboração da Tabela 11.

Tabela 11. Grau de Importância do FCS Alinhamento com o negócio

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Alinhamento com o negócio	Nível 1	3,4
	Nível 2	4,6
	Nível 3	4,8
	Nível 4	5,0
	Nível 5	5,0

Após a identificação do GIF, foi possível estabelecer o grau de importância geral do fator (GIGF) em análise, produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}4\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(5{,}0\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}80$$

O FCS Alinhamento com negócio, está intimamente relacionado com o FCS Estrutura Organizacional, pois através da inter-relação entre os objetivos de negócio e a segurança da informação é possível manter um alinhamento entre as estratégias de GSI e as estratégias institucionais. Esse fator obteve um GIGF de 4,80 pontos.

Chang et al. (2011, apud Tu, 2015), afirmam que o alinhamento com o negócio se refere aos esforços colaborativos entre a segurança da informação e os gerentes de negócios para a consolidação das práticas de GSI com as estratégias de negócio da organização. O propósito principal desse alinhamento é apoiar os objetivos institucionais.

Solms e Solms (2004, apud Dzazali e Zolait, 2012), afirmam que as organizações precisam perceber que a proteção da informação é uma questão de negócios e não somente técnica. Os autores ainda acrescentaram que a gestão da segurança da informação é uma disciplina multidimensional, e que todas as dimensões devem ser tidas em conta para assegurar um ambiente adequado e seguro para ativos de informação da organização.

O verdadeiro valor da segurança da informação é reconhecido, quando seus objetivos e metas estão se movendo na mesma direção que a missão, metas e objetivos organizacionais gerais. Dessa forma, a GSI passa a ser vista não somente como um instrumento de suporte, mas como um agregador de valor ao negócio (DZAZALI e ZOLAIT, 2012).

5.1.6 Grau de importância do FCS Medição e Avaliação

Considerando o resultado do questionário, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Medição e avaliação**, foi possível a elaboração da Tabela 12.

Tabela 12. Grau de Importância do FCS Medição e avaliação

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Medição e avaliação	Nível 1	3,8
	Nível 2	4,8
	Nível 3	4,8
	Nível 4	4,8
	Nível 5	4,8

Estabelecido o GIF para o fator Medição e Avaliação, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}73$$

Medição e avaliação, obteve o mesmo GIGF que o fator Gestão de incidentes, ambos com 4,74 pontos. Estes fatores estão relacionados a atividades de monitoramento e análise, não só de incidentes de segurança como também de todos os processos de GSI.

Coelho et al. (2014a), afirma que atividades de monitoração e análise crítica são fundamentais para o sucesso de um Sistema de Gestão da Segurança da Informação (SGSI) e consequentemente da GSI de um órgão. Os mesmos autores, informam que essas atividades permitem o acompanhamento, por meio de evidencias, e também o processo de melhoria contínua.

A medição e avaliação refere-se ao monitoramento dos indicadores, que servirão para realimentar o processo de segurança, aprimorando as medias e controles adotados (ALEXANDRIA e QUONIAM, 2010). Ou seja, é necessário implementar um sistema de medição, que seja usado para avaliar o desempenho da GSI e obtenção de dados que servirão como sugestões de melhoria (ABNT, 2005).

A Medição e Avaliação é um FCS que tem ênfase principalmente no nível de maturidade 5 (Melhoria Contínua), pois é neste nível que os objetivos de desempenho quantitativo (metas) para a eficácia dos processos e eficiência são estabelecidos, com base nas metas de negócios da organização. O GIF obtido por esse fator no nível de maturidade 5 (4,8), corrobora com essa afirmação.

5.1.7 Grau de importância do FCS Gestão de incidentes

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Gestão de incidentes**, foi possível a elaboração da Tabela 13.

Tabela 13. Grau de Importância do FCS Gestão de incidentes

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Gestão de incidentes	Nível 1	3,8
	Nível 2	4,8
	Nível 3	4,8
	Nível 4	4,8
	Nível 5	4,8

Dessa forma, esse resultado possibilitou estabelecer o grau de importância geral do fator (GIGF) em análise, produto do somatório da pontuação do grau de importância do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}73$$

A Gestão de Incidentes de Segurança, além de ser um FCS para a GSI, também é uma das seções trabalhadas na norma ABNT NBR ISO/IEC 27002. Este fator obteve o mesmo GIGF de 4,73 que o fator Medição e avaliação, abordado no tópico anterior. Esse resultado evidencia a relação direta que existe entre esses fatores.

Alshaikh et al. (2014), comenta que independentemente dos controles de segurança da informação que as organizações implementam, não há garantias de que incidentes de segurança não irão acontecer, e de fato eles irão. O mesmo autor ainda informa que a gestão de incidentes procura gerir de forma eficaz a resposta a incidentes de segurança, minimizando o seu impacto e protegendo os ativos de informação das organizações.

Diversas organizações acreditam que estão seguras pelo simples fato de que os seus sistemas de informações ainda não tenham sido comprometidos. Entretanto, isso não significa que a organização tenha boas medidas de segurança, ela simplesmente pode ter tido sorte até agora (DZAZALI e ZOLAIT, 2012). Outras acreditam que por não atuarem nas áreas alvo de atacantes, estão seguras. Contudo, estudos recentes afirmam que grande parte dos atacantes não precisam de um motivo para atacar (BERINATO, 2003, apud DZAZALI e ZOLAIT, 2012).

A norma ABNT NBR ISO/IEC 27002, na sua seção 16, Item 16.1, tem como objetivo:

> Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Werlinger et al. (2010, apud Alshaikh, 2014), afirmam que os gerentes de segurança devem liderar e gerenciar o processo de resposta a incidentes e ter habilidades e conhecimentos adequados para gerenciar a equipe de resposta a incidentes. Desta forma, constata-se que um gerenciamento de incidentes adequado e eficaz é importante para reduzir o impacto das ameaças e manter a continuidade dos negócios. Ou seja, é um FCS que deve ser considerado na GSI.

5.1.8 Grau de importância do FCS Política de segurança da informação

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Política de segurança da informação**, foi possível a elaboração da Tabela 14.

Tabela 14. Grau de Importância do FCS Política de segurança da informação

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Política de segurança da informação	Nível 1	4,0
	Nível 2	4,6
	Nível 3	4,8
	Nível 4	4,8
	Nível 5	4,8

Determinado o GIF do fator Política de Segurança da Informação (PSI), foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}0\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}72$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,72 pontos, classificando-o em sétimo lugar. Contudo, por mais que a PSI não tenha sido classificada entre os 5 primeiros FCS para a GSI, o GIGF obtido por este fator, evidencia a importância que ele tem sobre a GSI de forma geral.

A Política de Segurança da Informação (PSI) é o documento que define a importância da segurança da informação para a organização, especificando os objetivos de segurança e a responsabilidade dos funcionários com a segurança da informação (Ma et al., 2009, apud Tu, 2015). Disterer (2013), afirma que a aplicação e distribuição da PSI dentro de uma organização serve para enfatizar a importância da segurança da informação e a atenção da gerencia para esse propósito. O mesmo autor ainda informa que a segurança da informação deve estar organizada na instituição em forma de políticas, para que dessa forma as medidas de segurança possam ser eficientemente promovidas e estabelecidas.

Uma PSI eficaz garante que a cultura da segurança da informação seja integrada as rotinas de trabalho, dessa forma cria-se uma atmosfera de segurança que se torna preocupação entre os funcionários (ALNATHEER, 2015). É nela que estão dispostos os papéis e responsabilidades, e principalmente os deveres para com a confidencialidade e as regras de uso dos ativos de informação. Ou seja, a PSI, se bem elaborada, é o produto final de uma GSI eficaz numa instituição.

5.1.9 Grau de importância do FCS Papéis e responsabilidades

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Papéis e responsabilidades**, foi possível a elaboração da Tabela 15.

Tabela 15. Grau de Importância do FCS Papéis e responsabilidades

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Papéis e responsabilidade	Nível 1	3,8
	Nível 2	4,6
	Nível 3	4,8
	Nível 4	4,8
	Nível 5	4,8

Dessa forma, esse resultado possibilitou estabelecer o grau de importância geral do fator (GIGF) em análise, produto do somatório da pontuação do grau de importância do fator multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\mathrm{GIGF} = \frac{\sum (\mathrm{GIFxPN})}{\mathrm{SPN}} = \frac{(3{,}8\mathrm{x}1)+(4{,}6\mathrm{x}2)+(4{,}8\mathrm{x}3)+(4{,}8\mathrm{x}4)+(4{,}8\mathrm{x}5)}{15} = 4{,}71$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,71 pontos. Este FCS está relacionado com a definição clara dos papéis e responsabilidades pela segurança da informação na organização.

Lange et al. (2015), afirma que a distribuição clara dos papéis e responsabilidades é necessária para permitir uma implementação eficaz da GSI, e também uma compreensão da

propriedade e responsabilidade dos ativos de informação na organização. Além disso, é essencial que os membros da alta gestão tenham a sensibilidade, quanto a definição dos papéis e responsabilidades, para garantir a aplicação efetiva e o funcionamento das políticas de segurança da informação.

Coelho et al. (2014a), informa que para cada ativo e procedimento de segurança, é importante atribuir responsabilidades a um funcionário (ou cargo). Em outras palavras, o funcionário deverá efetuar a gestão do ativo ou procedimento segundo a determinação da política de segurança.

Quanto a definição de papéis e responsabilidades a Instrução Normativa GSI nº 01, de 14 de junho de 2008, elaborada de forma colaborativa pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), com o objetivo de disciplinar a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, em seu artigo 5º, incisos IV, V e VI, afirma o seguinte:

> Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:
> IV - nomear Gestor de Segurança da Informação e Comunicações;
> V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;
>
> VI - instituir Comitê de Segurança da Informação e Comunicações (BRASIL, 2008, p.3);

O aumento do grau de importância do FCS Papéis e responsabilidades a partir do nível de maturidade 2 (Planejado), confirma o que diz o modelo SSE-CCM (2003): “Pratica Genérica 2.1.2 – Atribuir responsabilidades”. Neste modelo, a atribuição de responsabilidades é uma das práticas citadas a partir do nível de maturidade 2.

5.1.10 Grau de importância do FCS Provisão de Recursos

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Provisão de recursos**, foi possível a elaboração da Tabela 16.

Tabela 16. Grau de Importância do FCS Provisão de recursos

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Provisão de recursos	Nível 1	3,8
	Nível 2	4,6
	Nível 3	4,8
	Nível 4	4,8
	Nível 5	4,8

Após o cálculo do GIF do fator Provisão de Recursos, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importância do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}71$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,71 pontos.

Tu et al. (2015), afirma que os custos elevados de implementação dos controles de segurança da informação estão aumentando a pressão sobre os gerentes para distinguir entre os controles que suas organizações precisam e aqueles que são menos críticos. O mesmo autor, informa que organizações mais maduras, concentram seus recursos limitados nas coisas que realmente fazem a diferença entre o sucesso e o fracasso dos objetivos de negócio.

Coelho et al. (2014a), afirma que o processo de estabelecimento da segurança da informação e de sua gestão pode ser realizado quando as seguintes questões estiverem sido respondidas:

> Quanto tempo, recurso financeiro e humano se pretende gastar para atingir os objetivos de segurança desejados? Que recursos estão disponíveis para os objetivos de segurança e o que pode ser feito com os recursos existentes?

Através da disponibilização de recursos para elaboração e manutenção contínua da segurança da informação e o uso adequado desses recursos, é possível alcançar uma GSI eficaz e, consequentemente, um nível de maturidade desejado (ALNATHEER, 2015). Dessa forma, fica evidente que a definição correta dos requisitos e controles de segurança da informação leva a um dimensionamento mais eficaz dos recursos.

5.1.11 Grau de importância do FCS Competência da TI

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Competência da ti**, foi possível a elaboração da Tabela 17.

Tabela 17. Grau de Importância do FCS Competência da TI

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Competência da TI	Nível 1	3,8
	Nível 2	4,6
	Nível 3	4,6
	Nível 4	4,6
	Nível 5	4,8

Concluindo a análise do fator Competência da TI, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importância do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}6\text{x}2)+(4{,}6\text{x}3)+(4{,}6\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}61$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,71 pontos.

O FCS Competência da TI, obteve um GIF de 3,8 no nível de maturidade 1, GIF de 4,6 nos níveis de maturidade 2 ao 4 e GIF de 4,8 no nível de maturidade 5. Dessa forma, evidencia-se mais uma vez, que conforme o nível de maturidade aumenta, o grau de importância do fator também aumenta.

