Pós-Graduação em Ciência da Computação

GLINER DIAS ALENCAR

PRIMASIA: Uma Estratégia para Priorização e Avaliação da Maturidade da Segurança da Informação Adaptável ao Ambiente Corporativo

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

Recife
2018

GLINER DIAS ALENCAR

PRIMASIA: Uma Estratégia para Priorização e Avaliação da Maturidade da Segurança da Informação Adaptável ao Ambiente Corporativo

Trabalho apresentado ao Programa de Pós-graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Doutor em Ciência da Computação.

Área de concentração: Segurança da Informação.

Orientador: Prof. Dr. Hermano Perrelli de Moura.

Recife
2018

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

A368p Alencar, Gliner Dias
Primasia: uma estratégia para priorização e avaliação da maturidade da segurança da informação adaptável ao ambiente corporativo / Gliner Dias Alencar. – 2018.
265 f.: il., fig., tab.

Orientador: Hermano Perrelli de Moura.
Tese (Doutorado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2018.
Inclui referências e apêndices.

1. Segurança da informação. 2. Priorização. I. Moura, Hermano Perrelli de (orientador). II. Título.

005.8 CDD (23. ed.) UFPE- MEI 2019-048

Gliner Dias Alencar

Primasia: Uma Estratégia para Priorização e Avaliação da Maturidade da Segurança da Informação Adaptável ao Ambiente Corporativo

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Doutor em Ciência da Computação.

Aprovado em: 11/12/2018.

_____

Orientador: Prof. Dr. Hermano Perrelli de Moura

BANCA EXAMINADORA

_____

Prof. Dr. Alexandre Marcos Lins de Vasconcelos
Centro de Informática/ UFPE

_____

Prof. Dr. Ruy José Guerra Barretto de Queiroz
Centro de Informática / UFPE

_____

Prof. Dr. André Luis de Medeiros Santos
Centro de Informática / UFPE

_____

Prof. Dr. Jorge Henrique Cabral Fernandes
Departamento de Ciência da Computação / UnB

_____

Prof. Dr. José Gilson de Almeida Teixeira Filho
Departamento de Ciências Administrativas / UFPE

Dedico a conclusão deste trabalho à minha amada esposa, Juliana Ferreira, por estar ao meu lado em todos os momentos, sendo coautora deste projeto e da formação do meu ser.

AGRADECIMENTOS

Após a longa caminhada do Doutorado é chegado o momento final. Ao mesmo tempo que analisa-se o trabalho, é importante refletir sobre o aprendizado técnico, evolução pessoal e profissional, bem como agradecer aos que contribuíram para que fosse possível iniciar e concluir esta etapa.

Primeiramente agradeço a Deus pelo dom da vida e da saúde.

Ao professor e orientador Hermano Perrelli de Moura que abraçou o projeto no momento mais difícil deste Doutorado. Agradecimento e gratidão pelos ensinamentos, apoio, confiança e liberdade dada na produção deste trabalho. Bem como, pelo exemplo para a minha formação acadêmica, profissional e pessoal.

Ao professor e orientador do mestrado Ruy José Guerra Barretto de Queiroz pelos ensinamentos e diretrizes que perduram por toda minha trajetória acadêmica e profissional.

Agradeço aos amigos, empresas e órgãos parceiros neste projeto que contribuíram no debate e construção das ideias, na disponibilização dos formulários de pesquisa, indicação de empresas para participar dos surveys, bem como de profissionais para atuar como especialistas nas diversas etapas.

Ao Instituto Brasileiro de Geografia e Estatística (IBGE), chefes e amigos pelo apoio e liberação, quando necessário, para as etapas do Doutorado sendo, desta forma, possível conciliar o curso com as atividades laborais. Em especial, aos amigos Alcides Tenorio Junior e Carlos Augusto Menezes pelas diversas conversas, apoio e incentivos quando estava na Unidade Estadual do IBGE em Alagoas e, posteriormente, aos amigos e toda equipe da Unidade Estadual do IBGE em Pernambuco que guiaram o órgão, me proporcionando espaços para as ausências necessárias nesta reta final.

Aos amigos coautores dos trabalhos. Cada artigo produzido gerava novas reflexões e evoluções no projeto como um todo.

Aos amigos do Grupo de Pesquisa em Gestão de Projetos (GP2) pelos compartilhamentos, dicas e debates para o aprimoramento deste projeto.

Aos familiares, amigos e todos aqueles, presentes ou ausentes, que direta ou indiretamente contribuíram, incentivaram e torceram durante toda a realização do curso.

Agradeço também a todos que falaram que seria loucura tocar o projeto sem dedicação exclusiva, que não iria dar certo ou que, por qualquer motivo, duvidaram que fosse possível. Essas ações se juntaram a todos os pensamentos positivos e incentivos recebidos tornando-se molas que impulsionaram, ainda mais, a vontade de terminar este projeto.

Por fim, e especialmente, à minha esposa, Juliana Ferreira, pela revisão, compreensão, ajuda, apoio e incentivo em todos os sentidos.

RESUMO

A falta de segurança em sistemas de informação tem provocado inúmeros prejuízos financeiros e morais para as organizações. As organizações dispõem de uma série de medidas de segurança da informação recomendadas por normas internacionais e pela literatura. Porém a implementação de políticas, ações e adequação a alguma norma não é algo simples, devendo ser balizada pelas necessidades específicas identificadas pela Governança da Segurança da Informação em cada organização. Muitos são os desafios enfrentados para estabelecer, manter e medir a segurança da informação de forma eficaz e que de fato agregue valor. Estas dificuldades demonstram a necessidade de pesquisar formas para tentar suprir esta carência. Este trabalho apresenta uma estratégia para mensurar a maturidade em segurança da informação visando, também, auxiliar a aplicação e priorização das ações de segurança da informação no meio corporativo. Para isto, a pesquisa alicerçou-se na Design Science Research, utilizando o survey como principal instrumento metodológico de coleta de dados, alcançando 157 empresas distintas. Para propor essa estratégia de priorização e maturidade optou-se por um estudo ad-hoc da literatura, seguido por um mapeamento sistemático da literatura e análises de revisões sistemáticas da literatura já existentes. Como resultado foi possível classificar os controles da ISO/IEC 27001 e 27002 em quatro estágios de acordo com a importância dada pelas empresas. Utilizou-se, também, os níveis de maturidade do COBIT e uma matriz para análise de riscos. Quatro versões do artefato foram geradas, sendo avaliadas por empresas e especialistas, utilizando questionários, aplicação em caso real e realizando um grupo focal. A quarta e última versão do artefato foi chamada de Estratégia Primasia, uma Estratégia para Priorização e Maturidade da Segurança da Informação Adaptável. Neste sentido, a principal contribuição desta pesquisa de doutorado é a estratégia de priorização e maturidade em segurança da informação adaptável que visa estabelecer boas práticas de segurança da informação para maximizar o seu sucesso nas empresas. Acredita-se que este trabalho também contribui com o ainda incipiente corpo de conhecimento da área de priorização e maturidade em segurança da informação. Este entendimento é útil não apenas para estudos futuros na academia, mas também para empresas que estejam iniciando ou pretendendo melhorar suas ações de segurança da informação.

Palavras-chave: Segurança da Informação. Priorização. Maturidade. Governança. Gestão.

ABSTRACT

The lack of security in information systems has caused numerous financial and moral losses to several organizations. The organizations have a series of information security measures recommended by literature and international standards. However, the implementation of policies, actions, and adjustment to such standards is not simple and must be addressed by specific needs identified by the Information Security Governance in each organization. There are many challenges in effectively establishing, maintaining, and measuring information security in a way that adds value. Those challenges demonstrate a need for further investigations which address the problem. This work presents a strategy to measure the maturity in information security aiming, also, to assist in the application and prioritization of information security actions in the corporate environment. For this, the research was based on Design Science Research. A survey was used as the main methodological instrument of data collection, reaching 157 distinct companies. To propose this prioritization and maturity strategy, an ad-hoc review of the literature was chosen, followed by a systematic mapping and analysis of existing systematic reviews of the literature. As a result, it was possible to classify the ISO/IEC 27001 and 27002 controls in four stages according to the importance given by the companies. The COBIT maturity levels and a risk analysis matrix were also used. Four versions of the artifact were generated, being evaluated by companies and specialists, using questionnaires, application in a real case and realizing a focus group. The fourth and final version of the artifact was the Primasia Strategy, an Adaptable Prioritization and Maturity Strategy for Information Security. Therefore, the main contribution of this doctoral research is the Adaptable Prioritization and Maturity Strategy for Information Security that aims to establish good information security practices to maximize its success in companies. It is believed that this work also contributes to the still incipient body of knowledge about prioritization and maturity in the information security area. This understanding is useful not only to further studies in the academy but also to companies that are starting or intending their information security actions.

Keywords: Information Security. Prioritization. Maturity. Governance. Management.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

BMIS	BUSINESS MODEL FOR INFORMATION SECURITY
C2M2	CYBERSECURITY CAPABILITY MATURITY MODEL
CISO	CHIEF INFORMATION SECURITY OFFICER
CMM	CAPABILITY MATURITY MODEL
CMMI	CAPABILITY MATURITY MODEL INTEGRATION
COBIT	CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY
CSF	CYBERSECURITY FRAMEWORK
DSR	DESIGN SCIENCE RESEARCH
DSRM	DESIGN SCIENCE RESEARCH METHODOLOGY
E-SCM	ESOURCING CAPABILITY MODEL
GP2	GRUPO DE PESQUISA EM GESTÃO DE PROJETOS
GRSI	GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO
GSI	GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO
IEC	INTERNATIONAL ELECTROTECHNICAL COMMISSION
ISF SOGP	INFORMATION SECURITY FORUM STANDARD OF GOOD PRACTICE
ISO	INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ITIL	IT INFRASTRUCTURE LIBRARY
M3	MANGVE MATURITY MODEL
MMGP	MODELO DE MATURIDADE EM GERÊNCIA DE PROJETOS
MPS.BR	MELHORIA DO PROCESSO DE SOFTWARE BRASILEIRO
MSL	MAPEAMENTO SISTEMÁTICO DA LITERATURA
NICE-CMM	NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION – CAPABILITY MATURITY MODEL
NIST	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
O-ISM3	OPEN INFORMATION SECURITY MANAGEMENT MATURITY MODEL
OCTAVE	OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION
OPM3	ORGANIZATIONAL PROJECT MANAGEMENT MATURITY MODEL
PDCA	PLAN, DO, CHECK E ACT

PMF	PROCESS MATURITY FRAMEWORK
PMI	PROJECT MANAGEMENT INSTITUTE
PMBOK	PROJECT MANAGEMENT BODY OF KNOWLEDGE
PRIMASIA	PRIORIZAÇÃO E MATURIDADE EM SEGURANÇA DA INFORMAÇÃO ADAPTÁVEL
PSI	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
ROI	RETURN ON INVESTMENT
ROSI	RETURN ON INFORMATION SECURITY INVESTMENT
RSL	REVISÃO SISTEMÁTICA DA LITERATURA
RUP	RATIONAL UNIFIED PROCESS
SAS 70	STATEMENT ON AUDITING STANDARDS NO. 70: SERVICE ORGANIZATIONS
SGSI	SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
SSE-CMM	SYSTEMS SECURITY ENGINEERING CAPABILITY MATURITY MODEL
SW-CMM	CAPABILITY MATURITY MODEL FOR SOFTWARE
TI	TECNOLOGIA DA INFORMAÇÃO
TIC	TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

SUMÁRIO

1 INTRODUÇÃO

Desde o início dos processos industriais, pode-se citar o uso da tecnologia como destaque na tentativa de aprimoramento dos processos operacionais, tendo seu marco principal a revolução da Tecnologia da Informação e Comunicação (TIC), na década de 1970, com uma vasta quantidade de descobertas e com as invenções do microcomputador e do microprocessador. Essa revolução propiciou uma série de avanços nas mais diversas áreas, beneficiando os que detêm maior conhecimento das mesmas (CASTELLS, 2009; NOBRE, 2009).

Na sociedade atual, competitiva e que necessita de ações e tomadas de decisões rápidas e alinhadas ao negócio, a obtenção e a guarda do conhecimento é de suma importância. Nesse contexto, a informação tornou-se um dos mais valiosos ativos das empresas, visto que informações manuseadas nas corporações podem gerar tanto lucro como grandes prejuízos, assim como o setor que a gerencia tornou-se, nas organizações, estratégico (CASTELLS, 2009; FERREIRA; ARAUJO, 2009; NOBRE, 2009; SÊMOLA, 2013). Com o avanço da tecnologia, cada vez mais o conhecimento está sendo transferido da mente humana e dos papéis para os aparatos tecnológicos, cabendo à TIC processos como manipulação, guarda e tráfego de informações corporativas, muitas delas confidenciais, em diversos tipos de ambientes, podendo abranger ambientes heterogêneos, complexos e distribuídos.

Nesta nova situação, percebe-se a ampliação dos papéis da Tecnologia da Informação e Comunicação, que é responsável pelo gerenciamento de um bem com valor, muitas vezes, imensurável. Consequentemente, estas informações são extremamente visadas e os mais diversos tipos de ameaças buscam alcançá-las.

Diante desse cenário, percebe-se a existência de duas forças: de um lado as corporações que se esforçam para manter protegido seu bem vital, especialmente, as informações avaliadas como estratégicas; e, em sentido oposto, encontram-se os invasores, podendo ser externos ou internos, que objetivam capturar ou adulterar as informações, sendo movidos pelos mais variados fatores (lazer, desafio, vingança, protesto), mas normalmente visando alguma forma de impacto financeiro (ALENCAR; QUEIROZ; QUEIROZ, 2013a).

Diferentes tipos de ameaças tentam, por diversos meios, ter acesso às informações. A complexidade deste contexto é mostrada pelos mais variados meios tecnológicos utilizados para o armazenamento, manipulação e acesso às informações, pela variedade e particularidade de cada informação armazenada e pelo grande número de ameaças existentes no ambiente externo e interno, envolvendo desde as ameaças inerentes ao ambiente, como os malwares, até as pessoas.

Ciente que a segurança da informação tem foco na organização e traz como princípios básicos a garantia da Disponibilidade (visando garantir que a informação esteja sempre

disponível), da Confidencialidade (visando garantir que a informação seja acessada somente por pessoas com autorização) e da Integridade (visando que a informação não seja modificada sem autorização, garantindo a sua exatidão); ações que afetem tais princípios, sejam intencionais ou não, podem alterar o desempenho da organização, chegando, em casos mais críticos, a causar grandes impactos financeiros e, até mesmo, falências.

Mesmo diante da importância das informações e da criticidade dos riscos, atualmente, diversas organizações não contam com planos adequados na área de segurança da informação e alinhamento dos mesmos ao negócio, tendo, em alguns casos, medidas de segurança da informação apenas para atender as forças externas, normalmente oriundas de obrigações legais e regulamentares, como detalha Albuquerque Junior e Santos (2014).

A segurança das informações no ambiente atual carece de benfeitorias e estudos contínuos devido à crescente importância da Tecnologia da Informação e Comunicação e da sua complexidade, assim como das mutações e melhoramentos constantes dos diversos tipos de ameaças, o que torna extremamente relevante e justifica as constantes pesquisas para ampliar as tecnologias de segurança e seus processos. Porém, a quantidade de pessoas envolvidas no processo, faz com que o uso dos melhores artefatos de segurança não seja suficiente para garantir a guarda e o correto uso das informações (MARCIANO; LIMA-MARQUES, 2006; ALENCAR, 2008; FERREIRA; ARAUJO, 2009). Sendo necessário, também, a melhoria e simplificação dos processos de alinhamento da segurança da informação ao negócio, bem como o estudo da variável "pessoa" que, normalmente, está envolvida desde a concepção da informação e dos meios de armazenamento até o descarte (SALEH, 2011; ALENCAR; LIMA; FIRMO, 2013a).

O presente Capítulo está dividido em seis seções. Na primeira Seção será demonstrada a evolução da pesquisa. A seguinte Seção 2, apresentará a motivação e justificativa do trabalho. Na terceira Seção, o problema de pesquisa será abordado. Na Seção 4 será explicitada uma possível proposta de solução. Na quinta Seção os objetivos geral e específicos serão explanados. E, por fim, na última Seção, a organização do trabalho será demonstrada.

1.1 Evolução da Pesquisa

Definição de um tema de pesquisa interessante e relevante não é algo simples. O processo consiste, normalmente, em um conjunto de ideias, debates, avaliações, testes e melhoramentos contínuos. Na presente pesquisa não foi diferente.

A ideia central sempre foi trabalhar aspectos da segurança da informação no ambiente corporativo, buscando resolvê-lo de modo aplicado. Algumas pesquisas foram realizadas como forma de avaliar a aceitação da comunidade corporativa e acadêmica aos encaminhamentos sugeridos. Com foco na análise do fator humano na segurança da informação, duas linhas correlacionadas foram concebidas: análise dos insiders (ALENCAR; QUEIROZ;

QUEIROZ, 2013a; ALENCAR; QUEIROZ; QUEIROZ, 2013b) e análise da capacitação dos funcionários como meio para o tratamento de ameaças e vulnerabilidades (ALENCAR; LIMA; FIRMO, 2013a; ALENCAR; LIMA; FIRMO, 2013b).