King (2002, apud TU, 2015), afirma que competências da TI está relacionada às capacidades integradas e inter-relacionadas de elementos essenciais da TI para o cumprimento dos objetivos de negócio da organização.

A norma ABNT NBR ISO/IEC 27002, na sua seção 7, Item 7.1, subitem 7.1.1, afirma que:

> Convém que quando um indivíduo seja contratado para desempenhar o papel de segurança da informação, a organização certifique-se de que o candidato:
> a) Tem a competência necessária para executar as atividades de segurança da

> informação;

A norma ABNT NBR ISO/IEC 27001, na sua seção 7, Item 7.2, afirma que:

> A organização deve:
> a) Determinar a competência necessária das pessoas que realizam trabalhos sob o seu controle e que afeta o desempenho da segurança da informação;
> b) Assegurar que essas pessoas são competentes com base na educação, treinamento ou experiência apropriados;
> c) Onde aplicado, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e
> d) Reter informação documentada apropriada como evidência da competência.

Ambas, as principais normas internacionais de GSI, confirmam a importância que o FCS Competências da TI tem sobre segurança da informação das organizações. Tu (2015), confirma essa colocação ao afirmar que o reforço das competências da TI tornou-se crítico para o fortalecimento da gestão da segurança da informação nas organizações.

5.1.12 Grau de importância do FCS Estrutura organizacional

Considerando o grau de importância, apontado pelos respondentes, em relação aos níveis de maturidade (1 ao 5) e aplicada a fórmula estabelecida anteriormente para a apuração do grau de importância do fator (GIF) **Estrutura organizacional**, foi possível a elaboração da Tabela 18.

Tabela 18. Grau de Importância do FCS Competência da TI

Fator Crítico de Sucesso	Nível de maturidade	Grau de Importância do Fator (GIF)
Estrutura organizacional	Nível 1	3,8
	Nível 2	4,4
	Nível 3	4,4
	Nível 4	4,4
	Nível 5	4,6

Concluindo a análise do fator Estrutura Organizacional, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela somatória dos pesos dos níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3,6x1)+(4,4x2)+(4,4x3)+(4,4x4)+(4,6x5)}{15} = 4,41$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,41 pontos.

Estrutura Organizacional, foi o FCS considerado com menor grau de importância em comparação aos demais fatores, segundo os respondentes. Entretanto, o fato desse fator ter recebido um GIGF acima de 4 pontos (numa escala de 1 a 5), significa que é um fator a ser considerado no aprimoramento da maturidade de GSI.

Alexandria e Quoniam (2010), afirma que é necessária a criação de uma estrutura organizacional específica e adequada para administrar a segurança da informação. Dzazali e Zolait (2012), afirmam que uma estrutura organizacional que suporta os objetivos de segurança da informação deve ser flexível, permitindo o envolvimento do usuário e uma maior participação e apoio da administração. Além disso, Solms (2000) informa que a estrutura organizacional deve reconhecer que a segurança da informação é uma das principais funções da organização (apud Dzazali e Zolait, 2012).

A GSI deve estar posicionada adequadamente no organograma da instituição, ou seja, ligada diretamente ao core business (carro-chefe da organização), se reportando diretamente ao nível estratégico (ALEXANDRIA e QUONIAM, 2010). Sêmola (2014), afirma que na estrutura organizacional é importante incluir a formação de um Comitê Corporativo de Segurança da Informação, composto por membros da esfera tático-operacional e por gestores dos processos críticos da organização.

Deste modo, a Estrutura Organizacional, como um FCS para a GSI, deve encorajar a colaboração entre especialistas de segurança da informação e os gestores de negócio, de modo que a missão, metas e objetivos da GSI estejam alinhadas com a missão global, metas e objetivos da organização.

5.2 Classificação dos FCS

Após a análise individual de cada Fator Crítico de Sucesso (FCS) e identificação do seu grau de importância para o aprimoramento de maturidade da Gestão da Segurança da Informação

(GSI), foi possível consolidar toda a informação obtida, de forma a se ter uma visão macro dessa relação: FCS e Maturidade de GSI.

Deste modo, foram identificados quais os FCS devem ser priorizados para que seja possível aprimorar a maturidade de GSI. As etapas seguidas neste trabalho de pesquisa, iniciando pela RSL, levantamento do nível de maturidade de GSI das IFES, identificação dos FCS e do grau de importância para o aprimoramento da maturidade, possibilitou a consolidação dos resultados, demonstrados através da Tabela 19.

Tabela 19. Classificação dos Fatores quanto ao GIGF

Nº	Fator Crítico de Sucesso	Grau de Importância Geral	Classificação
1	Treinamento e conscientização	4,93	1º
2	Gestão de Riscos de Segurança da Informação	4,88	2º
3	Cultura de Segurança da Informação	4,84	3º
4	Apoio da alta gestão	4,83	4º
5	Alinhamento com o negócio	4,80	5º
6	Medição e avaliação da GSI	4,73	6º
7	Gestão de Incidentes de SI	4,73	
8	Política de Segurança da Informação	4,72	7º
9	Papéis e Responsabilidades	4,71	8º
10	Provisão de Recursos	4,71	
11	Competências da TI	4,61	9º
12	Estrutura organizacional	4,41	10º

Dessa forma, entende-se que os responsáveis pela segurança da informação das IFES poderão alcançar os níveis desejados de maturidade em seus processos de segurança da informação investindo esforços e uma atenção redobrada aos FCS mais importantes, e já identificados nesse cenário das Instituições Federais de Ensino Superior (IFES).

Através da classificação dos fatores pelo do Grau de Importância Geral do Fator (GIGF), percebeu-se que os fatores relacionados ao aspecto humanos foram os que receberam os maiores graus de importância. Diversos autores afirmam que o fator humano é o mais importante a ser trabalhado num processo de GSI e que este é o elo mais fraco de todo sistema de gestão de

segurança da informação (MITNICK e SIMON, 2003, apud PARANHOS, 2010; SALEH, 2011; DZAZALI e ZOLAIT, 2012; Tu, 2015).

Segundo Saleh (2011), muitas instituições não classificam seus usuários como ameaças aos seus sistemas, entretanto as ações dos usuários são o ponto de partida para diversos tipos de ataques e, em muitos casos, os próprios usuários podem lançar esses ataques. O mesmo autor ainda afirma que o usuário é classificado como fator humano de alto risco devido ao uso de senhas fracas, suscetibilidade a ataques de engenharia social e falha na manutenção de atualizações de segurança, entre outras vulnerabilidades.

Tu (2015), afirma que a estratégia da segurança da informação de uma organização deve abordar os fatores humanos, através da sensibilização para a segurança e treinamento de segurança de forma abrangente. O mesmo autor, constatou em sua tese de doutorado "*Effective Information Security Management: A Critical Success Factors Analysis*", através de evidencias empíricas, que os fatores humanos podem ser mais importantes do que os controles de segurança para o sucesso da GSI de uma organização.

5.3 Conclusão do capítulo

Este capítulo apresentou os fatores críticos de sucesso (FCS) e seu grau de importância para o aprimoramento da maturidade da gestão da segurança da informação (GSI) das instituições federais de ensino superior (IFES). As 5 melhores instituições avaliadas no diagnóstico de maturidade foram contatadas para responder a um questionário que identificou o grau de importância dos fatores identificados na revisão sistemática. Este resultado possibilitou classificar os fatores quanto a sua importância para o alcance dos níveis de maturidade de GSI.

Dessa forma, a priorização dos fatores elencados neste trabalho de pesquisa é um meio para se aprimorar os níveis de maturidade da gestão da segurança da informação definidos e estudados especificamente no cenário das Instituições Federais de Ensino Superior.

6 CONSIDERAÇÕES FINAIS

Este capítulo tem por objetivo apresentar as conclusões, contribuições, limitações e trabalhos futuros acerca da presente pesquisa.

6.1 Conclusão

O presente trabalho de pesquisa teve como objetivo principal identificar os fatores críticos de sucesso para o aprimoramento da maturidade da Gestão da Segurança da Informação (GSI) das Instituições Federais de Ensino Superior (IFES). Estes fatores foram identificados e classificados quanto ao seu grau de importância para o aprimoramento da maturidade de GSI. Para alcance desses fatores, 4 fases ou etapas foram desenvolvidas no decorrer desta pesquisa.

Primeiramente, na fase 1, foi realizado um levantamento na literatura dos trabalhos científicos já conceituados relacionados a área de segurança da informação e gestão de segurança da informação. Esta fase subdividiu-se em: (1) uma revisão bibliográfica, das principais normas e frameworks, nacionais e internacionais, relacionados ao tema gestão da segurança da informação; (2) análise documental, das principais leis e decretos que tratam do assunto gestão da segurança da informação, no âmbito da Administração Pública Federal e; (3) Revisão Sistemática da Literatura (RSL), que objetivou a busca pelos trabalhos mais relevantes na área da gestão da segurança da informação, maturidade de segurança da informação e principais fatores de sucesso para uma gestão de segurança eficaz. Através deste levantamento, foi possível identificar os trabalhos mais relevantes na área de pesquisa, auxiliando na definição da metodologia, e nas ferramentas utilizadas para conclusão desta pesquisa. A RSL possibilitou também a identificação de 12 fatores considerados críticos para sucesso da GSI. Os fatores coletados foram: **Apoio da Alta Gestão; Treinamento e conscientização; Cultura de Segurança da Informação; Gestão de Riscos; Política de Segurança da Informação; Provisão de Recursos; Papéis e Responsabilidades; Medição e Avaliação, Estrutura Organizacional; Alinhamento com os objetivos de negócio; Gestão de Incidentes de SI e; Competências da TI**. Esses fatores foram

organizados em um ranking, utilizando como critério o número de trabalhos da RSL que o citaram.

A segunda fase da pesquisa foi composta de um levantamento, por meio da definição e aplicação de um questionário, baseado no *Information Security Program Assessment Tool*. Esta ferramenta foi estudada e baixada do site da Biblioteca EDUCAUSE em formato XLSM (Excel) e posteriormente traduzida e disponibilizada por meio eletrônico, através do software LimeSurvey, para as Diretorias de Tecnologia da Informação de 104 IFES. O questionário é composto por um total de 101 perguntas e, em média, levou cerca de 30 minutos para que os respondentes completassem a ferramenta. No total obteve-se 27 respostas completas e satisfatórias, de acordo com o cálculo da amostra realizado.

Na terceira fase da pesquisa baseou-se realizar um diagnóstico de maturidade da gestão da segurança da informação, por meio da análise dos dados coletados na fase 2. A norma utilizada no *Information Security Program Assessment Tool* para definição da maturidade é a ISO/IEC 21827:2008, que avalia os níveis numa escala de 0 a 5, sendo 5 o nível mais alto de maturidade. Foram avaliados o domínio Gestão de Riscos (ISO/IEC 27005) e cada domínio (seção) da ISO/IEC 27002, alcançando uma média, que proporcionou a identificação do nível de maturidade geral de cada IFES. Através desse diagnóstico foi possível obter uma percepção holística da atual situação quanto a maturidade da gestão da segurança da informação das IFES pesquisadas. O que se percebeu foi uma situação crítica quanto a maturidade dessas instituições no domínio gestão de segurança da informação.

Quanto a Maturidade Geral, do total de 27 IFES pesquisas, 59% foram identificadas no nível de maturidade 0 (59%), o que indica que os procedimentos e controles de segurança da informação não estão sendo realizados adequadamente. Apenas 4 intuições (15%) foram identificadas no nível de maturidade 2, onde as práticas base para elaboração de uma GSI eficaz são planejados e gerenciados. Nenhumas das IFES foram identificadas nos níveis de maturidade 3, 4 e 5. Ou seja, nenhumas das IFES pesquisadas possuem seus processos de GSI Bem Definidos, Controlados ou em Melhoria Contínua.

Quanto a Maturidade por Domínio, percebeu-se que os domínios que alcançaram os maiores níveis de maturidade na pesquisa foram: Política de Segurança da Informação;

Segurança nas Operações e; Segurança nas Comunicações. Contudo isso, não garante que seus controles de segurança estejam sendo executados adequadamente, pois a maior parte das instituições foram identificadas nos níveis de maturidade 0 e 1. Já os domínios que obtiveram os menores níveis de maturidade foram: Gestão de Riscos; Aspectos de Segurança da Informação na Gestão da Continuidade dos Negócios e; Conformidade. Esse resultado revela que uma atenção maior deve ser dada a esses domínios, principalmente ao domínio Gestão de Riscos, pois é através deste que são definidos os requisitos necessários para a implementação da gestão da segurança da informação alinhada ao negócio.