Com essa temática e objetivos em mente, o presente pesquisador iniciou, em 2014, o curso de doutorado. Ao refletir sobre o tema, algumas questões foram levantadas:

i. A problemática escolhida configura-se suficiente para uma tese de doutorado?

ii. Será possível realizar tal estudo em termos de tempo e custos em um doutorado?

Com o caminhar do curso, disciplinas, pesquisas e orientações, surgiu a proposta de alinhar duas questões de pesquisa, a saber:

i. Elaborar um processo para melhoria e simplificação dos arcabouços de segurança da informação mais utilizados nos ambientes corporativos; e

ii. Analisar o envolvimento do fator humano na concepção, administração e uso dos serviços de TIC e de segurança da informação.

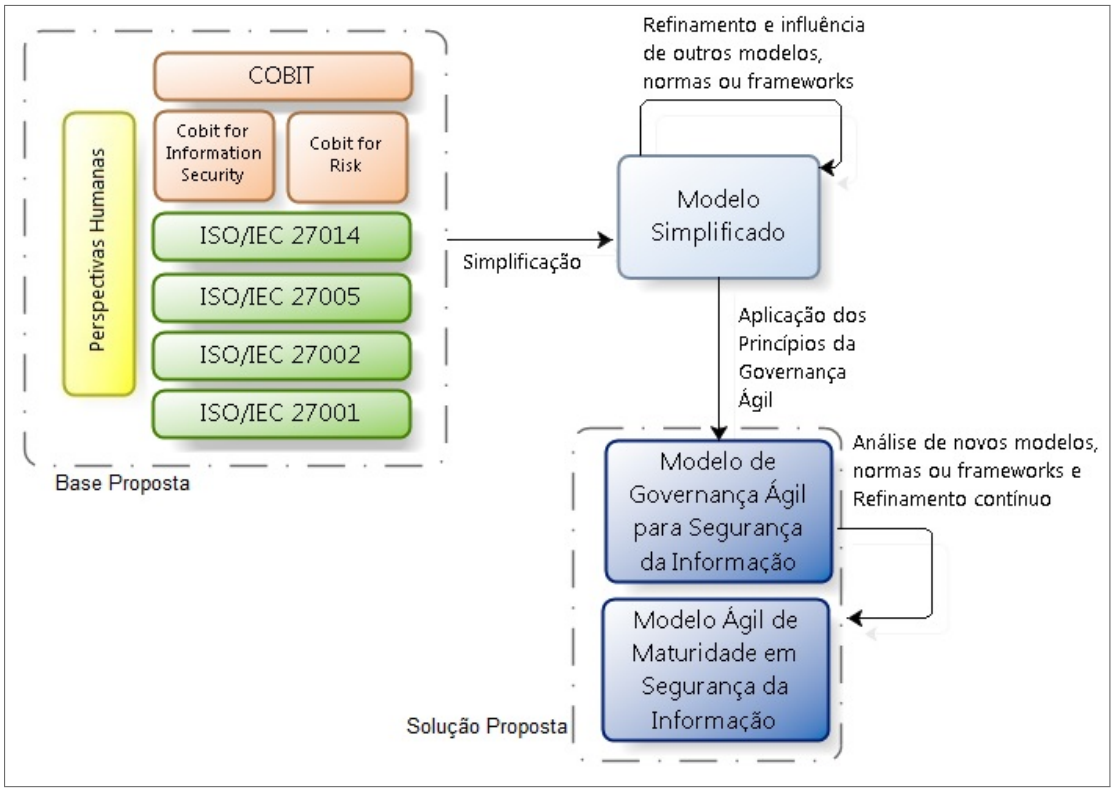
Acreditou-se que investigando essas duas questões alinhadas, seria possível elaborar uma solução holística de melhoria para a segurança da informação corporativa. Nessa linha de pesquisa, trabalhos como: Silva Neto, Alencar e Queiroz (2015) e Alencar, Tenorio Junior e Moura (2017a) foram produzidos pelo autor e parceiros.

Porém o interesse em criar algo maior e que proporcionasse um auxílio efetivo ao meio corporativo fez o escopo do trabalho crescer, abordando: governança, gestão, maturidade e agilidade da segurança da informação, sem esquecer dos aspectos humanos. Chegando a uma solução completa, na visão do pesquisador, para o problema então pesquisado: um modelo de governança ágil e um modelo ágil de maturidade em segurança da informação concebidos, em linhas gerais, através de um processo de simplificação de um conjunto dos principais documentos da área (COBIT e normativos ISO/IEC), inserindo uma visão das perspectivas humanas e aplicando os princípios da governança ágil, conforme Figura 1.

Tal proposta foi defendida na qualificação do doutorado, no segundo semestre de 2016, sob título de: "Proposta de Modelo de Governança, Gestão e Maturidade Ágil para Segurança da Informação: Uma Abordagem sob o Viés dos Aspectos Humanos". Após a aprovação na banca de qualificação do doutorado, a incerteza sobre a validade do tema, importância e porte para um doutorado, não mais existia. O problema, então, se transformou em outro: a necessidade de diminuir o escopo. Pois, para a banca de qualificação, cada área selecionada (governança, gestão, maturidade, agilidade e aspectos humanos na segurança da informação) já teria relevância e conteúdo suficiente para um doutorado. Devendo diminuir, drasticamente, o escopo.

Mesmo não sendo totalmente tratada neste projeto, por questões de escopo e tempo, ainda acredita-se que tal visão holística (Figura 1) seja essencial para a área, sendo publicada em Alencar, Tenorio Junior e Moura (2017b).

Figura 1 – Solução Holística para Segurança da Informação



Fonte: Alencar, Tenorio Junior e Moura (2017b, p. 3683)

Após revisitar a literatura, orientações, apresentações e debates no Grupo de Pesquisa em Gestão de Projetos (GP2), grupo de pesquisa encabeçado pelo Professor Hermano Perrelli de Moura, no qual o autor faz parte, o tema foi se consolidando na área de maturidade e agilidade (governança ágil) de segurança da informação, tendo sido debatido em dois eventos de propostas de doutorado (ALENCAR; MOURA, 2017a; ALENCAR; MOURA, 2017b). A aceitação serviu, mais uma vez, como apontamento para a importância e relevância do tema para a área. Porém, nos dois eventos, os avaliadores aconselharam, entre outras melhorias, a redução do escopo do trabalho.

Ressalta-se que o artigo de Alencar e Moura (2017a) recebeu, em julho de 2018, o convite para ser expandido e publicado em dezembro do mesmo ano como capítulo no livro "Princípios e Aplicações da Computação no Brasil". O capítulo foi produzido e aceito pela editora para compor o citado livro.

Mais orientações, reflexões e debates no GP2 guiaram para a versão atual. Embasado pelos princípios da governança ágil, chegou-se à temática de maturidade e priorização em segurança da informação. Tal proposta foi defendida em Alencar e Moura (2018) e Alencar et al. (2018a), sendo uma área em expansão, mais ainda carente na literatura, como apontou os resultados da revisão da literatura realizada nessa pesquisa (ALENCAR et al., 2018b; ALENCAR et al., 2018c), bem como outras pesquisas na área, por exemplo, os trabalhos de Albuquerque Junior e Santos (2013) e de Rea-Guaman et al. (2017).

Finalizando as publicações realizadas, uma versão revisada do artigo de Alencar, Tenorio Junior e Moura (2017b) foi submetida e aceita como capítulo no livro "Information Systems and Technology Management" a ser publicado em fevereiro de 2019.

A lista dos onze trabalhos publicados ou aceitos, que, de certa forma, descrevem o caminho trilhado, pode ser vista no Apêndice K.

1.2 Motivação e Justificativa

Atualmente, no ambiente corporativo, independente de seu porte, a utilização de sistemas e troca de informações em rede são atividades corriqueiras, o que traz como exigência a utilização de meios de controle, normas e padrões de segurança, a fim de evitar perdas e vazamento de informação, assim como, afetar os bens e a imagem da empresa perante o mercado e seus clientes. Segundo Diniz, Medeiros e Veras (2012, p. 9), "com a popularização da tecnologia e o avanço da economia digital a TI encontra-se em posição de destaque no ambiente empresarial, exercendo papel decisivo nos negócios".

Nesse ambiente, o aumento dos incidentes de segurança cresce aceleradamente em todo o mundo. Os ataques atingem diversos tipos de organizações, tanto as governamentais quanto empresas privadas de diversos portes e segmentos. Além disso, vem se tornando cada vez maior a lista de empresas, países e instituições governamentais que estão em um verdadeiro duelo contra "hackerativistas" (PWC, 2017).

Por conta deste e de outros fatores, existem diversos padrões, frameworks, normas e regulamentos para a implementação de modelos de segurança da informação. Esses modelos fornecem um conjunto de boas práticas visando a Gestão da Segurança da Informação que, em sua maioria, para incorporar todos os possíveis pontos inerentes à Segurança da Informação, torna-se grande e complexo, fazendo com que, de forma geral, as empresas não apliquem e não gerenciem as características de segurança da informação de forma adequada.

A complexidade dos modelos tradicionais mais utilizados atualmente abre uma oportunidade para rever os processos de implantação de tais padrões, modelos, normas ou frameworks, adequando-os às necessidades específicas de cada organização, visto que mesmo não implantando todos os processos ou controles, a organização consegue obter uma grande mudança organizacional, uma melhoria em seus processos e um maior alinhamento entre a área de TIC e as estratégias organizacionais, como demonstram os resultados de Silva Neto, Alencar e Queiroz (2015) e Prado et al. (2016).

Almeida Neto et al. (2015a) também ressaltam esse problema ao apontar a necessidade de se ter um maior controle nas empresas, porém é necessário ter agilidade para tratar o dinamismo atual.

Na área acadêmica, a maioria das pesquisas no campo da segurança da informação tem se concentrado, prioritariamente, no desenvolvimento, melhoria e aplicação de as-

pectos técnicos nos sistemas, redes e segurança física (DAYANAND; KUMAR, 2015; FETAJI et al., 2016; WANG; LIU, 2018). No entanto, a pura aplicação da tecnologia não é suficiente para o tratamento da segurança da informação. Para os novos desafios, também é necessário abordar outras áreas, olhando para a segurança da informação de forma mais ampla (CHOO, 2011). Dentro dessa visão holística destacam-se os estudos que abordam os aspectos e influências humanas em segurança da informação (WARKENTIN; WILLISON, 2009; POSEY; BENNETT; ROBERTS, 2011) e a área relacionada a processos, procedimentos e controles, que abrange gestão, governança, auditoria, conformidade, Política de Segurança da Informação (PSI) e maturidade, sendo este último o foco do presente estudo. Ressalta-se que tais áreas não são excludentes e podem ser trabalhadas em conjunto, como pode ser visto em Choi e Hwang (2013) e Choi (2017) que abordam aspectos humanos e política de segurança da informação.

É importante destacar, também, a escassez de estudos que investigam esta temática, comparando com outras áreas da computação. Por exemplo, tem-se constantemente visto nos tópicos de interesses dos últimos anos dos principais eventos nacionais da área (pode-se citar: CONTECSI - Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação; SBSEG - Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais; SBSI – Simpósio Brasileiro de Sistemas de Informação; SBTI - Simpósio Brasileiro de Tecnologia da Informação) chamadas para a área de "Governança de TIC", "Gestão da Segurança da Informação", "Normatização da Segurança da Informação", "Políticas de Segurança da Informação", "Maturidade em Segurança da Informação", ou temas semelhantes, porém, mesmo com o aumento nos últimos anos, ainda são poucos os trabalhos que abordam tais áreas nos anais. Essa carência de trabalhos na área de segurança da informação abordada nesta pesquisa não é apenas no ambiente nacional, sendo exposta em Albuquerque Junior e Santos (2013), Rea-Guaman et al. (2017), Alencar et al. (2018b) e Alencar et al. (2018c).

Saleh (2011b) corrobora com a temática ao informar que é possível mensurar a segurança da informação corporativa através de um modelo de maturidade, porém ainda são necessárias muitas pesquisas para amadurecer esta área. Neste mesmo sentido, Proença e Borbinha (2018) apontam a necessidade de se aferir a maturidade da segurança da informação, porém os principais modelos de maturidades existentes não atendem, em sua completude, as atividades necessárias para aferir o nível de maturidade de segurança da informação conforme os principais normativos da área, em especial, a ISO/IEC 27.001.

Neste contexto, acredita-se ser relevante para a área de segurança da informação realizar estudos na tentativa de se produzir meios para aferir a maturidade da área de segurança da informação, dando subsídios para um melhor alinhamento da área à governança de TIC e corporativa e buscando formas menos complexas ou burocráticas que as costumeiramente aplicadas atualmente. Assim como, acredita-se ser relevante, facilitar a concepção e uso da Política de Segurança da Informação (PSI) e do Sistema de Gestão

de Segurança da Informação (SGSI) e priorizar as ações e recursos relacionados à área.

Diante do exposto, o presente trabalho propõe, utilizando os arcabouços existentes e o pensamento de agilidade, uma estratégia para priorização e maturidade na área de segurança da informação como forma de melhoria para a área.

Lessing (2008) afirma que o ato de verificar e adequar as melhores práticas existentes para que seja implantada e mensurada a segurança da informação é um desafio árduo, mas que necessita ser vencido, preenchendo a lacuna de trabalhos que utilizem boas práticas para modelos de maturidade. Sendo, um possível caminho, a estruturação de um modelo que utilize as melhores práticas já existentes nos melhores modelos atuais, como abordam Radanliev et al. (2018).

Acredita-se, por fim, que a segurança deverá ser constituída em camadas, como cita MacCarthy (2011), dessa forma, qualquer melhoria implantada contribuirá para se ter um ambiente mais seguro. Com este pensamento, espera-se que o melhor entendimento do nível de maturidade da segurança da informação no qual a empresa se encontra, bem como ações para priorização da segurança da informação, modifique o ambiente como um todo, provendo melhorias para que as vulnerabilidades não sejam exploradas, o que diminuirá os riscos e aumentará o patamar de segurança do ambiente.

1.3 Problema de Pesquisa

A segurança da informação transformou-se em algo crítico e essencial para a sobrevivência dos negócios neste meio globalizado e extremamente competitivo. Para manter a sustentabilidade da empresa é primordial a proteção dos ativos de valor e a eficácia na gestão dos riscos, para que assim, possa maximizar os lucros e aumentar o valor da organização. Com base nesse contexto, a International Organization for Standardization (ISO) e a International Electrotechnical Commission (IEC) criaram a Família de normas 27.000, que abordam a segurança da informação, como detalha Palma (2016) e ISO27k (2016), sendo esse um dos principais mecanismos na área de segurança da informação no que tange, principalmente, aos aspectos táticos e operacionais.

Apesar desses modelos serem muito bem estruturados, o formalismo, por algumas vezes excessivo, tem tornado a adoção e melhoria contínua de seus processos uma tarefa complexa, como abordam Silva Neto, Alencar e Queiroz (2015) e Prado et al. (2016).

Tal pensamento também é corroborado por Fazenda e Fagundes (2015), ao demonstrar que a necessidade corporativa por segurança da informação e a adesão às normas da família 27.000 da ISO/IEC crescem em todo o mundo, porém ainda sofrem sérias dificuldades em sua implantação, assim como, carecem de estudos na área.

Na área conhecida como quantificação de segurança também fica evidente a necessidade de padronização e validação dos métodos empregados, existindo uma carência de estudos mais aprofundados (MIANI; ZARPELÃO; MENDES, 2015).

A família de normas ISO/IEC de segurança da informação apresenta um conjunto de controles. Porém estudos que demonstrem se sua aplicação realmente afeta na maturidade de segurança da informação da corporação, assim como os alinhando à Governança de TIC ainda são escassos.

Formas de mensuração da governança de TIC de uma corporação têm sido exploradas, por exemplo a abordagem de Almeida Neto et al. (2015a), como forma de se analisar a situação da corporação, assim como a possibilidade de comparar o nível dela com outras. Tal aspecto pode ser útil para agregar valor à empresa, como pode ser visto em casos de análises para mercado de ações, vendas, fusões, etc. A área de engenharia e qualidade de softwares também são exemplos que utilizam com constância níveis de qualidade e maturidade para diferenciar empresas e produtos.

Diante do contexto citado, o problema de pesquisa que tem motivado o desenvolvimento deste trabalho está, principalmente, relacionado aos desafios da área de maturidade e priorização como apoio à governança e gestão de um domínio complexo, amplo e multidisciplinar: o domínio da Segurança da Informação.

Esta pesquisa pretende explorar a lacuna supracitada como uma oportunidade para expandir e explorar tal paradigma respondendo o questionamento:

Como mensurar e priorizar a segurança da informação corporativa com base nos atuais arcabouços existentes na área?

Para responder este questionamento foi concebida uma proposta de solução, descrita na próxima seção, que é norteada pelos objetivos detalhados em seguida.

1.4 Proposta de Solução

O presente trabalho está voltado a abordar os desafios de adoção e melhoria contínua da área de segurança da informação em organizações de natureza variadas, através da concepção, definição e avaliação de uma estratégia para a segurança da informação corporativa abordando as áreas de priorização e maturidade concebida, principalmente, segundo os princípios expostos na família de normas ISO/IEC 27.000 e no COBIT, de forma a subsidiar melhorarias na área de segurança da informação, sua gestão e governança.