Na quarta fase desta pesquisa buscou-se identificar e classificar os fatores mais importantes para o aprimoramento da maturidade de GSI das IFES. Através do diagnóstico de maturidade realizado na fase 3 foi possível classificar as IFES quanto a maturidade de GSI. Desta forma, as 5 IFES com maior nível de maturidade foram contatadas e convidadas a responder a um questionário. Neste questionário os respondentes informaram o grau importância (numa escala likert de 1 a 5) para o alcance dos níveis de maturidade, de cada um dos 12 fatores críticos de sucesso identificados na RSL (fase 1). Como resultado, obteve-se o grau de importância dos 12 fatores. Dentre estes, os 5 fatores com maior grau de importância segundo os respondentes foram: **Treinamento e conscientização; Gestão de Riscos de Segurança da Informação; Cultura de Segurança da Informação; Apoio da alta Gestão; Alinhamento com o negócio.** Dessa forma, os gestores de segurança da informação das IFES poderão focar seus esforços nos fatores com maior grau de importância para o alcance dos níveis de maturidade desejados.

Com isso, quanto aos objetivos propostos para este estudo, considera-se que: (1) os **objetivos específicos** foram atingidos, pois foi realizado todo o levantamento da literatura, através de uma revisão sistemática, servindo de arcabouço teórico para o desenvolvimento do trabalho e identificação dos fatores críticos de sucesso. Adicionalmente, foi realizado um levantamento que possibilitou diagnosticar a atual situação da maturidade em Gestão de Segurança da Informação das Instituições Federais de Ensino Superior; (2) o **objetivo geral** deste trabalho foi alcançado, na medida em que se identificou os Fatores Críticos de Sucesso, e seu grau de importância, para o aprimoramento da maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior.

Desta forma, a questão de pesquisa proposta neste trabalho foi respondida, através dos Fatores Críticos de Sucesso identificados na Revisão Sistemática da Literatura (ver Quadro 9, p. 68) e sua classificação quanto ao grau de importância (ver Tabela 19, p. 148), por meio do questionário aplicado as 5 instituições com maior nível de maturidade em Gestão da Segurança da Informação (ver Tabela 4, p. 83).

6.2 Contribuições e Limitações

Após o resultado obtido com essa pesquisa, algumas contribuições foram identificadas, tais como:

- Apresentação de uma Revisão Sistemática da Literatura, atualizada, com os trabalhos mais relevantes, com base nos critérios de busca;
- Apresentação de um levantamento, através de um diagnóstico, da atual situação da maturidade da gestão de segurança da informação das instituições federais de ensino superior;
- Utilização de práticas profissionais e acadêmicas, em gestão de segurança da informação, que permitam adquirir conhecimento necessário para a elevação da maturidade da Gestão da Segurança da Informação;
- Identificação dos fatores críticos de sucesso para aprimorar o nível de maturidade da gestão de segurança da informação (GSI) das instituições federais de ensino, utilizando as melhores práticas de gestão de TI na área de segurança da informação, internacionalmente reconhecidas e aceitas, tais como as normas internacionais ISO/IEC 27001, 27002, 27005 e a ISO/IEC 21827;

Muitas dificuldade e limitações foram encontradas durante a construção deste trabalho de pesquisa, afetando de alguma forma a sua confecção de maneira mais consistente e precisa. As principais limitações encontradas neste trabalho de pesquisa foram:

- Limitação relacionada a falta literatura específica de fatores críticos de sucesso para elevação de maturidade de gestão da segurança da informação, exigindo que esses fatores fossem identificados neste trabalho;

- Limitação referente a não aplicação dos resultados deste trabalho em instituições que queiram elevar seu nível de maturidade, devido ao pouco tempo restante para sua conclusão;
- Limitação concernente ao número de instituições participantes nesta pesquisa, pois de um universo de 104 instituições, somente 27 foram analisadas.

6.3 Trabalhos Futuros

Como sugestão para pesquisas futuras derivadas deste trabalho, existe a possibilidade da continuidade dos estudos a respeito dos Fatores Críticos de Sucesso para o aprimoramento da maturidade da gestão da segurança da informação propostos nesta pesquisa. Dentre as opções de trabalhos futuros, pode-se destacar:

- Aplicar os resultados dessa pesquisa em uma instituição federal de ensino superior que queira elevar seus níveis de maturidade de gestão da segurança da informação, utilizando o modelo de maturidade ISO/IEC 21827 (SSE-CMM);
- Relacionar os fatores críticos de sucesso e seus graus de importância encontrados nesta pesquisa com outros modelos de maturidade de GSI, como COBIT, O-ISM3, entre outros;
- Elaborar um Sistema de Gestão de Segurança da Informação (SGSI) para as instituições federais de ensino superior, relacionando os fatores críticos de sucesso com as etapas de elaboração do SGSI;
- Comparar os índices de maturidade das instituições federais de ensino superior do Brasil com instituições de ensino de outros países.

REFERÊNCIAS

ABNT. **ABNT Catálogo: Segurança, Qualidade, Padrão e Confiança**. Rio de Janeiro. 2015. Disponível em: < http://www.abntcatalogo.com.br/>. Acesso em: janeiro de 2016.

ABNT. **NBR ISO/IEC 27001:2013: Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação – Requisitos**. Rio de Janeiro: ABNT, 2013.

ABNT. **NBR ISO/IEC 27002:2013: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

ABNT. **NBR ISO/IEC 27002:2013: Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2013.

ABNT. **NBR ISO/IEC 27005:2011: Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação**. Rio de Janeiro: ABNT, 2011.

ALEXANDRIA, João Carlos Soares de; QUONIAM, Luc Marie. **Proposta para a Estruturação da Gestão da Segurança da Informação em um Ambiente de Pesquisa Científica.** 7º CONTECSI – International Conference on Information System and Technology Management, São Paulo, Brasil, 2010.

ALNATHEER, Mohammed A. **Information Security Culture Critical Success Factors.** 12th International Conference on Information Technology – New Generations, Riyadh, Arábia Saudita, 2015.

ALSHAIKH, Moneer; AHMAD, Atif; MAYNARD, Sean B.; SHANTON, Chang. **Towards a Taxonomy of Information Security Management Practices in Organisations.** 25th Australian Conference on Information Systems. 8 – 10 Dec 2014, Auckland, New Zealand, 2014.

ARAUJO, Wagner Junqueira de. **Leis, Decretos e Normas Sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal.** João Pessoa, v.22, p.12-24, 2012.

BRASIL. Portal Brasil. **Autarquias integram a administração pública indireta**. Brasília, DF, 2012. Disponível em: < http://www.brasil.gov.br/governo/2012/04/autarquias >. Acesso em: 15 de dezembro de 2015.

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.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar no 02/IN01/DSIC/GSI/PR**. Metodologia de Gestão da Segurança da Informação e Comunicações. Brasília, DF, GSI/PR, 2008.

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 Politica de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2009.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar no 04/IN01/DSIC/GSI/PR**. Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC. Brasília, DF, GSI/PR, 2013.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar no 09/IN01/DSIC/GSI/PR**. Orientações Específicas para o uso de Recursos Criptográficos em Segurança da Informação e Comunicações. Brasília, DF, GSI/PR, 2014.

BRASIL. Tribunal de Contas da União. **Levantamento de Governança de TI 2008**. 2008.

BRASIL. Tribunal de Contas da União. **Levantamento de Governança de TI 2014**. 2014.

BRAVIM, Jhordano Malacarne. **Benchmark da Governança de TI para as Instituições Federais de Ensino.** Fundação Universidade Federal de Rondônia, Núcleo de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Administração. Porto Velho, RO, 2015.

CHAPIN, D. A.; AKRIDGE, S. **"How can security be measured".** Information Systems Control Journal, v. 2, p. 43-47, 2005.

CHOLEZ, Hervé; GIRARD, Frédéric. **Maturity assessment and process improvement for information security management in small and medium enterprises.** Journal of Software: Evolution and Process. J. Softw. Evol. And Proc. 2014.

COELHO, Flavia Estélia Silva; ARAUJO, Luiz Geraldo Segadas de; BEZERRA, Edson Kowask. **Gestão de Segurança da Informação: NBR 27001 e NBR 27002**. Rio de Janeiro: RNP/ESR, 2014.

COELHO, Roger W.; FERNANDES, Gilberto; PROENÇA, Mario Lemes. **GAIA-MLIS: A Maturiy Model for Information Security.** SECURWARE 2014: The Eighth International Conference on Emerging Security Information, System and Technologies. 2014.

COSTA, Danielle Rocha da. **Fatores Críticos de Sucesso para Elaboração de Politicas de Segurança da Informação e Comunicação no Âmbito da Administração Pública Federal.** Universidade de Brasília. Departamento de Ciência da Computação. Curso de Especialização em

Gestão da Segurança da Informação e Comunicações. Brasília. 2009.

DEY, Manik. **Information Security Management: A Pratical Approach.** AFRICON, 2007.

DISTERER, Georg. **ISSO/IEC 27000, 27001 and 27002 for Information Security Management.** Journal of Information Security, p. 92-100, 2013.

DZAZALI, Suhazimah; ZOLAIT, Ali Hussein. **Assessment of information security maturity: An exploration study of Malaysian public servisse organizations.** Journal of Systems and Information Technology. v. 14 No. 1, p. 23-57, 2012.

FAZENDA, Rodrigo Valle; FAGUNDES, Leonardo Lemes. **Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro.** XI Simpósio Brasileiro de Sistema de Informação, Goiânia, GO, Maio, 2015.

GILLIES, Alan. **Improving the quality of information security management systems with ISO27000.** The TQM Journal. v. 23, No. 4, p. 367-376. 2011

GUNTHER, H. **Como elaborar um projeto de pesquisa** (Série: Planejamento de Pesquisa nas Ciências Sociais, Nº 02). Brasília, DF: UnB, Laboratório de Psicologia Ambiental, 2004.

ITGI – IT Governance Institute. **Cobit 4.1 – Control Objectives for informtion and related Technology – Framework**. Rolling Meadows – USA: [s.n.), 2007. Disponível em < http://www.isaca.org/Knowledge-Center/cobit/Pages/Downloads.aspx>. Acesso em: 10 outubro 2015.

JOHNSON, Luciano; PINTO, José Simão de Paula. **Proposta de um Programa de Segurança da Informação para as Autarquias Federais.** Congresso InfoBrasil TI e Telecom, 2010.

KROLL, Josiane; FONTOURA, Lisandra M.; WAGNER, Rosana; D'ORNELLAS, Marcos C. **Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008.** Rio Grande do Sul: LaCA – UFSM. 2010.

KAUARK, Fabiana; MANHÃES, Fernanda Castro; MEDEIROS, Carlos Henrique. **Metodologia da pesquisa: guia prático**. Itabuna: Via Litterarum, 2010.

LANGE, Joshua de; SOLMS, Rossouw Von; GERBER, Mariana. **Better Information Security Management in Municipalities.** IST-Africa 2015 Conference Proceedings. Paul Cunningham and Miriam Cunningham (Eds). IIMC International Information Management Corporation, 2015.

MANSUR, Ricardo. **Governança de TI: Metodologias, Frameworks, Melhores Práticas**. Rio de Janeiro, Ed. Brasport, 2007.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de Pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados.** 7. Ed. Reimp. São Paulo: Atlas, 2011.

MATRANE, Oussama; TALEA, Mohammed; OKAR, Chafik. **Towards A New Maturity Model for Information Security Management.** International Journal of Advanced Research in Computer Science and Software Engineering, v. 4, issue 6, junho, 2014.

MOETI, Michael; KALEMA, Billy Mathias. **Analytical Hierarchy Process Approach for the Metrics of Information Security Management Framework.** Sixth International Conference on Computational Intelligence, Communication Systems and Networks, 2014.

NORMAN, Azah Anir; YASIN, Norizan Mohd. **Information Systems Security Management (ISSM) Success Factor: Restrospection From the Scholars.** 11th European Conference on Information warfare and security, 2012.

NUNES, Francisco José Barreto; BELCHIOR, Arnaldo Dias. **Um Processo Seguro para o Desenvolvimento de Software.** VI Simpósio Brasileiro em Segurança da Informação e de sistemas Computacionais - SBSEG, 2006.

PARANHOS, Mauricio Machado. **Framework de Segurança da Informação para Medição do Nível de Maturidade das Organizações.** Programa de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação – Mestrado. Brasília-DF, 2010.

PARK, Jung-Oh; KIM, Sang-Geun; CHOI, Beyeong-Hun; JUN, Moon-Seog. **The Study on the Maturity Measurement Method of Security Management for ITSM**. In: Proc. of the International Conference on Convergence and Hybrid Information Technology, p.826-830, 2008.

QUINTELLA, Heitor Luiz Murat de; BRANCO, Marcelo Pereira de Oliveira. **Fatores Críticos de Sucesso em Segurança da Informação em um Órgão da Administração Pública Federal.** II Simpósio Internacional de Gestão de Projetos (II Singep). São Paulo – SP, novembro, 2013.

RIGON, Evandro Alencar; WESTPHALL, Carla Merkle. **Modelo de Avaliação da Maturidade da Segurança da Informação: Information Security Maturity Assessment Model.** Revista Eletrônica da Sistemas de Informação, v. 12, n. 1, artigo 3, jan-mai 2013.

RIGON, Evandro Alencar; WESTPHALL, Carla Merkle; SANTOS, Daniel Ricardo dos; WESTPHALL, Carlos Becker. **A cyclical evaluation modelo f information security maturity.** Information Management & Computer Security, v. 22, p. 265 – 278. 2014

ROCKART, J. F. **Chief executives define their own data needs.** Harward Business Rewiew, v. 57, n.2, p. 81-83. 1979.

SALEH, Malik F. **Information Security Maturity Model.** International Journal of Computer Science and Security (IJCSS), v. 5, issue 3, 2011.

SANTOS, Sabina Aneide Amaral da Mota. **Práticas de Segurança da Informação: um estudo de caso num centro hospitalar.** Porto: Instituto Politécnico do Porto, 2014.

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

SILVA, E.; MENEZES, E. **Metodologia da pesquisa e elaboração de dissertação**. Florianópolis: UFSC, 4. Ed. 2005. Disponível em: <http://soniaa.arq.prof.ufsc.br/roteirosmetodologicos/metpesq.pdf>. Acessado em: 25 Jan. 2016.
SILVA, Claudete Aurora. **Gestão da Segurança da Informação: um olhar a partir da Ciência da Informação.** Campinas, São Paulo, 2009.

SSE-CMM Project (2003) **"Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document"**, Version 3.0. Disponível em: <http://all.net/books/standards/ssecmmv3final.pdf>. Acessado em julho de 2016.

STAMBUL, Mohd Asri Mohamad; RAZALI, Rozilawati. **An Assessment Model of Information Security Implementation Levels.** International Conference on Electrical Engineering an Informatics, Bandung, Indonesia, 2011.

TEIXEIRA FILHO, J. G. A. **MMPE-SI/TI (Gov) - Modelo de Maturidade para Planejamento Estratégico de SI/TI direcionado às Organizações Governamentais Brasileiras baseado em Melhores Práticas**. v. 1 e 2, 2010. Tese (Doutorado em Ciências da Computação) – Universidade Federal de Pernambuco (UFPE), Recife, 2010.

The Open Group. **Open Information Security Management Maturity Model (O-ISM3).** Van Haren Publishing, Zaltbommel, 2011.

TORRES, Marcelo Teixeira; ANHESINE, Marcelo Wilson; AZZOLINI JUNIOR, Walther. **A Gestão da Segurança da Informação e seu Alinhamento Estratégico na Organização.** Interface Tecnológica – v.7 – n.1., 2010.

TU, Zhiling. **Effective Information Security Management: A Critical Success Factors Analysis.** MCMaster University DOCTER OF PHYLOSOPHY, Hamilton, Ontario, 2015.

WASLAWICK, Raul Sidnei. **Metodologia de Pesquisa para ciência da computação.** 2. Ed. Rio de Janeiro: Elsevier, 2014.

WOODHOUSE, Steven. 2008. **An ISMS (Im)-Maturity Capability Model**. In: Proceedings of the 2008 IEEE 8th International Conference on Computer and Information Technology Workshops (CITWORKSHOPS '8). IEEE Computer Society, Washington, DC, USA, p. 242-247, 2008.

YILDIRIM, Ebru Yeniman; AKALP, Gizem; AYTAC, Serpil; BAYRAM, Nuran. **Factors incluencing information security management in small-and-medium-sized enterprises: A case study from Turkey.** International Journal of Information Management, Bursa, Turkey, 2010.

APÊNDICE A. REVISÃO SISTEMÁTICA DA LITERATURA

A Segurança da Informação diz respeito à proteção de determinados dados, com a intenção de preservar seus respectivos valores para uma organização ou um indivíduo (ALVES e MOREIRA, 2012). Para isso, alguns procedimentos são utilizados na tentativa de manter a disponibilidade, integridade, confiabilidade e autenticidade das informações, tais como a Política de Segurança da Informação, gestão de riscos e a própria gestão da segurança da informação.

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, 2013).

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 implantação e revisão de uma Política de Segurança da Informação. 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).

> A revisão sistemática atua como um meio para identificar, avaliar e interpretar toda pesquisa relevante e disponível sobre uma questão de pesquisa específica, tópico ou fenômeno de interesse, fazendo uso de uma metodologia de revisão que seja confiável, rigorosa e que permita auditagem (TEIXEIRA FILHO, 2010, p. 2).

Dessa forma, uma das razões para se utilizar o método de revisão sistemática é buscar fundamentação teórica, obtendo, com isso, agregação de conteúdos que tragam 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).

Através desta sintetização de evidências, pretende-se obter um resultado de maior valor quantitativo, devido ao grande número de fontes primárias de informação selecionadas utilizando metodologia sistemática e explícita, selecionados com o objetivo de minorar erros, evidenciando que estudos e pesquisas com maior precisão de confiabilidade possam ser utilizados na tomada de decisão e aproximação das questões de estudo em pesquisa (TEIXEIRA FILHO, 2010). Assim, a utilização dessa metodologia evita o erro sistemático ou a tendenciosidade e possibilita uma análise mais objetiva dos resultados, facilitando uma síntese conclusiva sobre determinada intervenção (SAMPAIO e MANCINI, 2007).

Segundo Galvão e Pereira (2014), algumas etapas são necessárias para a condução da revisão sistemática: elaboração da pergunta de pesquisa; busca na literatura; seleção dos artigos; extração dos dados; avaliação da qualidade metodológica; síntese dos dados (metanálise); avaliação da qualidade das evidências e redação e publicação dos resultados. Porém, Teixeira Filho (2010) relata que alguns passos sistemáticos atrelados a um conjunto de fases são importantes para conduzir a pesquisa de forma precisa. Dessa forma, todas as etapas relatadas por Galvão e Pereira (2014), são descritas em um protocolo que conduzirá, de forma sistemática, todo o processo da revisão sistemática da literatura.

Segundo Biolchini et al. (2005) e Kitchenham (2004), são estabelecidas três etapas no processo que conduzirá a revisão de literatura: planejamento, execução/desenvolvimento e análise e divulgação dos resultados.

As fases de condução, etapas e demais atividades utilizadas na revisão desse estudo, foram seguidas conforme orientação de Teixeira Filho (2010):

Quadro 1. Fases do Processo de Condução da Revisão Sistemática

REVISÃO SISTEMÁTICA		
Planejamento de Revisão	**Execução da Revisão**	**Análise e divulgação dos resultados**
1. Formulação da questão de pesquisa; 2. Identificação dos estudos; 3. Avaliação crítica dos estudos.	1. Extração dos dados	1. Sintetização dos resultados; 2. Interpretação dos resultados.

Fonte: adaptado de Teixeira Filho (2010)

As seguintes atividades foram desenvolvidas em cada fase da revisão:

Planejamento:

1 - Formulação das questões de pesquisa com foco no objetivo da pesquisa;

2 - Intervenções coerentes e utilização de palavras chaves que levam a resultados positivos em estudos extremamente científicos;

3 - Utilização de critérios específicos que conduzam a uma filtragem de inclusão e exclusão dos estudos.

Execução:

A utilização de formulários específicos ajudou a catalogar e conduzir nas avaliações futuras dos estudos. Esses formulários ajudaram a manter um histórico dos estudos escolhidos para revisão e validação.

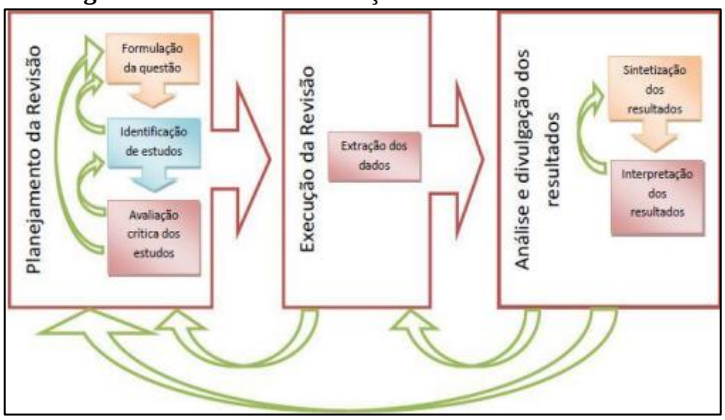
Análise e divulgação:

1 – Os dados são analisados de forma descritiva, levando-se em conta a qualidade dos estudos e relevância nas questões de pesquisa;

2 – Os resultados interpretados tendem estar menos susceptíveis a interesses pessoais, o que asseguram o sentido original dos estudos.

A Figura 1 apresenta o processo de condução da revisão sistemática e suas atividades relacionadas para este trabalho.

Figura 1. Processo de condução da 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.

Para utilização do protocolo nessa pesquisa, foi adaptado um formulário (ver Quadro 2), seguindo modelo de Teixeira Filho (2010), com o objetivo de testar e validar todas as etapas antes de sua utilização.

Quadro 2. Formulário Teste de Protocolo

Formulário de Teste de Protocolo (FTP)		
Responsáveis: Evandro Souza de Paula Cordeiro, Joilson Dantas Siqueira Silva e Orlivaldo Kléber Lima Rios	**Versão:** 02	
O protocolo já foi avaliado por especialistas? Caso positivo, em qual versão ocorreu essa avaliação e quem avaliou?	**SIM (x)**	**NÃO ( )**
Protocolo versão 01 e 02. Avaliador: Prof. Dr. José Gilson Almeida Teixeira Filho		
Foi testado todos os passos descritos no protocolo?	**SIM (x)**	**NÃO ( )**
O protocolo atendia as 03 (três) áreas de segurança da informação, assim foi necessário compreensão, avaliação e aprovação dos pesquisadores.		
Todas as *strings* de busca foram utilizadas para o teste? Caso não tenham sido utilizadas todas as *strings* propostas indicar as que ficaram de fora do teste.	**SIM (x)**	**NÃO ( )**
O uso do operador AND foi utilizado o mínimo possível por que restringia muito o resultado das buscas.		
As *strings* de busca propostas foram aceitas por todos os sites?	**SIM (x)**	**NÃO ( )**
A fonte de busca pesquisada retornou com erro? Caso afirmativo descrever quais foram os problemas encontrados.	**SIM (x)**	**NÃO (x)**
Foi necessário fazer ajustes nas *strings* de busca!		
Foram encontrados problemas na geração dos Bibtex nas fontes de busca pesquisadas. Caso positivo informar a base e descrever os problemas encontrados.	**SIM (x)**	**NÃO ( )**
A base Google Scholar não gerou o arquivo bibtex para todas as strings pesquisadas. O arquivo era gerado individualmente para cada estudo apresentado. Foi necessário criar um arquivo no formato bibtex para unificar os primeiros 115 estudos mais relevantes no período pesquisado.		
Dentre as *strings* testadas, alguma apresentou problemas? Caso tenha encontrado algum problema com as *strings* de busca nas fontes selecionadas, relatar a seguir.	**SIM ( )**	**NÃO (x)**
Todas as *strings* de busca retornaram resultados satisfatório com o que foi inicialmente proposto pela pesquisa? Caso negativo relatar o problema.	**SIM ( )**	**NÃO (x)**
Foi necessário desmembrar as categorias para melhor resultados de busca nas bases/fontes, conforme consta em protocolo.		

Foi necessário incluir outras strings após primeiro testes de consultas?	**SIM (x)**	**NÃO ( )**
Foi adicionada uma nova string (5, 6) após etapa II da revisão, na tentativa de obter maiores resultados em uma linha de pesquisa que ainda não tinha sido capturada com as *strings* iniciais.		
Na etapa de busca nas bases/fontes, houve a necessidade de inserir uma outra fonte de busca. Caso positivo identificar e justificar.	**SIM (x)**	**NÃO ( )**
Finalizado a filtragem de estudos, na Etapa II de seleção de trabalhos, a busca realizada nas bases ACM, IEEEXplore, ScienceDirect e Google Scholar, retornaram uma quantidade de estudos razoável em conformidade com as questões de pesquisa. Assim houve a compreensão de inserir a base Scopus e outras fontes de pesquisa (repositório de dissertações de universidades) em busca de outros estudos primários.		
Na etapa de busca, houve a necessidade de inserir estudos fora do período pesquisado?	**SIM ( )**	**NÃO (x)**

Fonte: adaptado de Teixeira Filho (2010).