A partir deste cenário, surge então a proposta de concepção de uma estratégia dedicada à avaliação de maturidade e priorização da segurança da informação no ambiente corporativo. Essa estratégia, através, principalmente, da ISO/IEC 27.001 (ABNT, 2013a) e 27.002 (ABNT, 2013b) que abordam a implantação e gestão da segurança da informação, bem como a ISO/IEC 27.005 (ABNT, 2011), que versa sobre a área de gestão de risco, visa propor um arcabouço para que se possa, na área de segurança da informação:

- Mensurar a situação atual da empresa;

- Apontar áreas com maior desenvolvimento;
- Apontar áreas com maior carência;
- Comparar se as ações implantadas impactaram na corporação de forma a aumentar seu nível de maturidade;
- Comparar empresas variadas;
- Priorizar as ações de segurança da informação de acordo com a criticidade;
- Planejar o caminho para que a organização atinja patamares melhores na área de segurança da informação;
- Auxiliar os gestores na tomada de decisão através da estratégia proposta.

Além dos pontos expostos, percebe-se, como já apresentado na problemática em questão, a dificuldade existente devido ao grande quantitativo de normas e controles que gera dificuldades em sua implantação e, quando implantados, uma burocracia, em alguns casos desnecessárias, nos processos. Neste sentido é possível observar um conflito entre o formalismo apresentado pela maioria destas iniciativas e a agilidade imposta por um mercado cada vez mais competitivo.

Em meados de 2001, pode-se observar, na área de desenvolvimento de software, uma dicotomia semelhante. Naquele período, metodologias como a Rational Unified Process (RUP), tidas como precursoras ao desenvolvimento de software (KRUCHTEN, 2004), também se depararam com um dilema parecido. Este problema motivou o surgimento do Manifesto for Agile Software Development (BECK et al., 2001), manifesto que abordou um conjunto inovador de valores e princípios, promovendo uma quebra de paradigmas.

Com essa mesma perspectiva, a área de Governança de TIC vem sofrendo com os processos lentos e já surgem estudos de uma visão ágil e prática da mesma utilizando alguns princípios do Manifesto Ágil, entre os quais pode-se citar Almeida Neto et al. (2015a), Ramlaoui, Semma e Dachry (2015) e Luna et al. (2016).

Dessa forma, a estratégia proposta também se debruçará sobre o ramo da praticidade e agilidade de modo a se nortear em tais princípios e ideais como um possível meio de minimizar problemas referentes ao formalismo dos modelos e arcabouços atuais utilizados na área de segurança da informação.

1.5 Objetivos

O objetivo principal deste trabalho é propor uma estratégia para avaliação da maturidade e priorização da segurança da informação no ambiente corporativo através da utilização, em conjunto, dos principais arcabouços existentes na área.

A estratégia proposta deve:

- Auxiliar na análise da situação atual da segurança da informação no ambiente corporativo;
- Acompanhar a evolução, através de estágios, da segurança da informação na corporação ou em seus setores;
- Prover subsídios para a gestão e governança da segurança da informação através da priorização de seus controles mais críticos para o ambiente corporativo.

O referido objetivo principal pode ser desdobrado em objetivos específicos onde se destacam os seguintes:

i. Consolidar uma visão geral de iniciativas para evolução de maturidade na área de segurança da informação;
ii. Compreender como a segurança da informação é tratada, nos diversos aspectos que abrangem essa área, no meio corporativo;
iii. Propor um meio para diminuir a burocracia e formalismos dos modelos atuais aplicados na área de segurança da informação, norteado pelos princípios de governança ágil de TIC;
iv. Definir uma estratégia para avaliação da maturidade da segurança da informação na corporação;
v. Definir uma estratégia para priorização das ações de segurança da informação;
vi. Propor um guia simplificado de controles para concepção de uma PSI e de um SGSI;
vii. Auxiliar a melhoria contínua do SGSI da empresa.

1.6 Organização do Trabalho

O trabalho prossegue dividido em mais cinco Capítulos. No próximo Capítulo será explanada a abordagem, técnicas e métodos utilizados. O Capítulo 3 apresentará a fundamentação teórica no que tange à segurança da informação, governança de TIC, ágil e de segurança da informação, modelos de maturidade, as principais normas para este trabalho da família de normas ISO/IEC 27.000 e, por fim, os trabalhos correlatos e principais influenciadores.

O Capítulo 4 abordará a análise descritiva dos dados coletados com as empresas. Enquanto o Capítulo 5 apresentará o artefato concebido e sua evolução.

O Capítulo 6 remeterá às considerações finais do trabalho, demonstrando uma síntese dos objetivos propostos e a forma de tratamento de cada um deles. Também será demonstrada as principais contribuições, limitações e dificuldades e, por fim, um conjunto de possíveis trabalhos futuros.

Como complemento, tem-se as referências e apêndices do presente trabalho.

2 METODOLOGIA DE PESQUISA

Definir corretamente os aspectos da abordagem, método, técnicas e ferramentas adequados à pesquisa científica não é uma tarefa simples, pois a escolha de determinado aspecto pode auxiliar ou inviabilizar a realização da pesquisa (ARAÚJO, 2009). De acordo com Marconi e Lakatos (2010), corroborado por Mendonça (2007) e Araújo (2009) a pesquisa é um procedimento formal que utiliza métodos para constituir caminhos com objetivo de se conhecer a realidade ou descobrir verdades parciais. O método deve ser entendido como um conjunto de atividades racionais e sistemáticas que permitem alcançar os objetivos pretendidos ou traçar o caminho a ser percorrido auxiliando as decisões do pesquisador.

O presente Capítulo está dividido em sete seções. Na primeira Seção a pesquisa será classificada e as principais etapas metodológicas serão apresentadas. A seguir, na Seção 2.2, serão apresentados o desenho metodológico e a estrutura de tomada de decisão, bem como o motivo de suas escolhas, de acordo com Wohlin e Aurum (2015). Na terceira Seção, as etapas de revisão da literatura serão exibidas. Na Seção 2.4 será explicitada a Design Science Research (DSR) com suas escolhas metodológicas e etapas desenvolvidas. Na quinta Seção será explanado o survey realizado e as características de sua amostra e avaliação de dados foram detalhadas. Na Seção 2.6 a avaliação da pesquisa será abordada, com ênfase na utilização de especialistas e na execução do grupo focal. E, por fim, na última Seção, uma síntese do capítulo será apresentada.

2.1 Classificação e Etapas Metodológicas

De acordo com Gil (2010, p. 1), "a pesquisa é desenvolvida mediante o concurso dos conhecimentos disponíveis e a utilização cuidadosa de métodos e técnicas de investigação científica". As pesquisas podem ter diversas classificações e estão divididas pela forma como o problema é abordado, quanto ao objetivo para o qual a pesquisa é realizada e em relação aos procedimentos utilizados para a coleta e análise dos dados.

Diante do exposto, a pesquisa em questão, que visou estabelecer uma estratégia para avaliação da maturidade e priorização da segurança da informação no ambiente corporativo, tem sua abordagem metodológica inserida no Quadro 1.

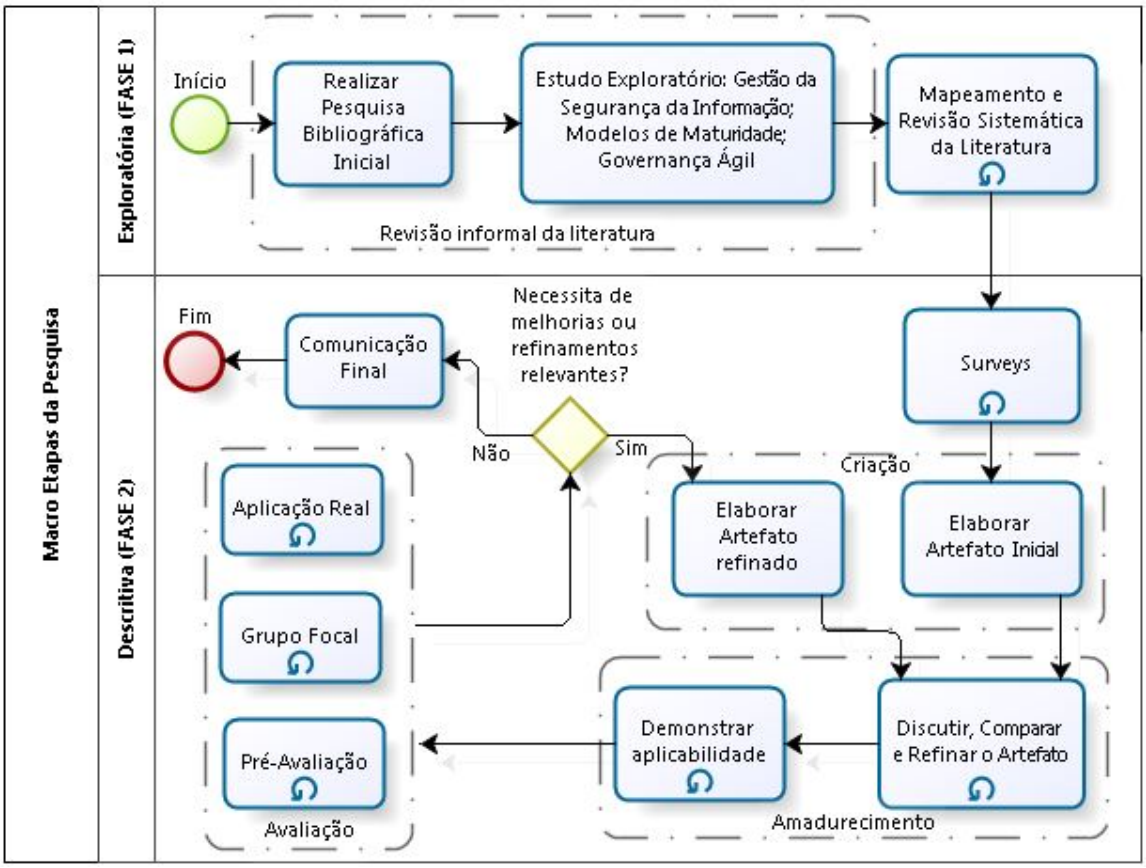
A execução da pesquisa foi realizada em atividades divididas em duas etapas distintas. A primeira etapa consistiu de uma fase exploratória e teve por objetivo a construção de uma base teórica consistente para suportar a etapa seguinte. A fase 2 apresenta uma característica mais descritiva e visa a real construção da estratégia proposta. As atividades estão detalhadas na Figura 2.

Como forma mais didática, as atividades foram estruturadas em blocos. Existindo um bloco inicial de revisão da literatura na fase explanatória. Na fase descritiva definiu-se

Quadro 1 – Classificação Metodológica

Característica	Classificação da Pesquisa
Objetivo	Exploratória e Descritiva
Procedimentos Técnicos	Pesquisa bibliográfica, Mapeamento Sistemático da Literatura (MSL), Revisão Sistemática da Literatura (RSL), Design Science Research (DSR), Levantamento (survey) e Grupo Focal.
Abordagem	Quanti-qualitativa
Áreas de Concentração	Ciência da Computação: Sistemas de Informação / Segurança da Informação

Figura 2 – Macro Etapas Metodológicas da Pesquisa



Fonte: autor.

o bloco de criação (contemplando a elaboração inicial e refinada dos artefatos), a fase de amadurecimento (contemplando análises, debates e melhoramentos do artefato) e, por fim, a fase de avaliação. Dependendo da versão a ser avaliada, um ou mais processo foram realizados, por exemplo, levantamento de dados com empresas e especialistas, publicação e participação em periódicos e eventos, grupo focal e aplicação real do artefato.

Vale salientar que, mesmo a figura apresentando de forma sequencial, algumas etapas foram executadas de forma contínua e paralela, interferindo, se necessário, em outras etapas. Por exemplo, a etapa de Mapeamento e Revisão Sistemático da Literatura, que,

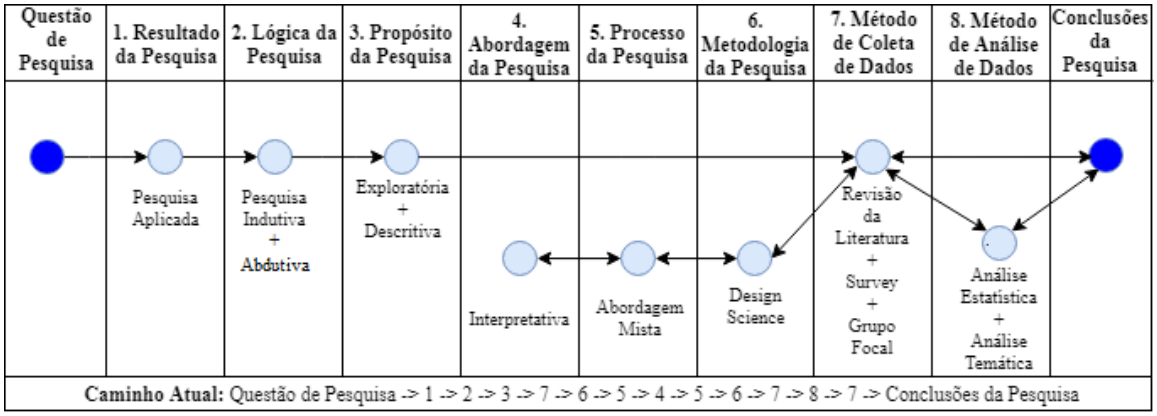
mesmo após a aplicação dos surveys, perdurou analisando os trabalhos publicados até o final do ano de 2017, possibilitando, uma melhor comparação no bloco de amadurecimento do artefato. Tais etapas que podem se repetir ou podem ser realizadas de forma contínua são representadas na Figura 2 com o símbolo de loop.

Os procedimentos metodológicos para elaboração, aplicação e descrição da pesquisa serão detalhados a seguir.

2.2 Desenho Metodológico e Estrutura de Tomada de Decisão

Seguindo a abordagem de Wohlin e Aurum (2015), a presente pesquisa se classifica de acordo com o exposto na Figura 3.

Figura 3 – Desenho Metodológico e Estrutura de Tomada de Decisão



Fonte: autor.

As justificativas para os resultados de cada ponto de decisão propostos por Wohlin e Aurum (2015) são exibidas a seguir.

2.2.1 Resultado e Lógica da Pesquisa

A pesquisa configurou-se como aplicada, visto que o resultado da pesquisa, a estratégia proposta, fornece uma solução para um problema específico, utilizando o conhecimento com o objetivo de melhorar a prática ou aplicação existente.

Categorizada como lógica da pesquisa do tipo abdutiva por ter um processo criativo e de inovação, produzindo um artefato novo. Também tem seu viés indutivo por basear-se em argumentos indutivos (fatos ou experiências), passando do conhecimento específico para o geral. Utilizando conceitos teóricos e padrões de dados observados para o desenvolvimento de algumas conclusões, soluções ou teorias gerais. Gil (1999) corrobora ao afirmar que o método indutivo tem seu resultado derivado de um conjunto de observações repetidas de casos particulares. Tais observações de fatos e fenômenos são analisadas, comparadas e por fim chega-se a conclusões prováveis e generalizáveis (GIL, 1999).

2.2.2 Propósito da Pesquisa

Quanto ao propósito ou objetivos, a pesquisa pode ser exploratória, descritiva ou explicativa (GIL, 1999). O presente trabalho foi categorizado como exploratório e descritivo.

Este trabalho é exploratório por ser aplicado em uma área sem muitas informações disponíveis, sendo necessária a coleta e levantamento de informações sobre o problema. Esta etapa teve por objetivo explorar a área do problema e fornecer informações básicas que possam ser usadas para uma segunda fase, descritiva.

A pesquisa exploratória é indicada quando se quer ter mais familiaridade com um tema e aprofundá-lo posteriormente. Geralmente inclui um levantamento com pessoas que já tiveram alguma experiência prática com o assunto que está sendo pesquisado (MASCARENHAS, 2012; GIL, 2010).

Após o levantamento da fase exploratória, a presente pesquisa deu continuidade visando descrever o fenômeno e as características do problema. Aprofundando a fase exploratória e categorizando-se, também, como descritiva.

A pesquisa descritiva tem como principal instrumento de coleta o questionário e a observação e visa descrever características de uma população ou de um fenômeno, identificando se há relações entre as variáveis estudadas (MASCARENHAS, 2012).

2.2.3 Abordagem e Processo da Pesquisa

No que tange à abordagem, a pesquisa foi inserida como interpretativa. Visto que visou compreender as atividades humanas e corporativas em seus contextos naturais, tendo etapas subjetivas e analisando o resultado através da perspectiva das pessoas e empresas que responderam aos eventos e questionamentos através de processos quantitativos e qualitativos. Tendo, portanto, um processo de pesquisa com abordagem mista (quanti-quali).

Para Mascarenhas (2012), no que tange ao processo, a pesquisa pode seguir duas vertentes: a pesquisa quantitativa e a pesquisa qualitativa. Para fazer a escolha correta, é necessário fazer uma observação sobre o objeto que está sendo estudado e se as conclusões serão mais aprofundadas ou terão resultados mais generalistas.

A pesquisa quantitativa baseia-se na quantificação para fazer a coleta dos dados e deve-se utilizar técnicas estatísticas para fazer a análise dos dados obtidos, evitando com isso, que o pesquisador influencie de algum modo os resultados. Esse tipo de pesquisa é útil quando se pretende dar mais confiabilidade e poder de generalização aos resultados (MASCARENHAS, 2012).