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". Essa avaliação deverá ser considerada em análise obedecendo rigorosamente aos critérios de inclusão e exclusão definidos no protocolo de pesquisa.

Assim, para essa pesquisa, 03 (três) pesquisadores (ver Quadro 3) validaram os estudos encontrados nas fontes pesquisadas, seguindo os critérios de inclusão e exclusão estabelecidos no protocolo de revisão.

Quadro 3. Identificação dos pesquisadores da revisão sistemática.

Pesquisadores/Avaliadores dos Estudos	
Avaliador	**Tema de pesquisa**
Evandro Souza de Paula Cordeiro	Maturidade em Gestão de Segurança da Informação.
Orlivaldo Kléber Lima Rios	Política de Segurança da Informação.
Joilson Dantas Siqueira Silva	Gestão de Risco em Segurança da Informação.

Fonte: adaptado de Teixeira Filho (2010).

As fases do processo de revisão sistemática são descritas a seguir:

1. **Fase de Planejamento**

Nesta etapa de revisão, primeiramente, deve-se definir qual será o foco ou qual será a pergunta a ser respondida, ou seja, o que se espera da elaboração e execução de uma revisão sistemática. A partir disso tem-se a base para a obtenção do volume inicial de fontes de informação primárias.

Magge (1998, apud SAMPAIO e MANCINI, 2007) ressalta a importância e necessidade da elaboração do protocolo de revisão, antes do início da pesquisa, incluindo os seguintes itens: palavras chaves de pesquisa, onde os estudos serão 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.

Para a etapa de planejamento, primeiro, foi estabelecido o seguinte objetivo - realizar levantamento bibliográfico e científico em segurança da informação com temas relacionados à Gestão de Risco, Política de Segurança da Informação e Gestão de Segurança da Informação, onde foi desenvolvido um protocolo de revisão adaptado, seguindo modelo de Kitchenham; Biolchini (2004; 2005, apud TEIXEIRA FILHO, 2010), contemplando itens como: questões de pesquisa, critérios de seleção de fontes, método de pesquisa, critérios de inclusão e exclusão, definição e procedimentos para seleção de trabalhos.

2. Fase de Execução

A etapa de execução envolve a seleção e validação das fontes primárias de informação através dos critérios de inclusão e exclusão levantados na etapa de planejamento, ou seja, deve ser aplicado os critérios nas fontes de informações pesquisadas, a fim de filtrar o que está de acordo com os critérios pré-estabelecidos.

Nessa etapa foi realizada toda a condução criteriosa dos estudos primários, conforme estabelecido no protocolo já citado. Para o desenvolvimento e execução da revisão sistemática, todas as atividades de seleção e leitura foram compreendidas entre o período de 17/12/2015 à 06/05/2016. 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 seguir é mostrado o resultado de todas as etapas de execução da revisão e os quantitativos de estudos encontrados e selecionados (ver Tabela 1).

Toda análise nas etapas apresentadas serviu como parâmetro para a extração dos dados que serão exibidos na Etapa de Resultados.

Tabela 1. Etapas da Revisão Sistemática

Base	Etapa 1. Busca nas bases	Etapa 2. Leitura Título	Etapa 3. Leitura Resumo	Etapa 4. Leitura Int. e Conc.	Etapa 5. Leitura Completa
ACM	368	11	3	1	1
IEEE Xplore	327	35	19	6	4
Science Direct	509	30	11	6	1
Google Scholar	114	44	25	19	15
Scopus	94	0	0	0	0
Outros	8	0	0	0	0
Total	**1420**	**120**	**58**	**32**	**21**

Na etapa 2, conforme apresentado na Tabela 1, foram lidos os títulos e selecionados apenas os que tinham relevância com o estudo em pesquisa. Por meio dessa filtragem, foram selecionados 120 estudos dos 1420 que retornaram por meio da busca na etapa 1. 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 58 estudos dos 120 estudos filtrados na etapa 2. Na etapa 4, foram lidas a introdução e a conclusão dos estudos da etapa anterior, passando por outra filtragem e sendo selecionados apenas os estudos que tivessem relação com as questões de pesquisa. Dessa forma, foram selecionados 32 dos 58 estudos selecionados na etapa anterior.

A etapa 5 serviu para realizar a leitura completa de todos os estudos selecionados na etapa anterior, nesta foram selecionados 21 trabalhos, destacando pontos relevantes de acordo com os propósitos estabelecidos pela pesquisa, ou seja, verificar e compreender as melhores práticas em gestão da segurança da informação de modo a encontrar os principais fatores para o aprimoramento da maturidade da gestão da segurança da informação.

3. Fase de análise e divulgação dos resultados

A etapa 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. Essa fase fornece subsídios para que a pergunta definida na Etapa de Planejamento seja respondida e os estudos primários que atenderam ao propósito da revisão sistemática sejam analisados criticamente e sintetizados no formulário de aprovação dos trabalhos - FAT, através da

preparação de resumos contendo as discussões e observações dos autores acerca de cada estudo (KITCHENHAM et al., 2007).

Quadro 4. Formulário de Aprovação de Trabalho (FAT).

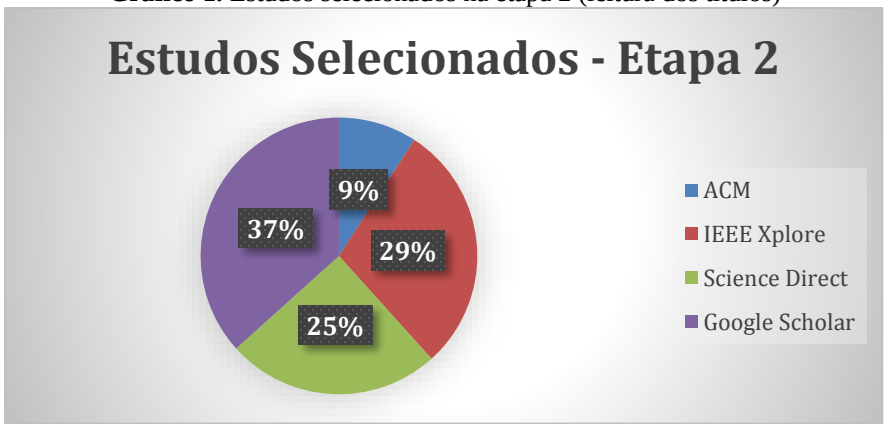
Ano	Trabalho	Tipo	Autor	Base
2010	A Gestão da Segurança da Informação e seu Alinhamento Estratégico na Organização	Artigo	TORRES, Marcelo Teixeira and ANHESINE, Marcelo Wilson and JúNIOR, Walther AZZOLINI	Google Scholar
2010	Framework de Segurança da Informação para Medição do Nível de Maturidade das Organizações	Dissertação	Paranhos, Maurício Machado	Google Scholar
2010	Proposal to Structure the Information Security Management in a Scientific Research Environment	Artigo	Alexandria, João Carlos Soares de and Quoniam, Luc Marie	Google Scholar
2010	Proposta de um Programa de Segurança da Informação para as Autarquias Federais	Artigo	Johnson, Luciano and Pinto, JosÉ Simão de Paula	Google Scholar
2011	Improving the quality of information security management systems with ISO27000	Artigo	Sinha, Madhav and Gillies, Alan	Google Scholar
2011	Information Security Maturity Model	Artigo	Saleh, Malik F	Google Scholar
2011	An assessment model of information security implementation levels	Artigo	Stambul, M.A.M. and Razali, R.	IEEE
2011	Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey	Artigo	Ebru Yeniman Yildirim and Gizem Akalp and Serpil Aytac and Nuran Bayram	Science Direct
2012	Assessment of information security maturity: an exploration study of Malaysian public service organizations	Artigo	Dzazali, Suhazimah and Hussein Zolait, Ali	Google Scholar
2012	Information Systems Security Management (ISSM) Success Factors: Retrospection from the Scholars	Artigo	Norman, Azah Anir and Yasin, Norizan Mohd	Google Scholar
2013	Iso/iec 27000, 27001 and 27002 for information security management	Artigo	Disterer, Georg	Google Scholar
2014	Fatores Críticos de Sucesso em Segurança da Informação em um Órgão da Administração Pública Federal	Artigo	Quintella, Heitor Luiz Murat de Meirelles and Branco, Marcelo Pereira de Oliveira	Google Scholar
2014	GAIA-MLIS: A Maturity Model for Information Security	Artigo	Coelho, Roger W and Fernandes Jr, Gilberto and Proen{\c{c	Google Scholar
2014	Maturity assessment and process improvement for information security management in small and medium enterprises	Artigo	Cholez, Herve and Girard, Frederic	Google Scholar
2014	Towards a Taxonomy of Information Security Management Practices in Organisations	Artigo	Alshaikh, Moneer and Ahmad, Atif and Maynard, Sean B and Chang, Shanton	Google Scholar
2014	A cyclical evaluation model of information security maturity	Artigo	Alencar Rigon, Evandro and Merkle Westphall, Carla and Ricardo dos Santos, Daniel and Becker Westphall, Carlos	Google Scholar
2014	Analytical Hierarchy Process Approach for the Metrics of Information Security	Artigo	Moeti, M. and Kalema, B.M.	IEEE

	Management Framework			
2015	Analysis of the Challenges Faced in Establishing and Maintaining an Information Security Management System on the Brazilian Scene	Artigo	Fazenda, Rodrigo Valle and Fagundes, Leonardo Lemes	ACM
2015	Information Security Culture Critical Success Factors	Artigo	Alnatheer, M.A.	IEEE
2015	Better information security management in municipalities	Artigo	De Lange, J. and Von Solms, R. and Gerber, M.	IEEE
2015	Information Security Management: A Critical Success Factors Analysis	Tese	Tu, Zhiling	Google Scholar

Fonte: adaptado de Teixeira Filho (2010)

Geralmente, nessa fase da revisão, os resultados são exibidos em forma de tabelas ou gráficos, tendo como base as fontes de informação primária selecionada (SAMPAIO e MANCINI, 2007). O Gráfico 1 exibe os resultados dos estudos com a relevância primária extraídos na etapa 2. O gráfico tem por objetivo apresentar as informações quantitativas referentes aos trabalhos selecionados nessa fase. Foram selecionados 120 estudos, sendo 9% advindos da base ACM (11 estudos); 29% advindos da base IEEE Xplore (35 estudos); 25% advindos da base Science Direct (30 estudos); 37% advindos da base Google Scholar (44 estudos).

Gráfico 1. Estudos selecionados na etapa 2 (leitura dos títulos)



O Gráfico 2 apresenta informações referentes ao número de trabalhos selecionados na etapa 5 e divididos por ano. Considerando que a busca da pesquisa foi planejada entre o período de janeiro de 2010 a dezembro de 2015, verifica-se que o ano de 2014 apresentou o maior número de estudos relevantes (06 estudos) e que o ano de 2013 apresentou o menor número (01 estudo). Analisando o Gráfico 3, percebe-se uma certa queda nos anos de 2012 a 2013 quanto ao

tema gestão de segurança da informação, porém em 2014, os estudos cresceram novamente e a faixa se manteve em 2015, com uma leve queda.

Gráfico 2. Quantidade de estudos selecionados por ano

Desta forma, algumas conclusões podem ser elaboradas quanto ao resultado apontado pela revisão sistemática e os estudos relevantes na área de segurança da informação e gestão da segurança da informação:

- Não há na literatura de segurança da informação atual uma definição de fatores críticos de sucesso específicos para o aprimoramento da maturidade da gestão da segurança da informação. O que se encontrou foram fatores considerados críticos para a gestão da segurança de forma geral;
- Modelos de maturidade conceituados e existentes na literatura já estão definidos, entretanto não definem ou apontam o grau de importância dos fatores críticos para o alcance dos níveis de maturidade desejados pelas instituições;
- Modelos de maturidade como COBIT, NIST, CMMI, O-ISM3, SSE-CMM entre outros, são largamente utilizados por instituições públicas e privadas, para avaliação e aprimoramento da maturidade;

- Os órgãos públicos, em sua maioria, seguem a Norma Complementar 02/IN01/DSIC/GSIPR como metodologia de gestão de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.

O que se percebeu durante o estudo de revisão sistemática é o investimento em pesquisas em gestão de segurança da informação com foco na elevação da maturidade e nos fatores críticos de forma separada. Nenhum trabalho foi encontrado com foco específico dos fatores responsáveis pelo aprimoramento da maturidade da gestão da segurança da informação. Todos os estudos selecionados nessa pesquisa da revisão sistemática foram lidos integralmente e seus resumos no Item 2.4.1 deste trabalho.

<table>
<tr><td colspan="2">PROTOCOLO DE REVISÃO SISTEMÁTICA (PRS)</td><td>Versão: 02</td></tr>
<tr><td>Foco da pesquisa</td><td colspan="2">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.</td></tr>
<tr><td rowspan="2">Amplitude da revisão sistemática</td><td colspan="2">Questão de pesquisa

Q1 – Quais Fatores Críticos de Sucesso podem aprimorar o nível de maturidade da Gestão da Segurança da Informação das Instituições Federais de Ensino Superior?

Q2 – Quais as melhores práticas em gestão de TI para o desenvolvimento e implantação de políticas de segurança da informação?

Q3 - Como realizar o gerenciamento dos riscos de segurança da informação para atender os riscos que afetam os negócios de forma eficiente, apropriada e condizente com a realidade das instituições de ensino superior da rede pública federal?</td></tr>
<tr><td colspan="2">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.</td></tr>
</table>

Os idiomas pesquisados serão o inglês e português, acreditando que bons materiais da literatura cientifica 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;	- Information security, information security maturity model, level of information security maturity, organizational maturity of information security;
- Política de segurança da informação, Gerenciamento de política de segurança da informação, ISO/IEC 27002, ITIL, COBIT, boas práticas;	- Information security policy, information security policy management, ISO / IEC 27002; ISO / IEC 27005; ITIL, COBIT, best practices,
- 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	- 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 Maturidade em segurança da Informação.

Efeito

Com a referida pesquisa pretende-se alcançar as seguintes ações:

- criação de um modelo de Gestão de Riscos de Segurança da Informação que possa direcionar as Instituições Públicas de Ensino Superior na busca pela implantação de um modelo de Gestão de Riscos de acordo com as peculiaridades e especificidades dessas instituições.
- atinar informações para que políticas de segurança tenham suas implementações orientadas a partir de práticas de gestão de TI, reconhecida internacionalmente, tais como ISO/IEC 27002, ITIL e COBIT.
- propor que a maturidade da gestão de segurança da informação possam ser aprimoradas e

	direcionados de maneira mais condizente com as melhores práticas internacionais e necessidades do negócio. **Métricas de Resultados** Os resultados obtidos com este trabalho serão mensurados através da abordagem GQM. **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 ensino; elaboração de um modelo a ser utilizado nas Instituições Públicas de Ensino Superior da rede Federal para a Gestão de Riscos de Segurança da Informação .
Seleção das fontes de pesquisa	**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 íntegra 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.
	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).
	Idiomas de estudos Português e Inglês.

<table>
<tr><td rowspan="4"></td><td rowspan="4">Identificação das fontes</td><td colspan="2">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;</td></tr>
<tr><td colspan="2">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:</td></tr>
<tr><td>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"</td><td>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 27005”)

6.</td></tr>
</table>

<table>
<tr><td rowspan="2"></td><td rowspan="2"></td><td>- "Gestão de risco "AND (Modelos OR framework OR metodologia OR “ISO/IEC 27005”)

3.
- COBIT OR ITIL OR “ISOIEC 27002”</td><td>- COBIT OR ITIL OR ISO/IEC 27002</td></tr>
<tr><td colspan="2">Lista de fontes de busca
ACM Portal, IEEE Xplore, ScienceDirect, Google Scholar, Scopus, outras (repositório de universidades).</td></tr>
<tr><td rowspan="3">Seleção dos trabalhos pesquisados</td><td colspan="3">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;</td></tr>
<tr><td colspan="3">Procedimentos para seleção dos trabalhos
Serão aplicadas cinco etapas para a seleção definitiva dos estudos a serem avaliados no contexto da pesquisa. Os seguintes procedimentos vão proporcionar filtrar os trabalhos mais relevantes para a pesquisa:</td></tr>
</table>

- ETAPA I – Realizar pesquisas de acordo com as *strings* de busca definidas para a pesquisa;
- ETAPA II – Os trabalhos retornados serão inicialmente avaliados segundo o título, sem a necessidade de fichar no formulário de condução da revisão. Caso o título seja relevante ao contexto da pesquisa, o trabalho será potencialmente selecionado para a próxima etapa, caso contrário ele será excluído;
- ETAPA III – Dos estudos pré-selecionados na primeira etapa, uma nova pesquisa (busca) será realizada, aplicando-se *strings* de busca de forma mais refinada. Os trabalhos que retornarem resultados com esse refinamento vão ter seus resumos (*abstract*) lidos, depois serão selecionados para a próxima etapa e fichados no formulário de condução da revisão. Caso contrário eles serão excluídos;
- ETAPA IV – Na próxima etapa será realizada uma leitura da introdução e conclusão de cada trabalho pré-selecionado. Se houver relevância com o contexto da pesquisa, o trabalho será selecionado para a próxima etapa e fichado no formulário de condução da revisão. Caso contrário ele será excluído;
- ETAPA V – A última etapa aprimora a seleção principalmente, porque o trabalho será completamente lido, analisado e criticado haja vista a relevância contextual e filtro proporcionado pelas etapas anteriores. Nesta última etapa o trabalho será considerado apto e será fichado no formulário de aprovação dos estudos.

APÊNDICE B. CÁLCULO DO GRAU DE IMPORTÂNCIA DOS FATORES

Para identificação do grau de importância dos FCS por nível de maturidade, foi utilizado o cálculo da média ponderada, conforme trabalho de Oliveira (2016). Multiplicou-se as pontuações das respostas (PR) com a quantidade de respondentes (QR), somando-a e, posteriormente, dividindo-se o resultado pelo número de respondentes (NR), o que conferiu o grau de importância do fator (GIF).

$$\mathrm{GIF} = \frac{\sum \mathrm{PRxQR}}{\mathrm{NR}}$$

Considerando que, conforme o nível de maturidade aumenta, a maturidade e a complexidade dos processos de segurança também aumentam, foi atribuído um peso para cada nível de maturidade, de modo que o grau de importância dado aos fatores pelos respondentes obtivesse um peso diferente em cada nível de maturidade, conforme Tabela 1.

Tabela 1. Peso dos níveis de maturidade

Nível 1	Nível 2	Nível 3	Nível 4	Nível 5
1	**2**	**3**	**4**	**5**

Desta forma, o grau de importância geral do fator (GIGF), foi alcançado através da soma da pontuação média do grau de importância do fator (GIF) multiplicado pelo peso do nível de maturidade (PN), dividida pela somatória dos pesos dos níveis (SPN), por meio da seguinte fórmula:

$$\mathrm{GIGF} = \frac{\sum (\mathrm{GIFxPN})}{\mathrm{SPN}}$$

Estabelecidas as fórmulas foi possível identificar o grau de importância dos FCS para os níveis de maturidade 1 ao 5, e posteriormente o grau de importância geral de cada FCS para o aprimoramento da maturidade de GSI, demonstrados nos tópicos a seguir.

Grau de importância do FCS Apoio da Alta Gestão

A Tabela 2 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Apoio da alta gestão, para cada um dos 5 níveis de maturidade.

Tabela 2. Grau de importância do FCS Apoio da Alta gestão

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Apoio da alta gestão	Nível 1	Sem importância	1	0	0	**4,4**
		Pouco importante	2	0	0	
		Indiferente	3	1	3	
		Importante	4	1	4	
		Muito importante	5	3	15	
		Total		**5**	**22**	
	Nível 2	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 3	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	
	Nível 4	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	1	3	
		Importante	4	0	0	
		Muito importante	5	4	20	
		Total		**5**	**23**	
	Nível 5	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	

Fonte: adaptado de Oliveira (2016)

Desta forma, o grau de importância do FCS Apoio da Alta Gestão, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Apoio da Alta Gestão - nível de maturidade 1: 4,4 pontos
- Apoio da Alta Gestão - nível de maturidade 2: 4,8 pontos
- Apoio da Alta Gestão - nível de maturidade 3: 5,0 pontos
- Apoio da Alta Gestão - nível de maturidade 4: 4,6 pontos

- Apoio da Alta Gestão - nível de maturidade 5: 5,0 pontos

Concluindo a análise do fator Apoio da Alta Gestão, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}4\text{x}1)+(4{,}8\text{x}2)+(5{,}0\text{x}3)+(4{,}6\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}83$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,83 pontos.

Grau de importância do FCS Treinamento e Conscientização

A Tabela 3 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Treinamento e Conscientização, para cada um dos 5 níveis de maturidade.

Tabela 3. Grau de importância do FCS Treinamento e Conscientização

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Treinamento e Conscientização	Nível 1	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 2	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**5**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	

		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	
	Nível 5	Sem importância	1	0	0	**5**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	

Fonte: adaptado de Oliveira (2016)

Com isso, o grau de importância do FCS Treinamento e Conscientização, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Treinamento e Conscientização - nível de maturidade 1: 4,6 pontos
- Treinamento e Conscientização - nível de maturidade 2: 5,0 pontos
- Treinamento e Conscientização - nível de maturidade 3: 4,8 pontos
- Treinamento e Conscientização - nível de maturidade 4: 5,0 pontos
- Treinamento e Conscientização - nível de maturidade 5: 5,0 pontos

Concluindo a análise do fator Treinamento e Conscientização, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importância do fator multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}6\text{x}1)+(5{,}0\text{x}2)+(4{,}8\text{x}3)+(5{,}0\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}93$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,93 pontos.

Grau de importância do FCS Cultura de Segurança da Informação

A Tabela 4 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Cultura de Segurança da Informação, para cada um dos 5 níveis de maturidade.

Tabela 4. Grau de importância do FCS Cultura de Segurança da Informação

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Cultura de Segurança da Informação	Nível 1	Sem importância	1	0	0	**4,4**
		Pouco importante	2	0	0	
		Indiferente	3	1	3	
		Importante	4	1	4	
		Muito importante	5	3	15	
		Total		**5**	**22**	
	Nível 2	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 5	Sem importância	1	0	0	**5**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	

Fonte: adaptado de Oliveira (2016)

Deste modo, o grau de importância do FCS Cultura de Segurança da Informação, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Cultura de Segurança da Informação - nível de maturidade 1: 4,4 pontos
- Cultura de Segurança da Informação - nível de maturidade 2: 4,8 pontos
- Cultura de Segurança da Informação - nível de maturidade 3: 4,8 pontos
- Cultura de Segurança da Informação - nível de maturidade 4: 4,8 pontos
- Cultura de Segurança da Informação - nível de maturidade 5: 5,0 pontos

Concluindo a análise do fator Cultura de Segurança da Informação, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis, conforme Figura 11.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}4\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}84$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,84 pontos.

Grau de importância do FCS Gestão de Riscos

A Tabela 5 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Gestão de Riscos, para cada um dos 5 níveis de maturidade

Tabela 5. Grau de importância do FCS Gestão de Riscos

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Gestão de Riscos	Nível 1	Sem importância	1	0	0	**4,2**
		Pouco importante	2	1	2	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	3	15	
		Total		**5**	**21**	
	Nível 2	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	5	25	

		Total		**5**	**25**	
	Nível 5	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	

Fonte: adaptado de Oliveira (2016)

Assim sendo, o grau de importância do FCS Gestão de Riscos, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Cultura de Segurança da Informação - nível de maturidade 1: 4,2 pontos
- Cultura de Segurança da Informação - nível de maturidade 2: 4,8 pontos
- Cultura de Segurança da Informação - nível de maturidade 3: 4,8 pontos
- Cultura de Segurança da Informação - nível de maturidade 4: 5,0 pontos
- Cultura de Segurança da Informação - nível de maturidade 5: 5,0 pontos

Concluindo a análise do fator Gestão de Riscos, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}2\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(5{,}0\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}88$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,88 pontos.

Grau de importância do FCS Política de Segurança

A Tabela 6 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Política de Segurança, para cada um dos 5 níveis de maturidade.

Tabela 6. Grau de importância do FCS Política de Segurança

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Política de Segurança	Nível 1	Sem importância	1	0	0	**4,0**
		Pouco importante	2	1	2	
		Indiferente	3	0	0	

		Importante	4	2	8	
		Muito importante	5	2	10	
		Total		**5**	**20**	
	Nível 2	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 5	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

Fonte: adaptado de Oliveira (2016)

Deste modo, o grau de importância do FCS Política de Segurança, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Política de Segurança - nível de maturidade 1: 4,0 pontos
- Política de Segurança - nível de maturidade 2: 4,6 pontos
- Política de Segurança - nível de maturidade 3: 4,8 pontos
- Política de Segurança - nível de maturidade 4: 4,8 pontos
- Política de Segurança - nível de maturidade 5: 4,8 pontos

Concluindo a análise do fator Política de Segurança, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(4{,}0\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}72$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,72 pontos.