Já a pesquisa qualitativa, é utilizada quando se quer descrever com mais detalhes o objeto que está sendo estudado, nela os dados são analisados ao mesmo tempo em que são coletados, tornando o estudo mais descritivo e voltado para a compreensão do objeto. Nesse tipo de pesquisa a influência do pesquisador não é só permitida, como considerada fundamental (MASCARENHAS, 2012).

Mascarenhas (2012) ainda salienta que a pesquisa não deve obrigatoriamente seguir um único modelo, para a abordagem de alguns problemas muitas vezes é aconselhável combinar os dois tipos para ter uma pesquisa mais completa.

2.2.4 Metodologia da Pesquisa

Gil (1999) chama esta etapa de delineamento da pesquisa, que consiste no "planejamento da pesquisa em sua dimensão mais ampla" (GIL, 1999, pp. 64).

Para fazer o referido planejamento, o método de pesquisa escolhido foi Design Science Research (DSR). O DSR foi selecionado por ser propício para construção e avaliação de artefatos que visam atender aos requisitos de um problema. Sendo o artefato de saída uma construção, modelo, método, instanciação ou estratégia nova. No presente caso é a construção da estratégia proposta para a área de segurança da informação.

Um maior detalhamento desta etapa será exibido na Seção 2.4.

2.2.5 Método de Coleta de Dados

Segundo Mascarenhas (2012), as pesquisas também podem ser classificadas quanto à forma de coletar e analisar os dados, assim se dividem, tradicionalmente, nos seguintes grupos: pesquisa bibliográfica, documental, pesquisa de levantamento (survey), estudo de caso, pesquisa-ação e pesquisa participante.

Quanto ao método de coleta de dados, foi realizada a revisão da literatura, em primeira instância de forma ad hoc, posteriormente um Mapeamento Sistemático da Literatura (MSL) e, por fim, análise das Revisões Sistemáticas da Literatura RSL. As três etapas de revisão da literatura foram importantes para identificar as pesquisas existentes e áreas com carência de pesquisas e soluções. Em cada etapa da revisão da literatura (ad hoc, MSL e RSL) foi-se afunilando os assuntos.

Foi utilizado também o método de survey para levantamento dos dados do mundo corporativo, avaliação e criação da estratégia proposta e, por fim, utilizou-se a técnica de grupo focal como avaliação da estratégia proposta.

Os métodos citados terão maior detalhamento em seções específicas (Seções 2.3, 2.5 e 2.6).

2.2.6 Método de Análise de Dados

Por fim, no que tange aos pontos de decisão propostos por Wohlin e Aurum (2015), a pesquisa utilizou, como método para análise de dados, a análise estatística descritiva para analisar os dados oriundos dos surveys e a análise temática para tratamento dos dados da fase de grupos focais e questões específicas nos surveys.

2.3 Revisão da Literatura

A revisão da literatura foi realizada em três etapas, funcionando com um funil. Sendo a primeira etapa mais ampla e a última mais focada no tema da presente pesquisa. Na primeira etapa foi realizada uma pesquisa bibliográfica informal (ad hoc) para análise dos trabalhos existentes e direcionamento inicial da presente pesquisa. Passando para um estudo exploratório nas áreas de interesse, como apresentado na Figura 2. Os resultados desta etapa serviram para encontrar as lacunas existentes na literatura e refinar a pergunta de pesquisa e os objetivos propostos.

Com o refinamento inicial da pesquisa concluído, foi realizado o Mapeamento Sistemático da Literatura para as áreas de governança, gestão e maturidade em segurança da informação no período de 10 anos (2008 até 2017). Os detalhes e resultados da pesquisa podem ser observados nos artigos publicados, especialmente em Alencar et al. (2018b) e Alencar et al. (2018c).

Para finalizar, foram analisados as seguintes revisões sistemáticas da literatura encontradas referentes ao tema: Rios (2016), De Lima (2017), Cordeiro (2017) e Rea-Guaman et al. (2017), conforme detalhado no Quadro 2.

Quadro 2 – RSL Analisadas

Autores	**Assunto Principal**	**Período**
Rios (2016)	Política (PSI)	2010 - 2015
De Lima (2017)	Maturidade	2005 - 2016
Cordeiro (2017)	Maturidade	2010 - 2016
Rea-Guaman et al. (2017)	Maturidade	2012 - 2017

Em síntese, a revisão da literatura realizada neste trabalho consistiu em:

i. Pesquisa informal por parte do autor;

ii. Mapeamento Sistemático da Literatura (MSL) realizada pelo autor e parceiros (ALENCAR et al., 2018b; ALENCAR et al., 2018c);

iii. Análise de revisões sistemáticas da literatura (RIOS, 2016; DE LIMA, 2017; CORDEIRO, 2017; REA-GUAMAN et al., 2017).

O processo de revisão da literatura composto pelas três etapas supracitadas resultou na seleção e análise de 102 trabalhos distintos (Apêndice J), além das próprias RSLs selecionadas, que auxiliaram nas definições, deram suporte e guiaram a presente pesquisa.

2.4 Design Science Research

A Design Science Research é o método que operacionaliza a pesquisa realizada sob o paradigma da Design Science, fundamentando a condução da pesquisa quando o objetivo

a ser alcançado é desenvolvimento de um artefato (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015).

A Design Science é a criação e a investigação de artefatos no contexto. Visto que os artefatos estudados na DSR são projetados para interagir com um ambiente de problema, a fim de melhorar algo nesse contexto (WIERINGA, 2014). Pensamento bem semelhante ao de Hevner et al. (2004) que apontam que a Design Science cria e avalia artefatos destinados a resolver problemas, busca fazer contribuições para pesquisas, para avaliar projetos e para comunicar os resultados para os públicos-alvo.

A Design Science Research busca preencher a falta de uma metodologia para servir como modelo aceito e válido para o desenvolvimento de artefatos. A DSR incorpora princípios, práticas, e procedimentos necessários para realizar tais pesquisas (PEFFERS et al., 2007), sendo citada, por estes autores, como Design Science Research Methodology (DSRM).

A DSR tem como objetivo estudar, pesquisar e investigar o artificial e seu comportamento, tanto do ponto de vista acadêmico quanto da organização. Constituindo-se como um processo rigoroso de projetar e avaliar artefatos para resolver problemas reais e diminuir a lacuna entre a teoria e a prática (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015).

Dresch, Lacerda e Antunes Júnior (2015) apontam que as pesquisas que utilizam a DSR devem prezar por dois fatores fundamentais para o sucesso: o rigor científico e a relevância para as organizações. Ou seja, a pesquisa deve ser aplicada e trazer melhorias ao ambiente. Para isso deve utilizar técnicas e fundamentos consolidados.

A DSR é orientada à solução de problemas específicos, não necessariamente buscando a solução ótima, mas sim, a solução satisfatória para a situação, sendo passível de generalização dentro de uma mesma classe de problemas (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015).

O processo de proposição de artefatos é essencialmente criativo. Porém, torna-se necessário ao pesquisador, além da criatividade, fazer uso dos seus conhecimentos prévios, visando propor soluções robustas que possam ser utilizadas para melhoria do ambiente atual, através da resolução do problema que está sendo estudado (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015).

Hevner et al. (2004) apontam como instruções gerais para a Design Science Research:

i. Design como Artefato;

ii. Relevância do Problema;

iii. Avaliação do Design;

iv. Contribuições do Design;

v. Rigor da Pesquisa;

vi. Design como um processo de pesquisa;

vii. Comunicação da Pesquisa;

Tais pontos também são demonstrados e debatidos em diversos trabalhos, entre eles o de Sordi, Meireles e Sanches (2010) que apontaram, em menos de uma década atrás, a incipiência da utilização do método de Design Science Research. Podendo ser considerado novo dentre os métodos de pesquisa.

Já Dresch, Lacerda e Antunes Júnior (2015), baseado na literatura existente, elencaram oito elementos principais que compõem a DSR, são eles:

i. Definição do problema;

ii. Revisão da literatura ou busca por teorias existentes;

iii. Sugestões de possíveis soluções;

iv. Desenvolvimento;

v. Avaliação;

vi. Decisão sobre a melhor solução;

vii. Reflexão e aprendizagens;

viii. Comunicação dos resultados.

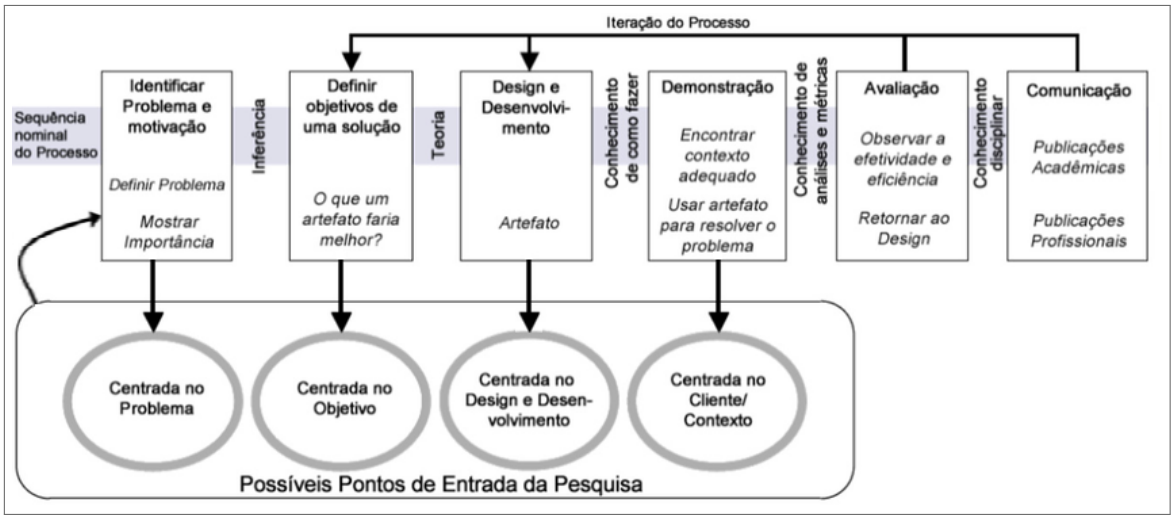
Percebe-se que os oito elementos citados formam uma sequência lógica de solução de um problema, partindo de sua concepção, análise do que já existe, desenvolvimento, avaliação, análises e reflexões da solução e a comunicação.

Dentre os treze trabalhos analisados por Dresch, Lacerda e Antunes Júnior (2015, p. 92), todos apontam, em sua estrutura, a necessidade de três etapas: Definição do problema (i), Sugestões de possíveis soluções (iii) e Desenvolvimento (iv). Ressalta-se também a importância da etapa de Avaliação (v), citada por onze dos treze trabalhos. Por fim, verificou-se que nenhum trabalho citado apresenta uma estrutura de Design Science Research completa, realizando, explicitamente, as oito etapas elencadas por Dresch, Lacerda e Antunes Júnior (2015).

Segundo Peffers et al. (2007), a DSR, como um processo metodológico, deve possuir seis etapas, conforme Figura 4.

Embora as atividades sejam inseridas de forma sequencial na representação de Peffers et al. (2007), não é imposta pelos autores uma ordem exata para o início da pesquisa. Sendo este um de seus grandes diferenciais, possibilitando que o início da pesquisa possa ocorrer em quatro pontos distintos, como apresentado na Figura 4, considerando o foco que se pretenda dar à investigação (PEFFERS et al., 2007). A presente pesquisa é centrada no problema, visto que a ideia central deste trabalho emergiu de problemas já existentes

Figura 4 – Modelo do Processo da Design Science Research



Fonte: Tradução de Peffers et al. (2007, p. 54)

no mercado. Dessa forma, o processo metodológico seguiu a sequência a seguir (PEFFERS et al., 2007; JAPPUR, 2014, p. 43):

i. Identificar o problema e sua motivação: define-se o problema de pesquisa específico e justifica-se o valor de sua solução, desde que a definição do problema seja usada para desenvolver um artefato que pode efetivamente oferecer uma solução. Os recursos necessários para esta atividade incluem o conhecimento do estado da arte do problema e da importância de sua solução.

ii. Definir os objetivos para uma solução: a partir da definição do problema e do conhecimento do que é viável e exequível, definem-se os objetivos da solução proposta. Recursos necessários para isso incluem o conhecimento do estado da arte dos problemas e das soluções, se existirem.

iii. Projetar e Desenvolver: determina-se e cria-se o artefato. Os recursos necessários para sair dos objetivos e chegar ao design e desenvolvimento inclui o conhecimento da teoria que pode ser exercida em uma solução.

iv. Demonstrar: demonstra-se o uso do artefato, resolvendo uma ou mais instâncias do problema. Isso pode envolver seu uso por meio de um experimento, simulação, estudo de caso, prova ou outra atividade apropriada. Os recursos necessários para a demonstração incluem o conhecimento efetivo de como usar o artefato para resolver o problema.

v. Avaliar: observa-se e mensura-se como o artefato atende à solução do problema, comparando se os objetivos que foram propostos para a solução foram atendidos. Essa atividade consiste em sua essência em comparar os objetivos de uma solução com os resultados obtidos com o uso do artefato. Dependendo da natureza do

problema e do artefato, a avaliação pode assumir muitas formas. Nesta atividade, os pesquisadores podem decidir se voltam a repetir o passo três e/ou quatro para tentar melhorar a eficácia do artefato ou para continuar com a comunicação.

vi. Comunicar: divulga-se o problema e sua relevância, o artefato concebido, sua utilidade e ineditismo, o rigor de sua concepção e a sua efetividade, para outros pesquisadores e outros públicos-alvo, quando isso for apropriado.

De uma forma geral percebe-se uma visão da DSR como um ciclo que, atendendo ao rigor necessário, contempla a definição e análise do problema, a verificação de uma possível solução (devendo o problema e a solução serem aplicáveis aos conceitos da DSR), ciclos para criar e avaliar o artefato até chegar a uma possível solução que deverá ser verificada se atende satisfatoriamente ao problema, reiniciando o ciclo se for necessário. Visões da DSR como ciclo, não exatamente iguais, mas com essências semelhantes são vistas em Hevner et al. (2004), Peffers et al. (2007), Hevner (2007), Alturki, Gable e Bandara (2011), Lacerda et al. (2013), Wieringa (2014) e Dresch, Lacerda e Antunes Júnior (2015).

Entre as orientações propostas para a utilização da Design Science Research, optou-se, para o presente trabalho, os procedimentos estabelecidos por Peffers et al. (2007). Porém pela convergência das propostas, pode-se afirmar que o mesmo também atendeu os oito elementos principais elencados por Dresch, Lacerda e Antunes Júnior (2015), bem como as instruções de Hevner et al. (2004). Por fim, também foi verificado que o trabalho atendeu aos parâmetros de verificação do rigor da Design Science Research propostos por Dresch, Lacerda e Antunes Júnior (2015), são eles:

i. Ter um problema de pesquisa relevante;

ii. Ser gerado um artefato como produto da pesquisa;

iii. Avaliar o artefato;

iv. Ter uma solução passível de generalização;

v. Rigor na condução do método.

2.5 Survey

A primeira etapa de coleta de dados da pesquisa buscou o entendimento do atual ambiente de TIC e segurança da informação nas empresas e uma simplificação dos controles da ISO/IEC 27001 e 27002, o instrumento de coleta de dados foi o survey, que é um meio de documentação direta para obter respostas a questões de forma que o próprio informante o preencha (GIL, 2010; MARCONI; LAKATOS, 2010).

Um survey é considerado um método tradicional de pesquisa, de abordagem quantitativa e tem como objetivos explorar, descrever e explicar. Tal método foca em descrever um fenômeno, testar alguma teoria ou avaliar o comportamente de pessoas ou de um ambiente, podendo ser utilizado em conjunto com a Design Science Research nestas etapas (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015). Wieringa (2014) corrobora apontando a técnica como um meio para investigação do problema e posterior avaliação na DSR.

As perguntas inerentes ao levantamento inicial foram realizadas através de dois questionários (Apêndices B e C). O primeiro (Apêndice B), tratado neste trabalho como Questionário 1, é uma aplicação do documento utilizado por Alencar (2011), Alencar, Queiroz e Queiroz (2013a) e Alencar, Queiroz e Queiroz (2013b). Questões que também basearam Silva Neto, Alencar e Queiroz (2015). Sendo composto pelas mesmas 43 questões divididas em seis categorias, sendo elas:

- Dados da empresa;
- Dados do respondente;
- Importância estratégica da informação;
- Ferramentas de SI na empresa;
- Recursos humanos e estrutura organizacional;
- Segurança da informação corporativa.

E adicionada ao final, mais cinco questões, inerentes à amplitude da pesquisa atual.

O segundo questionário (Apêndice C), tratado neste trabalho como Questionário 2, entregue na mesma etapa, consta do nome da empresa (para correlacionar com o primeiro) e os 114 controles da versão de 2013 ISO/IEC 27001 e 27002. Para os controles foram utilizados uma escala likert de cinco níveis em uma escala de 1 (nenhuma importância) a 5 (muito importante), sendo a nota 3 categorizada como neutro na escala. Questionário semelhante é utilizado por Silva Neto, Alencar e Queiroz (2015), porém o mesmo colocava a versão anterior da ISO/IEC 27002 (de 2005) que contemplava 133 controles.