Grau de importância do FCS Provisão de Recursos

A Tabela 7 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Provisão de Recursos, para cada um dos 5 níveis de maturidade.

Tabela 7. Grau de importância do FCS Provisão de Recursos

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Provisão de Recursos	Nível 1	Sem importância	1	0	0	**3,8**
		Pouco importante	2	0	0	
		Indiferente	3	2	6	
		Importante	4	2	8	
		Muito importante	5	1	5	
		Total		**5**	**19**	
	Nível 2	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 5	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

Fonte: adaptado de Oliveira (2016)

Desta forma, o grau de importância do FCS Provisão de Recursos, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Provisão de Recursos - nível de maturidade 1: 3,8 pontos
- Provisão de Recursos - nível de maturidade 2: 4,6 pontos
- Provisão de Recursos - nível de maturidade 3: 4,8 pontos
- Provisão de Recursos - nível de maturidade 4: 4,8 pontos
- Provisão de Recursos - nível de maturidade 5: 4,8 pontos

Concluindo a análise do fator Provisão de Recursos, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importância do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}71$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,71 pontos.

Grau de importância do FCS Estrutura Organizacional

A Tabela 8 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Estrutura Organizacional, para cada um dos 5 níveis de maturidade.

Tabela 8. Grau de importância do FCS Estrutura Organizacional

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Estrutura Organizacional	Nível 1	Sem importância	1	0	0	**3,6**
		Pouco importante	2	1	2	
		Indiferente	3	1	3	
		Importante	4	2	8	
		Muito importante	5	1	5	
		Total		**5**	**18**	
	Nível 2	Sem importância	1	0	0	**4,4**
		Pouco importante	2	0	0	
		Indiferente	3	1	3	
		Importante	4	1	4	

		Muito importante	5	3	15	
		Total		**5**	**22**	
	Nível 3	Sem importância	1	0	0	**4,4**
		Pouco importante	2	0	0	
		Indiferente	3	1	3	
		Importante	4	1	4	
		Muito importante	5	3	15	
		Total		**5**	**22**	
	Nível 4	Sem importância	1	0	0	**4,4**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	3	12	
		Muito importante	5	2	10	
		Total		**5**	**22**	
	Nível 5	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	

Fonte: adaptado de Oliveira (2016)

Com isso, o grau de importância do FCS Estrutura Organizacional, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Estrutura Organizacional - nível de maturidade 1: 3,6 pontos
- Estrutura Organizacional - nível de maturidade 2: 4,4 pontos
- Estrutura Organizacional - nível de maturidade 3: 4,4 pontos
- Estrutura Organizacional - nível de maturidade 4: 4,4 pontos
- Estrutura Organizacional - nível de maturidade 5: 4,6 pontos

Concluindo a análise do fator Estrutura Organizacional, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\mathrm{GIGF} = \frac{\sum(\mathrm{GIFxPN})}{\mathrm{SPN}} = \frac{(3{,}6\mathrm{x}1)+(4{,}4\mathrm{x}2)+(4{,}4\mathrm{x}3)+(4{,}4\mathrm{x}4)+(4{,}6\mathrm{x}5)}{15} = 4{,}41$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,41 pontos.

Grau de importância do FCS Alinhamento com o Negócio

A Tabela 9 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Alinhamento com o Negócio, para cada um dos 5 níveis de maturidade.

Tabela 9. Grau de importância do FCS Alinhamento com o Negócio

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Alinhamento com o Negócio	Nível 1	Sem importância	1	0	0	**3,4**
		Pouco importante	2	1	2	
		Indiferente	3	2	6	
		Importante	4	1	4	
		Muito importante	5	1	5	
		Total		**5**	**17**	
	Nível 2	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	
	Nível 5	Sem importância	1	0	0	**5,0**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	0	0	
		Muito importante	5	5	25	
		Total		**5**	**25**	

Fonte: adaptado de Oliveira (2016)

Assim sendo, o grau de importância do FCS Alinhamento com o Negócio, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Alinhamento com os Negócios - nível de maturidade 1: 3,4 pontos
- Alinhamento com os Negócios - nível de maturidade 2: 4,6 pontos
- Alinhamento com os Negócios - nível de maturidade 3: 4,8 pontos
- Alinhamento com os Negócios - nível de maturidade 4: 5,0 pontos

- Alinhamento com os Negócios - nível de maturidade 5: 5,0 pontos

Concluindo a análise do fator Alinhamento com o Negócio, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}4\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(5{,}0\text{x}4)+(5{,}0\text{x}5)}{15} = 4{,}80$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,80 pontos.

Grau de importância do FCS Medição e Avaliação

A Tabela 10 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Medição e Avaliação, para cada um dos 5 níveis de maturidade.

Tabela 10. Grau de importância do FCS Medição e Avaliação

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Medição e Avaliação	Nível 1	Sem importância	1	0	0	**3,8**
		Pouco importante	2	1	2	
		Indiferente	3	0	0	
		Importante	4	3	12	
		Muito importante	5	1	5	
		Total		**5**	**19**	
	Nível 2	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	

		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 5	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

Fonte: adaptado de Oliveira (2016)

Deste modo, o grau de importancia do FCS Medição e Avaliação, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Medição e Avaliação - nível de maturidade 1: 3,8 pontos
- Medição e Avaliação - nível de maturidade 2: 4,8 pontos
- Medição e Avaliação - nível de maturidade 3: 4,8 pontos
- Medição e Avaliação - nível de maturidade 4: 4,8 pontos
- Medição e Avaliação - nível de maturidade 5: 4,8 pontos

Concluindo a análise do fator Medição e Avaliação, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}73$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,73 pontos.

Grau de importância do FCS Papéis e Responsabilidade

A Tabela 11 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Papéis e Responsabilidades, para cada um dos 5 níveis de maturidade.

Tabela 11. Grau de importância do FCS Papéis e Responsabilidades

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Papéis e	Nível 1	Sem importância	1	0	0	**3,8**

Responsabilidades		Pouco importante	2	1	2	
		Indiferente	3	0	0	
		Importante	4	3	12	
		Muito importante	5	1	5	
		Total		**5**	**19**	
	Nível 2	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 5	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

Fonte: adaptado de Oliveira (2016)

Deste forma, o grau de importância do FCS Papéis e Responsabilidades, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Papéis e Responsabilidades - nível de maturidade 1: 3,8 pontos
- Papéis e Responsabilidades - nível de maturidade 2: 4,6 pontos
- Papéis e Responsabilidades - nível de maturidade 3: 4,8 pontos
- Papéis e Responsabilidades - nível de maturidade 4: 4,8 pontos
- Papéis e Responsabilidades - nível de maturidade 5: 4,8 pontos

Concluindo a análise do fator Papéis e Responsabilidades, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}6\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}71$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,71 pontos.

Grau de importância do FCS Competência da TI

A Tabela 12 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Competência da TI, para cada um dos 5 níveis de maturidade.

Tabela 12. Grau de importância do FCS Competência da TI

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Competência da TI	Nível 1	Sem importância	1	0	0	**3,8**
		Pouco importante	2	1	2	
		Indiferente	3	0	0	
		Importante	4	3	12	
		Muito importante	5	1	5	
		Total		**5**	**19**	
	Nível 2	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 3	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 4	Sem importância	1	0	0	**4,6**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	2	8	
		Muito importante	5	3	15	
		Total		**5**	**23**	
	Nível 5	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

Fonte: adaptado de Oliveira (2016)

Com isso, o grau de importância do FCS Competência da TI, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Competência da TI - nível de maturidade 1: 3,8 pontos
- Competência da TI - nível de maturidade 2: 4,6 pontos
- Competência da TI - nível de maturidade 3: 4,6 pontos
- Competência da TI - nível de maturidade 4: 4,6 pontos
- Competência da TI - nível de maturidade 5: 4,8 pontos

Concluindo a análise do fator Competência da TI, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}6\text{x}2)+(4{,}6\text{x}3)+(4{,}6\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}61$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,71 pontos.

Grau de Importância do FCS Gestão de Incidentes

A Tabela 13 apresenta o resultado do questionário aplicado acerca do Grau de Importância do FCS (GIF) Gestão de Incidentes para cada um dos 5 níveis de maturidade.

Tabela 13. Grau de importância do FCS Gestão de Incidentes

Fator Crítico de Sucesso	Fator Crítico de Sucesso	Grau de Importância	PR	NR	Total	GIF
Gestão de Incidentes	Nível 1	Sem importância	1	0	0	**3,8**
		Pouco importante	2	0	0	
		Indiferente	3	2	6	
		Importante	4	2	8	
		Muito importante	5	1	5	
		Total		**5**	**19**	
	Nível 2	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

	Nível 3	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 4	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	
	Nível 5	Sem importância	1	0	0	**4,8**
		Pouco importante	2	0	0	
		Indiferente	3	0	0	
		Importante	4	1	4	
		Muito importante	5	4	20	
		Total		**5**	**24**	

Fonte: adaptado de Oliveira (2016)

Deste modo, o grau de importância do FCS Gestão de Incidentes, para cada um dos 5 níveis de maturidade de GSI, de acordo com os respondentes foi de:

- Competência da TI - nível de maturidade 1: 3,8 pontos
- Competência da TI - nível de maturidade 2: 4,8 pontos
- Competência da TI - nível de maturidade 3: 4,8 pontos
- Competência da TI - nível de maturidade 4: 4,8 pontos
- Competência da TI - nível de maturidade 5: 4,8 pontos

Concluindo a análise do fator Gestão de Incidentes, foi calculado o grau de importância geral para este fator (GIGF), produto do somatório da pontuação do grau de importancia do fator, multiplicado pelo peso dos níveis de maturidade, dividido pela quantidade de níveis.

$$\text{GIGF} = \frac{\sum (\text{GIFxPN})}{\text{SPN}} = \frac{(3{,}8\text{x}1)+(4{,}8\text{x}2)+(4{,}8\text{x}3)+(4{,}8\text{x}4)+(4{,}8\text{x}5)}{15} = 4{,}73$$

Com isso, foi possível obter o grau de importância geral do fator em análise apurado nesta pesquisa, obtendo 4,73 pontos.

ANEXO I. QUESTIONÁRIO PARA COLETA DE DADOS

Este questionário foi traduzido do original *Information Security Program Assessment Tool* da EDUCAUSE.

A *Information Security Program Assesment Tool* foi a ferramenta escolhida e utilizada neste trabalho de pesquisa para identificação do nível de maturidade de GSI das IFES. Esta escolha se deu pelo fato dessa "ferramenta" ter sido desenvolvida especificamente para avaliar a maturidade dos programas de segurança da informação de Instituições de Ensino Superior e por ser baseada em normas de renome e internacionalmente reconhecidas como a ISO/IEC 21827:2008 e a ISO/IEC 27002:2013. O resultado da aplicação desta "ferramenta" pode ser visto no Capítulo 4 deste trabalho.

A ferramenta foi estudada e baixada do site da Biblioteca EDUCAUSE em formato XLSM (Excel), e posteriormente traduzida e disponibilizada por meio eletrônico, através do software LimeSurvey, para as Diretorias de Tecnologia da Informação das IFES. O questionário é composto por um total de 101 perguntas e, em média, levou cerca de 30 minutos para que os respondentes completassem a ferramenta.

Para que a avaliação da maturidade seja realizada adequadamente, cada pergunta deve ser respondida, selecionando o nível adequado de maturidade de 0 a 5. Cada seção da ISO 27002:2013 será avaliada, alcançando uma média, que proporcionará a identificação do nível de maturidade.

A "ferramenta" original pode ser baixada no site da EDUCAUSE através do link: https://library.educause.edu/resources/2015/11/information-security-program-assessment-tool

Gestão de Risco (ISO 27005: 2011)	
1	A sua instituição tem um programa de gestão de riscos?
2	A sua instituição tem um processo para identificar e avaliar os riscos internos e externos razoavelmente previsíveis para a segurança, confidencialidade e / ou a integridade de qualquer eletrônico, papel ou outros registros contendo informações confidenciais?
3	A sua organização realiza avaliações de risco de rotina para identificar os principais objetivos que precisam ser suportados pelo seu programa de segurança da informação?