Na construção do questionário alguns aspectos foram considerados a fim de manter uma padronização nas questões apresentadas. Por exemplo, as questões que apresentaram alternativas de respostas, foram dispostas em ordem alfabética de modo a não induzir o respondente, com exceção dos casos em que há uma ordem crescente ou lógica das alternativas (por exemplo, escala likert).

Não foi estipulado tempo para a resolução das questões. Os questionários foram construídos e disponibilizados, inicialmente, nas ferramentas de formulário e planilha do Google, como teste. Posteriormente foi disponibilizado no site de uma empresa parceira que

atua no ramo de serviços e consultorias em tecnologia da informação e segurança da informação. Sendo encaminhado por e-mail o link e o documento em anexo ou, em diversos casos, entregue impressos.

A escolha da utilização de questionários impressos ou anexados ao invés de utilizar apenas os questionários digitais publicados em sites se deu por questões de segurança e controle, pois, na opção online, teve-se uma resistência maior para conceder as informações sobre a área de segurança. Outro fato importante na aplicação manual de questionários é a possibilidade de conferir algumas respostas (rasuradas, por exemplo) e, principalmente, tentar convencer os respondentes a chegar ao final do questionário respondendo todas as questões. Por ser questionários longos, muitas vezes tinha-se problema com expirar a sessão ou erros na conexão de internet, resultando perdas nos questionário on-line.

Em todos os casos junto com o questionário foi enviado o termo de consentimento livre e esclarecido (Apêndice A). Este termo foi utilizado em todas as etapas de pesquisa e tinha as variáveis de nome da etapa, data e tempo ajustada de acordo com a etapa em questão. No Apêndice A está o exemplo utilizado na última etapa, do grupo focal.

Dresch, Lacerda e Antunes Júnior (2015) abordam que diversas técnicas para coleta de dados podem ser utilizadas na DSR, entre elas o questionário.

> "O questionário consiste na aplicação de uma série de perguntas a um entrevistado. Recomenda-se que ele responda ao questionário por escrito, para facilitar análise posterior das resposta pelo pesquisador" (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015, p. 34).

Após a análise dos dados obtidos pelos Questionários 1 e 2 (Apêndices B e C), bem como da etapa de revisão da literatura, os artefatos foram construídos e evoluídos. Para cada versão do artefato central gerado, um breve questionário foi enviado como meio de avaliação inicial e confirmação do caminho a seguir.

2.5.1 Amostra

Segundo Marconi e Lakatos (2010) o universo ou população é um conjunto de seres animados ou inanimados que podem ser unidos ou classificados por apresentarem, ao menos, uma característica em comum. Gil (2010) segue uma linha de pensamento similar ao afirmar que o universo ou população da pesquisa é um conjunto definido de elementos que possuem características similares e que a análise de uma parte representativa possibilita a compreensão do todo ou servirá para o estabelecimento de uma base em estudos posteriores mais sistêmicos e precisos.

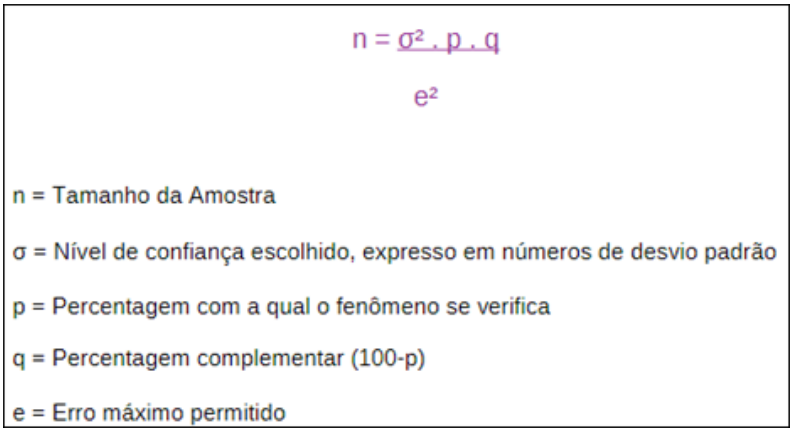
Para Gil (2010) e Marconi e Lakatos (2010) as pesquisas científicas podem abranger um universo de elementos tão grande que se torna impossível considerá-lo em sua totalidade. Bem como deve-se analisar o custo, normalmente alto, para a realização de uma operação censitária, que englobam todo o universo. Por essas razões, é frequente a utilização de amostras, ou seja, pequena parte dos elementos que compõe o universo. A

amostra é, portanto, um subconjunto do universo, convenientemente selecionado, que deve ser o mais representativo possível do todo para que resultados e características obtidos na porção estudada possam ser considerados como verdade para todo o escopo da população pesquisada. Gil (1999) afirma que existem quatro fatores que podem determinar o tamanho da amostra a ser utilizada:

- A amplitude do universo: classificada como finita quando não excede a 100.000 elementos ou infinita quando excede a 100.000 elementos;
- O nível de confiança: refere-se à área da curva "normal" definida a partir dos desvios-padrão em relação à sua média. Nesta situação um desvio-padrão corresponde a aproximadamente 68,0% da área total da curva. Dois desvios correspondem a aproximadamente 95,5% e três desvios correspondem a aproximadamente 99,7%. O valor da área representa o nível de confiança;
- O erro máximo permitido: erro de medição que diminui na proporção em que aumenta a amostra. É expresso em termos percentuais e, normalmente, varia entre 3,0% e 5,0% em pesquisas sociais, podendo ser maior em outros tipos de pesquisas;
- A percentagem com que o fenômeno se verifica: é a estimação prévia da percentagem com que se verifica o fenômeno.

Segundo o Cadastro Central de Empresas (IBGE, 2018), existem no Brasil 5.050.615 de empresas ou outras organizações. As empresas com 0 a 9 funcionários contabilizam 4.425.763 (IBGE, 2018), mesmo retirando essas empresas de menor porte, sobram mais de 600 mil (precisamente 624.852) possíveis participantes. Portanto será utilizada a fórmula para o cálculo de amostras para populações infinitas (excede a 100.000 elementos) considerada na teoria da amostragem exposta em Gil (1999), conforme Figura 5.

Figura 5 – Fórmula para Cálculo da Amostra



Fonte: Gil (1999, p. 106)

Salienta-se que ao mencionar no trabalho os integrantes da amostra como "empresa", refere-se a todos os integrantes, indiferente de sua classificação, porte ou abrangência.

Como características comuns utilizadas para delimitar a amostra utilizada na pesquisa, as empresas deveriam ter, no mínimo, quinze funcionários. Também deveria ser da área de TIC ou ter, ao menos, uma área específica de TIC ou terceirização específica para a área de Gestão ou Governança de TIC ou da Segurança da Informação. A quantidade mínima de funcionários foi estabelecida por presumir que empresas com menos de quinze funcionários, em sua maioria, não teriam procedimentos ou preocupações formais com a segurança da informação. Tal motivo foi o mesmo para se impor a exigência de ser uma empresa da área de TIC ou ter departamento específico de TIC, fatores também utilizados por Alencar (2011), Alencar, Queiroz e Queiroz (2013a) e Alencar, Queiroz e Queiroz (2013b).

Ressalta-se, também, que o respondente deverá ser da área de TIC ou responsável por ela. Preferencialmente, o responsável pela área de Segurança da Informação na empresa.

Como definição inicial para o survey, foi utilizada uma amostragem não-probabilística por acessibilidade ou conveniência (GIL, 1999). Visto que, mesmo grande parte da amostra sendo escolhida ao acaso, não houve o contato com todas as possíveis empresas (população) garantindo condições iguais de participar da amostra.

Com intuito de diversificar ao máximo a amostra, chegando mais próxima a amostragem probabilística, foi utilizado os contatos do autor, banco de clientes de empresas parceiras e, por fim, listas e grupos de contatos profissionais. No caso dos contatos do autor e das listas e grupos foi solicitado que respondessem aos questionários, como também, indicações de possíveis novos contatos.

O universo é superior a 100.000 possíveis participantes (população infinita), o percentual em que se admite a ocorrência varia de acordo com as questões utilizadas no questionário. Pegando-se o pior caso, questões binárias, tem-se o percentual de ocorrência de 50%, nível de confiança de 95,5% (corresponde a dois desvios-padrão) e erro máximo (intervalo de confiança) de 8,0%. Resultando, como esses dados, a necessidade de uma amostra mínima de 156 empresas respondentes, conforme cálculo exposto na Equação 2.1.

$$n = \frac{\sigma^2 \times p \times q}{e^2} = \frac{2^2 \times 50 \times 50}{8^2} = \frac{10000}{64} = 156,25 \tag{2.1}$$

2.5.2 Análise dos Dados

A fase de análise de dados tem por objetivo interpretação e explicitação dos dados obtidos na pesquisa, organizando e sumarizando-os de tal forma que possibilite o fornecimento de indícios ou respostas ao problema proposto (GABBAY, 2003; GIL, 2010; JANSSEN, 2008; MARCONI; LAKATOS, 2010).

Para tal análise e demonstração dos resultados obtidos, utilizou-se o modelo de estatística descritiva que, de acordo com Marconi e Lakatos (2010), consiste na tabulação dos dados por meio de frequência e porcentagens das respostas obtidas e apresentação dos dados utilizando um conjunto de gráficos. Tais análises se remetem à amostra citada que, como qualquer pesquisa estatística, pode sofrer com características inerentes ao grupo abordado e não necessariamente do universo amostral como um todo.

Após a análise dos dados, tratamento estatístico descritivo e levantamento dos pontos falhos ou pontos de melhorias no ambiente (Questionário 1 - Apêndice B), o estudo comparou com dados de pesquisas anteriores, obtendo subsídios para o encaminhamento da solução proposta.

Já para os dados do Questionário 2 (Apêndice C) foi calculada a média, mediana e desvio padrão para cada controle questionado, de acordo com a nota selecionada para o mesmo na escala likert de 1 a 5 proposta. Com base nesses dados estatísticos os controles serão ordenados para formulação da estratégia.

2.6 Avaliação da Pesquisa

Os artefatos desenvolvidos a partir de uma pesquisa fundamentada em design são a prova de sua validade (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015, p. 96). Devendo, por sua vez, serem previamente avaliados.

Alturki, Gable e Bandara (2011) corroboram com este tema inserindo que a avaliação na DSR não visa expor o "por quê" ou "como" o artefato funciona, mas sim explicitar se esse artefato desempenha suas funções.

Para as etapas de avaliação da pesquisas foram escutados especialistas (acadêmicos, profissionais da área de TIC e de negócio) e mercado (empresas), ambos os casos utilizando questionário como instrumento. Outras etapas de avaliação foram realizadas através da técnica de grupo focal e fazendo aplicação em caso real. Complementa a avaliação do projeto as reflexões, em particular do autor e do orientador, e apresentações, debates e publicações no Grupo de Pesquisa em Gestão de Projetos (GP2), eventos e periódicos.

Tais ações para avaliação e melhoramento do projeto podem ser dividades em contínuas e pontuais. As contínuas são, principalmente, baseadas nas reflexões do autor e do orientador, nas apresentações e debates no GP2 e na comparação entre os resultados alcançados e trabalhos da literatura. Essas ações foram realizadas no bloco de amadurecimento e na etapa de pré-avaliação da Figura 2.

Tal avaliação contínua é baseada na proposta de Hevner et al. (2004). Denominada como avaliação descritiva e busca, essencialmente, demonstrar a utilidade do artefato desenvolvido. Para tanto, o pesquisador poderá fazer uso de argumentos existentes na literatura ou construir cenários para procurar demonstrar a utilidade do artefato em contextos diversos. Fatos também apresentados por Lacerda et al. (2013) e Dresch, Lacerda

e Antunes Júnior (2015). Comparando com Peffers et al. (2007) a fase aqui nomeada de avaliação contínua está embutida, de certa forma, nas etapas de Demonstração e Avaliação.

As avaliações pontuais são as ações representadas no bloco de avaliação da Figura 2. As avaliações caracterizaram-se pela execução de uma ou mais atividades para cada versão consolidada do artefato. As atividades desta etapa são:

- Avaliação por especialistas (via questionário);
- Avaliação pelas empresas (via questionário);
- Grupo focal com especialistas;
- Submissão de artigos para eventos e periódicos;
- Aplicação real do artefato.

Com exceção das submissões para eventos e periódicos, em todos os outros casos foi enviado o termo de consentimento livre e esclarecido (Apêndice A). Este termo tinha as variáveis de nome da etapa, data e tempo ajustada de acordo com a etapa em questão. No Apêndice A está o exemplo utilizado na última etapa, do grupo focal.

O planejamento do grupo focal, bem como os questionários utilizados para avaliar as últimas versões do artefato (2 e 3) foram baseados em Salah, Paige e Cairns (2014).

Conforme Tremblay, Hevner e Berndt (2010), a pesquisa sustentada pela DSR pode estar voltada ao desenvolvimento do artefato em si, mas, também, em expor evidências de que o artefato poderá ser utilizado para resolver problemas reais. Embora haja uma etapa específica de avaliação do artefato, isso não dispensa que, em etapas intermediárias da condução da DSR, sejam utilizadas avaliações parciais dos resultados (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015). Tal explanação corrobora com o processo proposto nos blocos de amadurecimento e avaliação da Figura 2.

Ao todo foram geradas três versões do artefato para avaliação, culminando na versão atual. O detalhamento das etapas que aconteceram em cada versão avaliada e resultados será explicitado em seções específicas no Capítulo 5.

2.6.1 Especialistas

Para seleção dos especialista para compor as etapas de avaliação foram colocadas as seguintes características mínimas:

- Ter ao menos 6 (seis) anos de experiência na área de TIC;
- Ter ao menos 4 (quatro) anos de experiência em segurança da informação;

- Ter ao menos 2 (dois) anos de experiência como professor ou palestrante na área de segurança da informação;
- Ter titulação acadêmica (especialização, mestrado ou doutorado) na área de segurança da informação ou notório reconhecimento na área;
- Ter publicação acadêmica ou certificação na área de segurança da informação;
- Preferencialmente ter titulação de mestre ou doutor na área;

É considerada titulação acadêmica na área de segurança da informação quando os cursos são específicos da área de segurança da informação (por exemplo, especialização em segurança da informação) ou quando são na área de TIC e o trabalho de conclusão do autor for na área de segurança da informação (por exemplo, mestrado em computação e a dissertação defendida na área de segurança da informação).

Não existiu impedimento, nesta pesquisa, para o especialista participar em mais de uma fase.

Tais características foram baseadas nas definições propostas por Almeida Neto (2015) e Almeida Neto et al. (2015b) que, por sua vez, foram embasadas pela pesquisa de Farias Júnior (2014).

As atividades com os especialistas foram realizadas nas etapas designadas como pré-avaliação e grupo focal da Figura 2. O detalhamento das características de cada especialista estará explicitado em seção específica no Capítulo 5, exibindo um quadro para cada avaliação com especialistas.

2.6.2 Grupo Focal

Outro procedimento técnico para debate e coleta de informação é a ideia de Grupos Focais, técnica que tem crescido em estudos em diversas áreas nas últimas décadas, podendo ser entendida como uma técnica de investigação qualitativa comprometida com a abordagem metacientífica compreensivista (GONDIM, 2003).

Na mesma linha de pensamento, Kontio, Lehtola e Bragge (2004) afirmam que o método de grupo de focal é uma forma rápida e econômica para obter experiências de profissionais e usuários. Grupos focais são discussões cuidadosamente planejadas, projetadas para obter as percepções dos membros do grupo em uma área de interesse definida. A atividade é guiada e facilitada por um moderador, que segue uma estrutura pré-definida para que a discussão permaneça focada (KONTIO; LEHTOLA; BRAGGE, 2004).

Morgan (1996) define grupos focais como uma técnica de pesquisa que coleta dados por meio das interações em grupo ao se discutir um tópico sugerido pelo pesquisador. Onde, segundo Gondim (2003), o moderador de um grupo focal assume uma posição de facilitador do processo de discussão e da formação de opiniões sobre o tema selecionado. Descrições semelhantes sobre o papel do moderador são encontradas na literatura, entre

elas, Morgan (1996), Tremblay, Hevner e Berndt (2010) e Dresch, Lacerda e Antunes Júnior (2015).

Tremblay, Hevner e Berndt (2010), Lacerda et al. (2013), Wieringa (2014) e Dresch, Lacerda e Antunes Júnior (2015) corroboram com o pensamento supracitado e apontam a aplicação do grupo focal como prática para avaliar os artefatos concebido via Design Science Research. Quanto à sua utilização na avaliação de artefatos da DSR, Dresch, Lacerda e Antunes Júnior (2015) complementam:

> "O grupo focal (focus group) é uma outra importante forma de coletar dados. Técnica de natureza qualitativa, tem como objetivo buscar o entendimento das considerações um grupo de pessoas teve a partir de uma experiência, ideia ou evento. Trata-se de uma entrevista em profundidade, realizada em grupos com sessões estruturadas" (DRESCH; LACERDA; ANTUNES JÚNIOR, 2015, p. 34).