Políticas de Segurança da Informação (ISO 5)	
4	A sua instituição tem uma política de segurança da informação que tenha sido aprovado pela administração?
5	Ela já foi publicada e comunicada a todas as partes interessadas?
6	A sua instituição faz revisões na política em intervalos definidos para abranger uma mudança significativa e monitorar a conformidade?
Organização da Segurança da Informação (ISO 6)	
7	Em sua instituição há um indivíduo responsável pela gestão da segurança da informação, com autoridade e atividades institucionalizadas, ou equivalente? Nota: Este pode ser o CIO, CISO ou outro.
8	O seu gestor de segurança da informação tem a autoridade necessária para gerenciar e garantir a conformidade da instituição com o programa de segurança da informação?
9	A responsabilidade está claramente atribuída a todas as áreas da arquitetura da segurança informação, conformidade, processos e auditorias?
10	Existe um processo formalizado, definindo um indivíduo responsável da área de segurança, para avaliar e atestar hardware, software e serviços adequados, garantindo que estes seguem as políticas e os requisitos de segurança?
11	A sua instituição manter relações com as autoridades locais?
12	A sua instituição participa de grupos de segurança locais ou nacionais?
13	A sua instituição realiza revisões de segurança em períodos planejados de tempo ou quando ocorrem mudanças significativas no ambiente organizacional?
Segurança Recursos Humanos (ISO 7)	
14	Será que todos os indivíduos que interagem com sistemas universitários recebem treinamento de conscientização de segurança da informação?
15	A sua instituição administra formação especializada baseada em funções?
16	Será que os programas de segurança da informação deixam claras as responsabilidades, obrigações e consequências?
17	Possui um processo de controle de acesso aos sistemas, ao prédio e de devolução de ativos cedidos?
18	A sua instituição tem um processo para revogar o acesso ao sistema quando há uma mudança de setor ou responsabilidade?
Gestão de Ativos (ISO 8)	
19	A sua organização identifica os ativos de informação críticos e as funções que dependem deles?
20	A sua instituição classificar as informações para indicar os níveis adequados de segurança da informação?
Controle de Acesso (ISO 9)	
21	A sua instituição tem uma política de controle de acesso para a autorização e revogação de direitos de acesso aos sistemas de informação?
22	A sua instituição tem um processo em vigor para conceder e revogar o acesso apropriado aos usuários?
23	A sua instituição tem um programa de gerenciamento de senhas que segue os padrões de segurança atuais?
24	A sua instituição tem procedimentos para rever regularmente o acesso dos usuários e só garantir que os privilégios necessários são aplicados?
25	A sua instituição emprega medidas específicas para assegurar serviços de acesso remoto?

26	A sua instituição emprega tecnologias para bloquear ou restringir a informações confidenciais não criptografados de viajar para redes não confiáveis?
27	A sua instituição tem mecanismos para gerenciar identidades digitais (contas, chaves, tokens) em todo o seu ciclo de vida, desde o registo até a rescisão?
28	Existe uma política em vigor para restringir o compartilhamento de senhas?
29	A sua instituição proibi a utilização de contas genéricas com acesso privilegiado aos sistemas?
30	Tem um sistema de autenticação nos locais onde aplica níveis mais elevados de autenticação para proteção de recursos com maiores níveis de sensibilidade?
31	A sua instituição tem um sistema de autorização que impõe limites de tempo de bloqueio em caso de falha de login e padrões de privilégios mínimos?
32	A sua instituição tem normas para isolar dados confidenciais, procedimentos e tecnologias para protegê-lo contra o acesso não autorizado e adulteração?
33	A sua instituição tem uma orientação de uso estabelecido para dispositivos de computação móvel (independentemente da propriedade) que armazenam, processam ou transmitem dados institucionais?
34	A sua instituição exige criptografia em dispositivos móveis de computação (ou seja, laptops, tablets, etc.)?
35	A sua instituição tem uma política de teletrabalho que aborda o acesso multifatorial e requisitos de segurança para o ponto final usado?
Criptografia (ISO 10)	
36	A sua instituição utilizar métodos de criptografia apropriados / controlados para proteger dados confidenciais em trânsito?
37	As suas políticas indicam quando a criptografia deve ser utilizada (por exemplo, em repouso, em trânsito, com dados sensíveis ou confidenciais, etc.)?
38	Possui padrões para o gerenciamento de chaves documentado e empregado?
Segurança Física e Ambiental (ISO 11)	
39	Os centros de dados de sua instituição incluem controles para assegurar que apenas pessoas autorizadas têm permissão de acesso físico?
40	A sua instituição tem medidas preventivas para proteger hardware e fiação crítica de ameaças naturais e provocados pelo homem?
41	A sua instituição tem um processo para a emissão de senhas, códigos e / ou cartões que requerem autorização e verificação de segundo plano adequados para o acesso a estas instalações sensíveis?
42	A sua instituição segue as orientações recomendadas pelo fornecedor para a manutenção de equipamentos?
43	A sua instituição tem um processo de mídia de sanitização que é aplicado ao equipamento antes do descarte, reutilização, ou a liberação?
44	Existem processos no lugar para detectar a remoção não autorizada de equipamentos, informações ou software?
Operações de Segurança (ISO 12)	
45	A sua instituição mantem os padrões de configuração de segurança para sistemas de informação e aplicações?
46	As alterações dos sistemas de informação são testadas, autorizadas e relatadas?
47	As funções são suficientemente segregadas para assegurar que a modificação não intencional ou não autorizada de informações seja detectada?

48	Os sistemas em produção são separados de outras fases do ciclo de vida de desenvolvimento?
49	A sua instituição tem processos em andamento para monitorar a utilização dos principais recursos do sistema e para mitigar o risco de indisponibilidade?
50	Possui métodos para detectar, manter em quarentena e erradicar código malicioso conhecido em sistemas de informação, incluindo estações de trabalho, servidores e dispositivos de computação móvel?
51	Possui métodos para detectar e erradicar códigos maliciosos conhecidos transportados por correio eletrônico, web, ou em mídia removível?
52	Realiza com frequência o processo de backup de dados consistente com os requisitos de disponibilidade da sua organização?
53	A sua instituição tem um processo para verificação de estado atual do software de antivírus, firewall, nível de patch de sistema operacional, etc., de dispositivos que se conectam a sua rede?
54	A sua instituição tem uma arquitetura de rede segmentada para fornecer diferentes níveis de segurança com base na classificação da informação?
55	Os servidores acessíveis pela Internet são protegidos por mais de uma camada de segurança (firewalls, IDS de rede, IDS de host, aplicativo IDS)?
56	Possui controles em vigor para proteger, controlar e registrar a saída de mídia que tenham sido removidas de locais seguros de organização?
57	A sua instituição tem um processo em vigor para garantir que os dados relativos ao comércio electrónico (e-commerce) que atravessam redes públicas está protegido contra atividade fraudulenta, divulgação não autorizada ou modificação?
58	As atividades relacionadas com a segurança, tais como as alterações de configuração de hardware, de software, tentativas de acesso, atribuições de autorização e privilégios são automaticamente registradas?
59	A sua instituição tem um processo de monitoramento de logs para detectar atividades não autorizadas e anormais?
60	A sua instituição grava as suas análises de log (recertificação / prova)?
61	São tomadas medidas para proteger os dados de registro para evitar o acesso não autorizado e adulteração?
62	A sua instituição revisa regularmente o acesso administrativo e operacional para logs de auditoria?
63	Possui ferramentas utilizadas para alerta de modificação não autorizada de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo e realiza comparações de arquivos críticos pelo menos semanalmente monitorando a integridade dos arquivos?
64	A sua instituição tem um processo para garantir a sincronização dos relógios do sistema com uma fonte autorizada (por exemplo, via NTP) em uma base periódica proporcional aos riscos potenciais?
Segurança das Comunicações (ISO 13)	
65	A sua instituição exige o uso de confidencialidade ou acordos de não divulgação para empregados e terceiros?
66	A sua instituição testa rotineiramente seus procedimentos de restauração?
67	A sua instituição monitora continuamente suas redes com e sem fios de acesso não autorizado?
68	A sua instituição tem políticas e procedimentos para proteger informações trocadas (dentro de sua organização e nos acordos de terceiros) de interceptação, cópia, modificação, misrouting (caminho errado) e destruição?
69	A sua instituição garante que o acesso dos usuários as portas de diagnóstico e configuração é restrita aos indivíduos e aplicações autorizadas?

70	A sua instituição adota medidas específicas para prevenir e detectar o acesso não autorizado de todas as suas LANs sem fio?
Sistemas de Aquisição, Desenvolvimento e Manutenção (ISO 14)	
71	A sua instituição tem um processo para validar a segurança dos produtos de software e serviços adquiridos?
72	Os novos sistemas de informação ou melhorias em sistemas existentes são validados mesmo estando contrários aos requisitos de segurança definidos?
73	Possui normas estabelecida para práticas de codificação seguras (por exemplo, validação de entrada, manipulação de erro adequada, gerenciamento de sessão, etc.), levando em consideração as vulnerabilidades de aplicativos comuns de segurança (por exemplo, CSRF, XSS, injeção de código, etc.)?
74	Faz verificações de validação incorporados nas aplicações para detectar qualquer corrupção de informações através de erros de processamento ou atos deliberados?
75	Tem processos em andamento para verificar se a integridade da mensagem é necessária?
76	Saídas incorretas podem ocorrer, mesmo em sistemas testados. A sua instituição tem verificações de validação para garantir que a saída de dados é como esperada?
77	Você estabeleceu procedimentos para manter o código-fonte durante o ciclo de vida de desenvolvimento e ao mesmo tempo na produção, para reduzir o risco de corrupção de software?
78	A sua instituição aplica as mesmas normas de segurança para os dados de teste sensível que você aplica aos dados de produção sensíveis?
79	A sua instituição restringi e monitora o acesso a bibliotecas de código fonte para reduzir o risco de corrupção?
80	A sua instituição tem um processo de gestão de configuração em vigor para garantir que as alterações nos seus sistemas críticos acontecem por razões do negócio válidas e têm recebido a devida autorização?
81	Realiza avaliações e testes para garantir que as alterações feitas aos sistemas de produção não têm um impacto negativo na segurança ou operações?
82	Possui implementadas ferramentas e procedimentos para monitorar e evitar a perda de dados sensíveis?
83	Será que os seus acordos contratuais incluem requisitos de segurança para o desenvolvimento de software terceirizado?
84	A sua instituição tem uma estratégia de gerenciamento de patches em vigor e responsabilidades atribuídas para o monitoramento e resposta imediata de correção de releases, boletins de segurança e relatórios de vulnerabilidade?
Relacionamento com Fornecedores (ISO 15)	
85	A sua instituição especifica requisitos de segurança nos contratos com entidades externas (terceiros) antes de conceder acesso aos ativos de informação institucionais sensíveis?
86	Os requisitos são abordados e corrigidos antes de conceder o acesso aos dados, ativos e sistemas de informação?
87	Os acordos relativos aos serviços do sistema de informação externo especificam os requisitos de segurança apropriados?
88	A sua instituição tem um processo em vigor para avaliar que os fornecedores de sistemas de informação externos cumprem com os requisitos de segurança apropriadas?
89	O provedor de serviços de sistemas de informação externo é monitorado quanto ao cumprimento dos controles de segurança?
90	Os acordos de serviço dos sistemas de informação externa são executado e rotineiramente revisados

	para garantir que os requisitos de segurança são atuais?
Gestão de Incidentes de Segurança da Informação (ISO 16)	
91	Possui procedimentos de tratamento de incidentes para informar e responder a eventos de segurança em todo o ciclo de vida do incidente, incluindo a definição de papéis e responsabilidades?
92	A sua equipe de resposta a incidentes está ciente das exigências legais ou da conformidade que cercam a coleta de evidencias?
93	Aspectos de segurança da informação na Gestão da Continuidade do Negócio (ISO 17)
94	A sua instituição tem um plano documentado continuidade de negócios de tecnologia da informação que é baseado em uma análise de impacto nos negócios, é testado periodicamente, e tem sido analisado e aprovado por altos funcionários ou do conselho de administração?
Conformidade (ISO 18)	
95	A sua instituição tem uma política de governança de gerenciamento de registros ou dados que aborda o ciclo de vida de ambos os documentos, impressos e eletrônicos, em sua instituição?
96	A sua instituição tem uma política de proteção de dados aplicável que abrange informações de identificação pessoal (PII)?
97	A sua instituição tem uma Política de Utilização Aceitável que define o uso incorreto?
98	A sua instituição fornece orientação para a comunidade sobre as leis de controle de exportação?
99	Os procedimentos operacionais padrão são periodicamente avaliados para conformidade com as políticas de segurança da sua organização, normas e procedimentos?
100	A sua instituição realiza, nas camadas de aplicação e rede, testes de vulnerabilidade periódicos ou testes de penetração contra sistemas de informação críticos?
101	Realiza auditorias independentes em sistemas de informação para identificar pontos fortes e fracos?
101	Possui ferramentas de auditoria devidamente separadas de desenvolvimento e ambientes de sistemas operacionais para evitar qualquer uso indevido ou comprometer a segurança?