Morgan (1996) afirma que os grupos focais podem ser utilizados para levantamento de dados iniciais, como para avaliar o assunto proposto pelo pesquisador podendo, em ambos os casos, ser associado a outras técnicas, por exemplo, entrevistas individuais, surveys ou experimentos. Combinação de técnicas que também é citada por Carlini-Cotrim (1996), Lacerda et al. (2013) e Dresch, Lacerda e Antunes Júnior (2015) para avaliação de artefatos, inclusive na DSR.

Quanto ao número de participantes do grupo focal, não existe um consenso na literatura sobre um número ideal. O quantitativo recomendado varia entre quatro e oito participantes (KITZINGER, 1995), quatro e dez (GONDIM, 2003), seis e dez (CARLINI-COTRIM, 1996), três e doze (KONTIO; LEHTOLA; BRAGGE, 2004) ou quatro e doze (TREMBLAY; HEVNER; BERNDT, 2010).

Neste impasse, Munaretto, Corrêa e Cunha (2013) afirma que:

> "é necessário haver uma quantidade de participantes que possa favorecer a criação de um ambiente propulsor aos interesses do pesquisador, bem como seus objetivos de estudo. No entanto, não existe um consenso entre os estudiosos sobre essa quantidade ideal de participantes" (MUNARETTO; CORRÊA; CUNHA, 2013, p. 17).

Munaretto, Corrêa e Cunha (2013) ainda insere que o importante é que esses grupos tenham tamanho adequado conforme a disponibilidade de participantes, do pesquisador e considerando a capacidade da infraestrutura disponível para os encontros, cabendo ao pesquisador julgar a quantidade adequada de participantes para a discussão proposta.

Com base no explicitado, para a presente pesquisa foi buscada a quantidade de seis a oito integrantes, de forma a atender a maioria das recomendações encontradas na literatura. Sendo realizado o grupo focal com seis integrantes.

Almeida Neto et al. (2015b, p. 24) utilizou tal técnica em seu estudo e apontou que esta abordagem tem, como principal objetivo "identificar o sentimento de participantes sobre um determinado assunto, produto ou atividade". Tal fato é corroborado por Gondim (2003, p. 160) ao afirmar que a utilização de grupos focais "em organizações formais auxiliam

na introdução de programas, na tomada de decisões, na aprendizagem organizacional, no diagnóstico e avaliação da qualidade de serviços, assim como na geração de novas ideias".

Entre outras finalidades, os grupos focais podem ser utilizados para gerar conhecimento necessário para a avaliação experimental do impacto de produtos em desenvolvimento e de futuros programas a serem implantados em organizações. Sendo vista pelos pesquisadores como uma "técnica que os ajuda na investigação de crenças, valores, atitudes, opiniões e processos de influência grupal, bem como dá suporte para a geração de hipóteses, a construção teórica e a elaboração de instrumentos" (GONDIM, 2003, p. 160).

Quanto às etapas de um grupo focal, não se viu muita diferença aos grupos de atividades propostos, são eles: planejamento inicial, condução e análise de dados. Com pequenas variações na nomenclatura, mas mantendo a mesma essência, os exemplos são diversos, entre eles Carlini-Cotrim (1996), Tremblay, Hevner e Berndt (2010) e Dresch, Lacerda e Antunes Júnior (2015).

Para execução do grupo focal foi utilizada a estrutura de etapas proposta por Kontio, Lehtola e Bragge (2004), que segue a mesma ideia supracitada. São elas:

i. Definir o problema de pesquisa;

ii. Planejar o evento do grupo de focal;

iii. Selecionar os participantes;

iv. Conduzir a sessão do grupo focal;

v. Analisar os dados e gerar relatório.

O planejamento do grupo focal (Apêndice I), quanto ao direcionamento do debate com os especialistas e formas de abordar os temas de interesse, foi baseado em Salah, Paige e Cairns (2014). O detalhamento da execução e resultados será explicitado na Seção 5.3.4.3.

2.7 Síntese do Capítulo

Em síntese a pesquisa concentrou-se na área de segurança da informação, tendo uma abordagem mista (quanti-qualitaviva) e foi dividida em duas fases: a primeira exploratória e a segunda descritiva.

A etapa exploratória desta pesquisa consistiu em três etapas de revisão da literatura, são elas:

1. Pesquisa informal por parte do autor;

2. Mapeamento Sistemático da Literatura (MSL) realizada pelo autor e parceiros (ALENCAR et al., 2018b; ALENCAR et al., 2018c);

3. Análise de revisões sistemáticas da literatura (RIOS, 2016; DE LIMA, 2017; CORDEIRO, 2017; REA-GUAMAN et al., 2017).

Já a etapa descritiva do trabalho foi baseada na Design Science Research e utilizando, em especial, os procedimentos técnicos de levantamento (survey) e grupo focal para criação e avaliação dos artefatos.

Para esta pesquisa foi estabelecido o nível mínimo de confiança de 95,5% (corresponde a dois desvios-padrão) e erro máximo (intervalo de confiança) de 8,0%. Para isso, a pesquisa teria que abordar, em seu levantamento, ao menos 144 empresas.

O Quadro 3 aponta a correlação das principais atividades desenvolvidas ou resultados entre cada versão do artefato e as etapas da Design Science Research propostas por Peffers et al. (2007), arcabouço metodológico utilizado.

Quadro 3 – Distribuição das Atividades em Cada Etapa da DSR

Etapas da DSR	**Versão 1**	**Versão 2**	**Versão 3**
Identificar Problema e Motivação	Iniciação centrada no problema baseada na revisão da literatura e no resultado do survey	Iniciação centrada no problema baseada na revisão da literatura, no resultado do survey e na versão anterior	Iniciação centrada no problema baseada na revisão da literatura, no resultado do survey e na versão anterior
Definir os Objetivos de uma Solução	Definir um guia simplificado de controles para concepção de uma PSI e de um SGSI	Definir uma estratégia para avaliação da maturidade da segurança da informação na corporação	Definir uma estratégia adaptável para avaliação da maturidade e priorização da segurança da informação na corporação

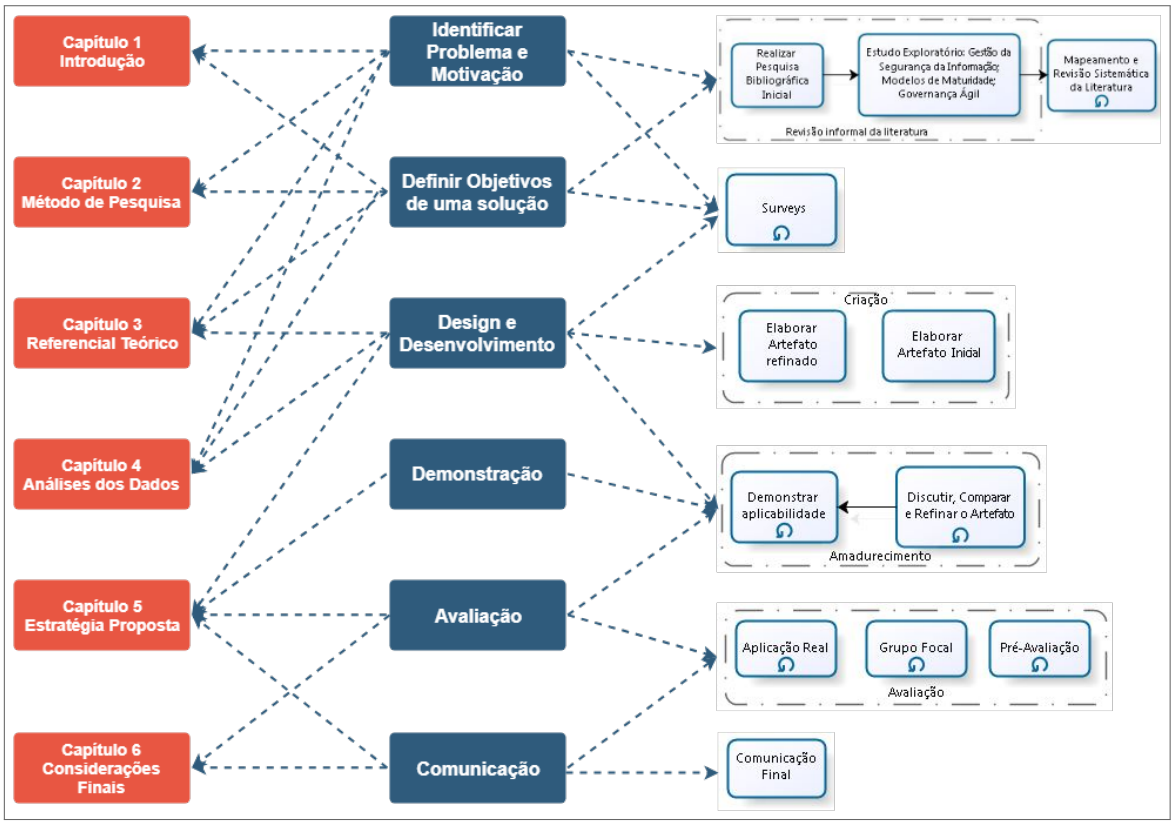
Quadro 3 Continuação

Etapas da DSR	**Versão 1**	**Versão 2**	**Versão 3**
Design e Desenvolvimento	Utilização da revisão da literatura, do resultado do survey e as ISO/IEC 27001 e 27002 para elencar o conjunto de controles críticos (PSI e SGSI simplificados)	Utilização da Versão 1 para evolução e geração da estratégia de maturidade	Utilização da Versão 2 para evolução e geração da estratégia de priorização e maturidade
Demonstrar	Verificada a sua aplicabilidade ao comparar com a literatura. Resolvido um problema ao gerar uma PSI e o SGSI simplificados. Utilizado na construção da Versão 2	Verificada a sua aplicabilidade ao comparar com a literatura. Utilizado na construção da Versão 3	Verificada a sua aplicabilidade ao comparar com a literatura. Aplicado em um caso real (empresa)
Avaliar	Avaliado por empresas, especialistas e congresso de TIC	Avaliado por empresas, especialistas e congresso de TIC	Avaliado por especialistas (grupo focal), congresso e periódico de TIC
Comunicar	Dois artigos publicados (SILVA NETO; ALENCAR; QUEIROZ, 2015; ALENCAR; TENORIO JUNIOR; MOURA, 2017a)	Dois artigos publicados (ALENCAR; MOURA, 2017a, 2017b)	Dois artigos publicados (ALENCAR; MOURA, 2018; ALENCAR et al., 2018)

Por fim, de forma simplificada, a correlação entre a estrutura desta tese com as etapas

da DSR utilizadas e com as macro etapas concebidas na Figura 2 é exibida na Figura 6.

Figura 6 – Desenho Metodológico e Estrutura de Tomada de Decisão



Fonte: Adaptada de Jappur (2014, p. 46).

3 REFERENCIAL TEÓRICO

A área de segurança da informação, em seu sentido mais amplo, até mesmo devido sua abrangência, vem sendo abordada de forma multidisciplinar e trabalhada por diferentes áreas do conhecimento como: Administração, Ciência da Computação, Ciência da Informação, Economia, Engenharias, Tecnologia da Informação, entre outras.

Particularmente na área de tecnologia da informação e da ciência da computação, diversos estudos têm sido realizados com sucesso na área de segurança da informação, em especial, relacionados à criptografia, protocolos de redes ou transações, análise de malwares ou mecanismos seguros para uso na Internet. Porém, para os desafios atuais, torna-se igualmente importante analisar a segurança sobre outros vieses, de forma mais ampla (CHOO, 2011). Neste sentido, a quantidade de estudos que abrangem as perspectivas humanas na área de Segurança da informação e o alinhamento ao negócio e às propostas de maturidades para à área, principalmente no Brasil, como é o caso do presente trabalho, é um subconjunto que ainda carece de debate e investigação.

Com objetivo de melhor elucidar o tema de segurança da informação e demonstrar a sua abrangência e ligação com o negócio, este Capítulo exibirá a revisão da literatura dos principais conceitos que abrangem o tema realizado nesta pesquisa. Neste sentido, os assuntos foram estruturados em seis seções. Inicialmente os conceitos da área de segurança da informação serão apontados (Seção 3.1). Posteriormente, na Seção 3.2, será abordada a área de governança. A terceira Seção apresentará os conceitos da área de Maturidade. As Normas ISO/IEC que abrangem o tema serão apresentadas na quarta Seção. A Seção 3.5 apresentará os trabalhos encontrados nas fases de revisão da literatura. E, por fim, na última Seção, uma síntese do capítulo será apresentada.

3.1 Segurança da Informação

Como já aludido, a área de segurança da informação é bastante ampla e carece de uma análise multidisciplinar. Com este pensamento e para um correto entendimento do contexto proposto pelo presente trabalho, esta Seção abordará a tríade essencial para a segurança da informação (Tecnologia, Processos e Pessoas). Posteriormente será abordado a evolução da segurança da informação e, por fim, os princípios da segurança da informação.

3.1.1 A Trinca Essencial para a TIC

A tecnologia da informação e comunicações e, consequentemente, a segurança da informação que visa a sua proteção como um todo, pode ser vista como uma área que envolve, primordialmente, tecnologia, processos e pessoas, sendo essa a trinca essencial para a TIC

e para a segurança da informação, devendo estar em equilíbrio para seu correto funcionamento, pois são elementos chaves para uma organização que busca uma segurança da informação mais efetiva (KIELY; BENZEL, 2006; ALENCAR, 2008; ARAÚJO, 2009).

Corroborando com o mesmo pensamento, Da Silva (2009, p. 26) relata que "o reconhecimento da segurança da informação como processo que garante a proteção da informação no ambiente físico e lógico, só é possível com o envolvimento simultâneo dos três principais recursos da organização que são pessoas, tecnologias e processos".

O mesmo pensamento é corroborado por Manoel (2014) que insere os Processos, Pessoas e Tecnologia como pilares para um correto entendimento e aplicação dos conceitos de governança, indiferente do seu âmbito.

Os referidos segmentos podem ser representados pela Figura 7, não necessariamente sendo obrigatória sua aplicação na ordem demonstrada, se destacando a ideia de camadas ou barreiras de segurança, pensamento corroborado por Nobre (2009) e MacCarthy (2011), que visam atender o conceito de segurança em profundidade (NORTHCUTT et al., 2005), tendo como premissa que a proteção de um ativo não deve depender apenas de uma única medida de segurança, mas sim de um conjunto delas que deve envolver toda a trinca citada.

Figura 7 – Camadas da Segurança da Informação

Fonte: Alencar (2011, p. 20).

O primeiro tópico da citada trinca relata o aspecto da própria tecnologia. Não há como criar uma estrutura de segurança da informação, com políticas e normas definidas, sem soluções que cuidem da enorme quantidade e variedade de pragas que infestam os computadores e a Internet atualmente. Para garantir a segurança por meio da tecnologia, precisa-se da:

- Integração de dispositivos nas mais diversas camadas para controle, segmentação e isolamento da rede e das aplicações;
- Domínio das portas de entrada e saída das informações como o correio eletrônico, controlando, entre outros fatos, os spams, vetor de muitas pragas da Internet e

destacado entrave para a produtividade, e o acesso web, evitando o acesso a sites maliciosos;

- Controle do acesso físico e lógico dos funcionários e demais pessoas ao ambiente, sistemas para atualização e correção dos aplicativos utilizados, entre outros.

Porém, a implantação da tecnologia deverá passar por etapas de escolha da correta solução, o que não significa a utilização das mais recentes descobertas ou das mais complexas, assim como, a correta solução, necessita da configuração adequada, manutenção e atualização (MARCIANO; LIMA-MARQUES, 2006; ALENCAR, 2008; TIPTON; NOZAKI, 2016).

O segundo ponto da trinca são os processos, que exigem revisões e adaptações constantes. O grande desafio para as empresas é equilibrar a flexibilidade dos processos sem que torne a companhia frágil, mas que, por outro lado, não enrijeça em demasia a produtividade, em busca do maior nível de segurança. "O crescente aumento das ameaças ao ambiente tecnológico exige que as organizações desenvolvam processos cada vez mais eficientes para manter as informações seguras" (MODULO, 2006, p. 12).

Fernandes e De Abreu (2014) corroboram com o assunto ao abordar que na tentativa de se proteger os ativos de TIC e manter a integridade da informação, é necessário implementar um processo de gestão da segurança. Esse processo deve buscar o estabelecimento e a manutenção de responsabilidades, papéis, padrões, procedimento e políticas abrangentes à área de segurança da informação. A gestão da segurança deve incluir o monitoramento, o teste periódico e a implementação de ações corretivas das deficiências ou dos incidentes de segurança da informação. A gestão eficiente e eficaz da segurança da informação acarreta, como benefícios, a proteção de todos os ativos de TIC e minimiza o impacto de vulnerabilidades e incidentes de segurança da informação sobre o negócio.

Os processos compreendem, dentre outros, a segurança aplicada aos procedimentos da organização (sequências lógicas de atividades inter-relacionadas que agregam valor a um produto ou serviço) e os processos de segurança propriamente ditos, inclusive os relativos à segurança das instalações prediais e infraestrutura física (ALENCAR, 2008).

A última parte da trinca, as pessoas, é a mais fácil de explicar e entender, porém é facilmente esquecida como uma parte integrante do processo de segurança e não apenas como um ponto a ser protegido (MARCIANO; LIMA-MARQUES, 2006; ALENCAR, 2008). Alexandria (2009) e Tipton e Nozaki (2016) afirmam que é comum citar que o usuário é o elo fraco da segurança da informação, porém não se pode esquecer que os sistemas, aplicativos e produtos de software são criados para pessoas e por pessoas.

Não é preciso raciocinar muito para chegar à conclusão de que as pessoas são pedras fundamentais dentro do ambiente corporativo, sobretudo na segurança da informação. Nesta direção, Maconachy et al. (2001) afirmam que as pessoas são o coração e a alma de um sistema seguro. Apesar de tal importância, normalmente elas são acusadas pelos responsáveis de prover a segurança, "além de culpar o usuário, pouco tem sido feito para

identificar os fatores que levam a comportamentos potencialmente inseguros e menos ainda para tentar resolver tais problemas" (DA SILVA; STEIN, 2007, p. 50).

Resumindo os papéis e posições desta trinca, Alencar (2008) finaliza abordando a visão de camadas empregada no âmbito da segurança da informação, havendo a segmentação dos três aspectos supracitados, visto que uma visão unicamente técnica das questões de segurança da informação não é satisfatória para identificar a gama de riscos existentes, cabendo a corporação apoiar com a utilização correta da tecnologia, gestão e procedimentos apropriados, além da participação e apoio dos funcionários e colaboradores da empresa.

3.1.2 A Evolução da Segurança da Informação

Ao analisar a evolução das espécies animais, inclusive da espécie humana, é notável a busca por segurança. Porém, o termo "Segurança da Informação" tornou-se mais perceptível quando se configurou um novo ambiente denominado por Castells (2009) como "Era da Informação". Esta nova configuração gerou a alta valorização da informação como um bem decisório e peça fundamental nas estratégias organizacionais (RAMOS, 2007; ARAÚJO, 2009; FERREIRA, 2009). Tal pensamento é compartilhado por Fontes (2012) quando o mesmo ressalta que a informação é um recurso que, atualmente, move o mundo, dando conhecimento do passado e guiando para onde seguir, sendo um recurso crítico para realização do negócio e execução das mais diversas missões da corporação, necessitando ser protegido.

Nos primeiros tempos da computação, as aplicações eram basicamente militares e os problemas de segurança eram restritos ao acesso físico (LANDWEHR, 2001). Com o aumento da sua utilização, impulsionado pela academia, governo e, posteriormente, as corporações, surgiram outros problemas com a segurança dos computadores como a necessidade do compartilhamento do processamento de informações e recursos entre diversos perfis de usuários com níveis de confiança diferentes. Fato que levou ao desenvolvimento de sistemas operacionais de tempo compartilhado. Tais sistemas, em sua concepção ideal, deveriam ser desenvolvidos de forma a garantir o referido compartilhamento, porém de forma segura, tendo ciência de que o compartilhamento de recursos (terminais de acesso, programas, impressoras e dispositivos de armazenamento de dados) gera possíveis problemas e vulnerabilidades (BENZ, 2008).

Pfleeger, Pfleeger e Margulies (2015) citam que nos anos 80, época em que a Internet era usada principalmente por profissionais da área computacional, academia e empresas de sistemas, começou a ser fomentada a questão sobre a "segurança em computador". Essa preocupação coincide com a cadeia de valor da economia citada por Castells (2009). Neste período "os códigos maliciosos e vírus não eram comuns, os crimes cibernéticos raramente eram notícia de jornal e as pessoas não tinham noção das ameaças por meio de computador" (MENDONÇA, 2007, p. 64).

Joia (2004) e Joia e Neto (2004) reforçam esse pensamento da evolução da economia atrelado ao da segurança da informação quando defendem que, já no início da década de 80, a TIC não era mais utilizada apenas como uma ferramenta de processamento mais rápido, mas sim como uma forma estratégica e essencial para alavancar o negócio, necessitando de maiores proteções.

Com o aumento exponencial do número de dispositivos computacionais, de usuários e com as informações assumido o papel estratégico e, ao mesmo tempo, tornando-se necessária a sua disponibilização e compartilhamento, tornou-se visada como algo extremamente valoroso. Neste ambiente, qualquer falha no acesso às informações passou a ser causa de prejuízo e até falência de algumas corporações, uma vez que aqueles que detêm as informações primeiro ou obtém conhecimentos dos concorrentes conseguem uma grande vantagem no mercado (NOBRE, 2009).

A necessidade de compartilhamento, disponibilidade e, consequentemente, de segurança agravou-se com a evolução das redes de computadores, particularmente com a popularização da Internet, que foi estabelecida como uma forma de atender pesquisas militares norte-americanas e prezava, inicialmente, por uma segurança mais robusta, expandindo-se na década de 90 com a criação da World Wide Web, denominada Web (BERNERS-LEE, 1996). Este novo ambiente foi percebido pelas organizações como uma possibilidade de expansão de negócios e consequente ampliação de lucros no ambiente privado, mas o aumento dos lucros não era possível sem o aumento das vulnerabilidades que necessitavam ser combatidas.

A partir desta nova realidade, diversos documentos e procedimentos foram criados e implementados na tentativa de fazer com que usuários autorizados possam ter acesso seguro a determinadas informações e, ao mesmo tempo, proibir o acesso não autorizado (BENZ, 2008). Entre os primeiros marcos das documentações relativas à segurança da informação têm-se as publicações do National Institute of Standards and Technology (NIST)[1], entre elas: "Security Control for Computing System: Report of Defense Science Boad Task Force on Computer Security[2]", em 1970; "Department of Defense, Trusted Computer System Evaluation Criteria[3]", em 1985, também conhecido como The Orange Book, e a publicação especial número 800-12, em 1995, "An Introduction to Computer Security: The NIST Handbook[4]".

Com o passar dos anos, guiados por documentos como os citados, foram criadas diversas normas, metodologias e sistemas com o objetivo principal de promover a segurança da informação nas corporações. Sêmola (2013) ressalta que a preocupação com a segurança da informação deve existir oficialmente nas organizações, tendo uma maior respeitabilidade pelos stakeholders quando existe a adoção de normas e padrões nacionais e internacionais,

[1] NIST: http://www.nist.gov/
[2] Security Control for Computing System: http://csrc.nist.gov/publications/history/ware70.pdf
[3] The Orange Book: http://csrc.nist.gov/publications/history/dod85.pdf
[4] The NIST Handbook: http://csrc.nist.gov/publications/nistpubs/800-12/

bem como de normativos internos à organização, como políticas e normas de segurança, por exemplo.

Tais arcabouços de segurança serviram como guia, para que a utilização, inevitável, das novas tecnologias fosse realizada de forma mais segura. Nesse contexto, a informação, que era mantida anteriormente em grandes computadores de processamento centralizado, os mainframes, e trafegava apenas em ambientes restritos e possivelmente controlados, passou, nos últimos anos, a trafegar pela Internet e utilizar os mais variados meios para recebimento e envio de informações, sendo a mobilidade e o acesso rápido às informações os pontos chaves (SÊMOLA, 2013), gerando uma maior complexidade para manter seus bens protegidos, uma vez que a barreira física pode não mais existir.

Percebe-se, portanto, o crescimento da dependência das organizações em relação à informação e conectividade. Décadas atrás, a tecnologia tinha uso mais restritivo pelas limitações de armazenamento e preços proibitivos dos computadores. Pouco tempo depois, compartilhar informações tornou-se algo vital e as corporações foram expandindo tal conectividade de seus ambientes internos e possivelmente controlados, para parceiros, fornecedores, clientes e assim por diante (NOBRE, 2009; SÊMOLA, 2013). A ampliação do desempenho das tecnologias de processamento e comunicação, bem como o desenvolvimento de novas rotinas de integração entre os stakeholders possibilitou uma ampliação da integração e compartilhamento de informações.

Desta forma, quanto mais a tecnologia compartilha informações e torna as organizações e indivíduos velozes, complexos e poderosos, mais as organizações dependem da tecnologia e maior é o risco em experimentar erros a ela relacionados. Ou seja, a economia precisa da tecnologia, a tecnologia propõe serviços e meios para melhorar a economia e agregar valor ao negócio, e a segurança precisa acompanhar os avanços mesmo quando inserida no final do processo ou quando problemas e falhas já foram gerados, o que vem ocorrendo com frequência e sem ser dado o devido valor em tempo hábil (FONTES, 2000; GABBAY, 2003). Pois, apesar dos sinais alarmantes dos prejuízos que as empresas vêm tendo com problemas relacionados à falta de segurança, e de ser cada vez maior a importância que a informação vem tendo no mundo dos negócios, a segurança da informação ainda não tem o devido respaldo ou envolvimento necessário nas corporações (GABBAY, 2003).

Na mesma linha, Fontes (2000, p. 23) cita que "apesar de inúmeras empresas afirmarem que o assunto segurança de informação é importante, esta declaração fica muito distante de ações práticas que permitam uma efetiva proteção do recurso informação". Alexandria (2009) corrobora afirmando que apesar da segurança da informação ser uma necessidade para todas as empresas, as pesquisas de mercado mostram que a implementação da segurança da informação está concentrada em organizações de grande porte em segmentos específicos da economia como, por exemplo, bancário-financeiro e telecomunicação.

Em síntese, mesmo que não seja no ritmo esperado, é visível a evolução das ferramentas, tecnologias e metodologias referentes à segurança de informação ao longo dos anos,

principalmente nas últimas duas décadas. Os procedimentos de segurança da informação têm se alterado bastante desde seus dias iniciais, quando a segurança física, junto com um conjunto de back-up, compunha os controles de segurança dos dados. Atualmente, a segurança da informação precisa ser composta por uma estratégia de segurança que se alinhe ao negócio. Para isso, deve ser pensada, aplicada e atualizada por especialista, abordando políticas, normas, metodologias, programas de conscientização, além das possíveis ferramentas e proteções já utilizadas.

Por fim, é importante entender que a TIC não pode ser vista como a solução de todos os problemas, bem com que a mesma insere novas vulnerabilidades no ambiente. Para isso, torna necessário estabelecer um nível de segurança equivalente ao bem que está sendo manipulado.

3.1.3 Princípios da Segurança da Informação

Impulsionadas, principalmente, pelas mudanças ocasionadas pela evolução econômica e tecnológica já citadas, as empresas começaram a despertar, mesmo que não seja no ritmo desejado, para a necessidade de segurança das informações. Uma vez que as informações tiveram um grande acréscimo de seu valor e importância, aumentou-se a busca por falhas e vulnerabilidades para capturá-las.

Diversos documentos (ABNT, 2006; JANSSEN, 2008; ARAÚJO, 2009; DA SILVA, 2009; NOBRE, 2009; OLIVEIRA, 2009; SÊMOLA, 2013) abordam os seguintes princípios como base para se tentar prover a segurança das informações:

- Confidencialidade: busca limitar o acesso somente às entidades (pessoas, sistemas, objetos) autorizadas, fazendo com que a informação esteja disponível para as mesmas e negue o acesso às demais;
- Disponibilidade: propriedade que visa garantir que a informação, quando solicitada, esteja sempre disponível para o uso;
- Integridade: propriedade que garante que a informação manipulada mantenha as características originais, ou seja, que os dados obtidos estejam íntegros. Pode ser vista como a capacidade de verificação se modificações intencionais ou acidentais dos dados ocorreram.

Segundo Pfleeger, Pfleeger e Margulies (2015), a "segurança de computador" apenas coexistiria se mantivessem em harmonia as três características fundamentais supracitadas, que se relacionam, devendo funcionar de forma coesa para se obter um resultado correto e eficaz. Pensamento compartilhado por Laureano e Moraes (2005) que citam que a combinação apropriada dos itens confidencialidade, disponibilidade e integridade serve como base para que as corporações alcancem suas metas, pois, baseados nesses princípios, seus sistemas de informação terão uma maior confiabilidade.

A segurança da informação, em seu sentido mais amplo, envolve requisitos voltados à garantia de origem, uso, armazenamento e trânsito da informação, buscando certificar todas as etapas do ciclo de vida. Estes requisitos, de certa forma, podem ser resumidos nos três primeiros princípios citados, porém algumas abordagens (MARCIANO; LIMA-MARQUES, 2006; TIPTON; NOZAKI, 2016) agregam mais dois, sendo eles:

- Autenticidade: propriedade que garante que a informação é autêntica, provinda das fontes anunciadas;
- Não repúdio: propriedade que associa ações e acessos a usuários e entidades de forma inquestionável, ou seja, o ato realizado não pode ser negado por quem o realizou.

Alguns outros autores (SHIREY, 2007; ALENCAR, 2008; SÊMOLA, 2013) defendem que o sistema que administra as informações deverá atentar, além dos cinco itens citados, aos seguintes pontos complementares:

- Auditoria: Consiste em rastrear e analisar os diversos passos que uma pessoa ou processo realizou ou a que uma informação foi submetida, visando identificar características como: os participantes, meios, horários e locais de cada fase;
- Legalidade: característica que visa garantir a legalidade da informação perante normas em vigência, visto que a mesma se adere a um sistema de legislação;
- Privacidade: característica que restringe e controla a exposição e disponibilidade das informações. Uma informação privada deve ser vista, lida ou alterada somente pelo seu dono ou grupo que detêm o privilégio

Laureano e Moraes (2005) ainda ressaltam que a veracidade se soma a todos esses critérios como estratégia de gestão da informação. Isto é, a informação deve estar baseada em argumentos lógicos ou acontecimentos verídicos. Pois, não basta que a informação esteja disponível em uma fonte confiável e que a mesma seja autêntica, mas também que sua fonte seja lícita.

A existência da correlação entre os diversos princípios é uma necessidade como demonstra, entre outros, Laureano e Moraes (2005), Shirey (2007), Alencar (2008) e Sêmola (2013) quando ressaltam que a confidencialidade depende da integridade, pois se for perdida a integridade de um sistema, as estruturas que controlam a confidencialidade tornam-se duvidosas. A integridade depende da confidencialidade, pois se algum dado confidencial for perdido e pessoas não autorizadas tiverem acesso ao sistema, os mecanismos de integridade podem ser desabilitados. A disponibilidade e a auditoria dependem da integridade e confidencialidade, pois de nada adiantará ter todos os dados disponíveis sempre que necessário, assim como realizar a correta auditoria e ter todos os seus registros históricos se os dados são inválidos, seja pela falta de integridade ou confidencialidade da informação.

Alencar (2008) e Sêmola (2013) ressaltam que cada princípio citado gera um custo adicional para a empresa, sendo necessário um estudo da viabilidade e dos critérios de segurança que serão abordados, pois, nem sempre, é possível ou vantajoso prover todos os itens para todas as informações. O fato é que diversos sistemas, os mais antigos principalmente, não foram concebidos com a preocupação de prover segurança a si mesmo e aos ativos que manipula, o que dificulta, e algumas vezes impede, a implantação dos princípios pretendidos, implicando que a segurança por meios técnicos seja deficiente.

Araújo (2009, p. 41) corrobora com a afirmação ao citar que "a interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de controlar o acesso. Sendo que muitos sistemas de informação não foram projetados para serem seguros". Desta forma, a necessidade por mecanismos de proteção da informação, além da tecnologia, cresce na tentativa de incorporar as características de segurança desde os princípios dos projetos. Neste modelo, tenta-se gerar produtos ou serviços com um número menor de vulnerabilidades.

3.2 Governança de TIC

Atualmente, é impossível imaginar uma empresa sem uma forte área de Tecnologia da Informação e Comunicação, para manipular os dados e prover informações, essenciais ao negócio e, principalmente, aos tomadores de decisões (CASTELLS, 2009). A estruturação, organização e manutenção de uma infraestrutura de TIC, incluindo pessoas, processos e tecnologias especializados requer altos investimentos (ALENCAR, 2011).

Diante disto, algumas vezes são impostas restrições orçamentárias aos investimentos de TIC, alguns casos por restrições orçamentária da própria instituição e outras por duvidarem dos reais benefícios de tal investimento. Mesmo sabendo-se que a carência de investimentos na área de TIC pode ocasionar o fracasso de um empreendimento na situação atual, competitiva e globalizada. Por outro lado, alguns gestores de TIC apresentam os projetos ou solicitam investimento sem demonstrar a real necessidade de sua aquisição ou dos riscos associados ao não investimento. Em outras situações, tais riscos e necessidades são inseridos no projeto, mas os gestores não possuem habilidade para demonstrá-los de forma correta ou debatê-los de modo a convencer a alta direção. Para melhorar o processo de tomada de decisão baseada em uma correta análise de riscos, torna-se necessária uma estrutura para gerenciar e controlar as atividades de TIC nas empresas, para garantir o retorno de investimentos e adição de melhorias nos processos empresariais. Este movimento é conhecido como governança de TIC (FERNANDES; DE ABREU, 2014).

O conceito de governança está essencialmente relacionado com os mecanismos e responsabilidades através dos quais a autoridade é exercida, as decisões são tomadas e a estratégia é coordenada e dirigida nas organizações indiferente de seu tamanho, abrangência ou porte financeiro (LUNA et al., 2014).

A governança corporativa pode ser vista como um conjunto de fatores (entre eles práticas, processos, políticas, leis) afetando a maneira como uma organização é gerida e conduzida, incluindo as relações entre todos os envolvidos (sejam internos ou externos) para o alcance dos objetivos estratégicos lançados, sendo a governança de TIC uma especialização da governança corporativa para a área específica de Tecnologia da Informação e Comunicação (FERNANDES; DE ABREU, 2014).

O termo governança de TIC pode ser visto como uma estrutura de relações e processos que visam dirigir, bem como controlar uma determinada instituição visando aditar valor ao negócio por meio do gerenciamento dos riscos e garantindo um melhor retorno do investimento de TIC (DE HAES; GREMBERGEN, 2016).

Manoel (2014) corrobora com o assunto apontando que a governança de TIC visa um processo pelo qual decisões são tomadas sobre os investimentos de TIC, envolvendo vieses de como as decisões são tomadas, quem toma as decisões, quem é responsabilizado pela função de operação e gestão da área de TIC e como os resultados são aferidos e monitorados. Ou seja, um processo que abrange o como dirigir, avaliar e monitorar todos os recursos de TIC. Para Gonçalves, Gaspar e Cardoso (2016), através de seu levantamento bibliográfico, a governança de TIC deve abranger as áreas de: alinhamento estratégico, entrega de valor, gestão de recursos, gestão de riscos e mensuração de desempenho.

Para muitas instituições, a tecnologia e a informação que suportam o negócio representam o seu mais valioso recurso (CASTELLS, 2009). Além disso, num ambiente de negócios altamente competitivo e dinâmico é requerido uma excelente habilidade gerencial, onde a área de TIC deve suportar as tomadas de decisão de forma rápida, constante e com custos cada vez mais baixos. Não existem dúvidas sobre o benefício da tecnologia aplicada aos negócios. Entretanto, para serem bem-sucedidas, as organizações devem compreender e controlar os riscos associados no uso das novas tecnologias (FERNANDES; DE ABREU, 2014).

Diniz, Medeiros e Veras (2012) apontam que:

> "a discussão acerca dos reais retornos dos investimentos em TI tem obtido importância, sobretudo as questões relativas à maior consistência e transparência da gestão da área de TI, chamada de IT Governance ou Governança de TI. Contudo, a dificuldade em criar uma estrutura interna, com características próprias, fez com que as organizações buscassem por modelos estruturados e flexíveis, que permitissem manter o foco nos negócios e na missão organizacional, ao mesmo tempo em que atendessem aos requisitos de conformidade legal" (DINIZ; MEDEIROS; VERAS, 2012, p. 2).

A governança de TIC se faz cada vez mais necessária diante da posição que a tecnologia da informação tomou nos dias atuais, como pode ser visto em Luna et al. (2014) ao afirmar que as tecnologias de informação e comunicação são o elo entre a capacidade de decisão, a disposição estratégica, e a competência para pôr em prática essas táticas concretamente.

Na mesma linha, Gomes et al. (2016) afirmam que a governança de TIC se tornou essencial dentro das organizações por garantir melhorias e eficiências nos processos e procedimentos da empresa, fornecendo, assim, a estrutura que interliga todos os processos e objetivos do negócio, sendo necessário um framework que oriente as atividades com melhores práticas e ferramentas de gestão na estrutura organizacional da empresa para se alcançar os melhores resultados. Os benefícios citados por Prado et al. (2016) inserem que a governança de TIC auxilia na eficiência e cumprimento dos prazos.

Conforme Fernandes e De Abreu (2014), trabalhar com governança de TIC permite à organização garantir: o alinhamento de TIC ao negócio e às normas regulatórias, bem como a continuidade do negócio. Fato corroborado pelos embasamentos de Diniz, Medeiros e Veras (2012).

Ramlaoui, Semma e Dachry (2015) contribuem com o tema ao colocar que o valor estratégico da TIC se manifesta na capacidade de gerar e produzir valor dentro de um contexto dinâmico e emergente. O valor é muitas vezes visto como sinônimo de eficiência e entendido como a capacidade de aumentar a produtividade, reduzindo os recursos, sendo a governança de TIC um facilitador neste processo de agregar valor.

De forma geral, as organizações que optam pela adoção da governança em sua rotina, tendem a obter diversos benefícios que podem auxiliar no crescimento da empresa, desde que exista disciplina e controle. As vantagens proporcionadas pela implantação da governança corporativa às organizações estão relacionadas à melhoria dos negócios, transformando princípios em ações, preservando e otimizando o desempenho organizacional, dando maior transparência aos acionistas, bem como aditando uma postura de decisões corretas, com base nos princípios da governança, respaldando no acesso ao capital e na contribuição para a longevidade dos negócios (FERNANDES; DE ABREU, 2014).

Puricelli (2015) corrobora com a visão supracitada de governança de TIC e ainda insere que, no ambiente atual, não é mais possível limitar a governança de TIC a questões apenas tecnológicas, diferentemente do passado, que seguir as melhores diretrizes era suficiente para manter um nível adequado de segurança ao adquirir novos aparelhos e configurar sistemas.

Prado et al. (2016) baseado no trabalho de Fernandes e De Abreu (2014), classificam os principais modelos, frameworks ou normas para governança de TIC em quatro categorias:

- Alinhamento estratégico e Compliance;
- Decisão, Compromisso, Priorização e Alocação de Recursos;
- Estrutura, Processos, Operação e Gestão;
- Gestão do Valor e do Desempenho.

No qual o Control Objectives for Information and related Technology (COBIT)[5] é o único inserido em todas as categorias e a família de normas de segurança da informação ISO/IEC 27.000 se enquadra na primeira categoria (alinhamento estratégico e compliance).

Segundo Gomes et al. (2016), entre os principais modelos, frameworks ou normas para governança de TIC têm-se:

- Serviços de TIC: ITIL[6] , ISO/IEC 20.000[7];
- Segurança da Informação: A família de normas ISO/IEC 27.000;
- Projetos: PMI[8] e PMBOK[9];
- Fornecedores: e-SCM[10] e SAS 70[11];
- Software: CMMI[12] e MPS.BR[13].

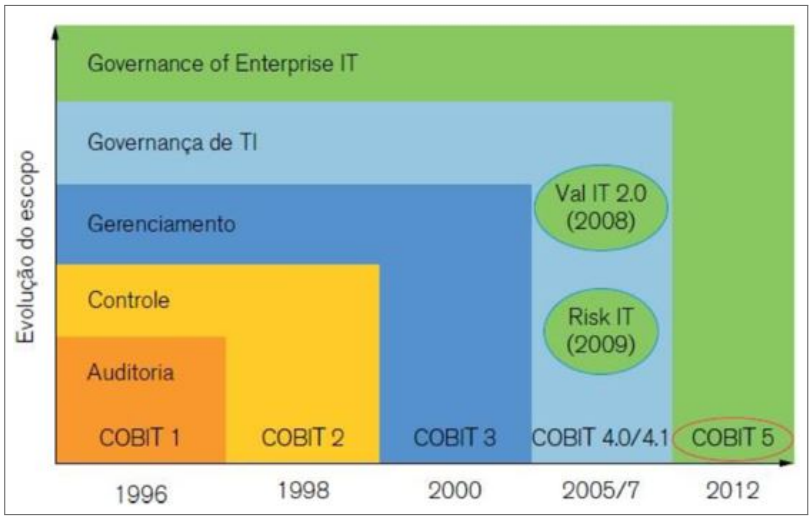
Gomes et al. (2016) ainda apontam que na área de governança de TIC, pode-se citar o COBIT que aborda melhores práticas para ser usada em todas as áreas citadas (serviço de TIC, Segurança da informação, Projetos, Fornecedores e Software). Almeida Neto et al. (2015b) ressaltam o COBIT como um framework para alinhamento entre TIC e o negócio, ou seja, governança de TIC. Desenvolvido e mantido pela ISACA , atualmente em sua versão 5 (ISACA, 2012a), cuja evolução pode ser observada na Figura 8.

Fernandes e De Abreu (2014), corroborado por ISACA (2012a), afirmam que o COBIT, em sua versão atual, pode ser visualizado como um modelo abrangente dos princípios, práticas e ferramentas analíticas globalmente aceitos que podem auxiliar a organização, indiferente de ramo ou porte, resolver efetivamente problemas críticos relacionados à governança e gestão de TIC. De Haes e Grembergen (2016) concordam com o pensamento ao demonstrar, em seus estudos, a aplicação do COBIT 5 para a governança de TIC.

O COBIT 5 aborda uma estrutura de cascateamento de metas que pode ser utilizada para vincular as necessidades de interesse em qualquer organização ou projeto com metas corporativas específicas, que são mais detalhadas e apoiadas por metas relacionadas à área de TIC, visando a possibilidade da organização maximizar o valor e minimizar o risco relacionado à informação (ISACA, 2012a).

[5] COBIT - Control Objectives for Information and related Technology - http://www.isaca.org/COBIT/Pages/default.aspx
[6] ITIL - IT Infrastructure Library - http://www.itil.org.uk/
[7] ISO/IEC 20.000 - https://www.iso.org/standard/51986.html
[8] PMI - Project Management Institute - https://www.pmi.org/
[9] PMBOK - Project Management Body of Knowledge - https://www.pmi.org/pmbok-guide-standards
[10] e-SCM - eSourcing Capability Model - http://www.itsqc.org/
[11] SAS70 - Statement on Auditing Standards No. 70: Service Organizations - https://www.aicpa.org/press/pressreleases/2011/nextgenerationofsas70.html
[12] CMMI - Capability Maturity Model Integration - https://cmmiinstitute.com/
[13] MPS.BR - Melhoria do Processo de Software Brasileiro - https://www.softex.br/mpsbr/

Figura 8 – Evolução do COBIT



Fonte: https://www.portalgsti.com.br/cobit/sobre/

Thomas (2015) adiciona que a versão atual do COBIT proporcionou uma abordagem mais organizada ao framework, incorporando vários outros documentos da ISACA (por exemplo, Val IT ou Risk IT) e alguns outros frameworks e padrões da indústria. Tal característica auxilia o melhor alinhamento da área de TIC ao negócio bem como auxilia o desafio de definir a diferença entre as atividades de governança e do gerenciamento (DUMOULIN, 2015).

Prado et al. (2016) apontam alguns elementos facilitadores e outros inibidores ou dificultadores na aplicação do COBIT. Dentre os inibidores tem-se:

- A não adaptação ou falta de postura proativa dos colaboradores para as novas rotinas e mudanças propostas pelo COBIT;
- A dificuldade na mudança organizacional e cultural, visto que transformar uma organização e seus colaboradores não é uma tarefa fácil e demanda tempo e perseverança para que todos entendam a necessidade e a importância da mudança, percebendo os benefícios.

Já como facilitadores, Prado et al. (2016) inserem:

- Apoio da direção da empresa e do diretor de TIC como primordiais;
- Revisão dos processos de implantação atuais e a criação de uma gerência de mudança para avaliar os impactos das mudanças e uma gerência de configuração para melhorar o controle dos ativos de TIC;
- Definição de acordo de níveis de serviço junto às áreas usuárias, definindo tempo de indisponibilidade dos sistemas ou processos a serem alterados.

DuMoulin (2015) ressalta que, atualmente, a maioria das organizações opera com um modelo de Gestão da TIC complexo, fragmentado por setores da empresa e sem alinhamento entre si, o que torna a gestão e governança de TIC em um mito e a estratégia corporativa em algo não existente, havendo brigas internas e conflitos de prioridades. Fatos que direcionam a empresa para um caminho mais árduo.

Prado et al. (2016) também traz alguns pontos de atenção para aplicação do COBIT, que podem ser generalizados para ações de implementação da governança de TIC como um todo, sendo eles:

- Procedimentos e acompanhamento para treinamento e controle do projeto de implantação para se mitigar os riscos e propor planos de ação para corrigi-los quando necessário;
- Definição cuidadosa e adequada do modelo de governança a ser implementado e sua estratégia de implantação;
- Envolvimento das partes interessadas, seja por meio do apoio da alta direção, ou de um programa de treinamento e conscientização dos colaboradores.

Prado et al. (2016) afirmam que muitas empresas adotaram as boas práticas descritas no COBIT a fim de proporcionar um melhor gerenciamento de serviços e um alinhamento entre a área de TIC e as estratégias e objetivos organizacionais, sendo um dos pontos fortes do COBIT o controle das atividades de TIC por meio de objetivos. Entretanto, a implantação do COBIT nem sempre ocorre de maneira trivial e intuitiva, dificultando a obtenção de um bom nível de maturidade de governança de TIC.

Diante dos fatos expostos, DuMoulin (2015) enaltece a necessidade de uma forma mais simples e didática para implantação de uma política de gestão e governança única e alinhada ao negócio, inserindo a nova versão do COBIT (versão 5) como uma possível solução devido às suas melhorias. Ponto que é corroborado por Fernandes e De Abreu (2014). Outro possível viés, mas não excludente aos demais, é a utilização da governança Ágil de TIC, tema que será abordado em seção própria posteriormente.

Dentro da área de governança de TIC, que já pode ser entendida como uma especialização da governança corporativa, temos ações específicas na área de segurança da informação. Diante da já conhecida e citada importância das informações nos dias atuais, é fácil notar a necessidade da segurança das mesmas. Neste mesmo pensamento, diversos modelos têm aprofundado suas práticas na área de segurança da informação, entre eles o COBIT que, dentro do escopo do presente trabalho, vale destacar os documentos COBIT 5 for Information Security (ISACA, 2012b) e COBIT 5 for Risk (ISACA, 2013), tratados com extensões do COBIT 5 para cada área.

O COBIT 5 for Information Security é um guia para a área de segurança da informação, fornecendo orientações para ajudar a área de TIC e os profissionais de segurança da

informação a entender, utilizar e implementar atividades relevantes relacionadas à segurança da informação, bem como tomar decisões mais informadas, mantendo a consciência sobre tecnologias emergentes e as ameaças que a acompanham (ISACA, 2012b).

Já o COBIT 5 for Risk, como o próprio nome aborda, trata sobre riscos. Não apenas sobre o risco de TIC, mas sobre os riscos do negócio, mais detalhadamente aos riscos de negócios associados ao uso, posse, operação e envolvimento de TIC na empresa. Atuando como um facilitador em sua área, visto que já aponta cenários genéricos de riscos que podem ser ajustados ao ambiente (ISACA, 2013; THOMAS, 2015).

Como complemento ao conteúdo exposto sobre governança, a presente Seção apresentou, em seguida, um maior detalhamento da área de governança ágil e, posteriormente, o conteúdo de Governança de Segurança da Informação.

3.2.1 Governança Ágil

Como já apresentado na problemática em questão, a burocracia existente nos processos, bem como a dificuldade na aplicação dos modelos ou frameworks atuais torna-se um entrave em diversos casos (PRADO et al., 2016). Neste sentido é possível observar um conflito entre o formalismo apresentado pela maioria destas iniciativas e a agilidade imposta por um mercado cada vez mais competitivo. Com este pensamento, surgem ações para tentar impor agilidade e respostas mais rápidas.

Em meados de 2001, pode-se observar, na área de desenvolvimento de software, uma dicotomia semelhante. Naquele período, metodologias como a Rational Unified Process (RUP), tidas como precursoras ao desenvolvimento de software (KRUCHTEN, 2004), também se depararam com um dilema parecido. Este problema motivou o surgimento do Manifesto for Agile Software Development (BECK et al., 2001), manifesto que abordou um conjunto inovador de valores e princípios, promovendo uma quebra de paradigmas.

Com esta mesma perspectiva, a área de governança de TIC vem sofrendo com os processos lentos, mas já se mostram estudos para tratamento de tal deficiência, como uma visão mais enxuta dos modelos atuais conforme aponta Prado et al. (2016) ao reduzir a vasta quantidade de processos do COBIT, visto que estes frameworks estão ficando cada vez mais complexos e de difícil implantação, e as organizações podem obter excelentes resultados sem necessariamente implantar todos os processos previstos. Fato semelhante apontado no estudo de Silva Neto, Alencar e Queiroz (2015) e Alencar, Tenorio Junior e Moura (2017a), sendo estes para a área de segurança da informação, reduzindo os controles da ISO/IEC 27.001 e 27.002 para propor uma política simplificada.

Ademais, visões mais ágeis e práticas para a governança de TIC estão surgindo utilizando os princípios do Manifesto Ágil (LUNA et al., 2014; LUNA; KRUCHTEN; MOURA, 2015; ALMEIDA NETO et al., 2015a; ALMEIDA NETO et al., 2015b; RAMLAOUI; SEMMA; DACHRY, 2015; LUNA et al., 2016).

Os quatro valores propostos por Beck et al. (2001) no manifesto ágil são:

- Indivíduos e interações com mais valor que processos e ferramentas;
- Software em funcionamento com mais valor que documentação abrangente;
- Colaboração com o cliente com mais valor que negociação de contratos;
- Responder a mudanças com mais valor que seguir um plano.

Para suportar os valores supracitados propostos por Beck et al. (2001) foram inseridos doze princípios no manifesto ágil, sendo eles:

- Nossa maior prioridade é satisfazer o cliente através da entrega contínua e adiantada de software com valor agregado;
- Mudanças nos requisitos são bem-vindas, mesmo tardiamente no desenvolvimento. Processos ágeis tiram vantagem das mudanças visando vantagem competitiva para o cliente;
- Entregar frequentemente software funcionando, de poucas semanas a poucos meses, com preferência à menor escala de tempo;
- Pessoas de negócio e desenvolvedores devem trabalhar diariamente em conjunto por todo o projeto;
- Construa projetos em torno de indivíduos motivados. Dê a eles o ambiente e o suporte necessário e confie neles para fazer o trabalho;
- O método mais eficiente e eficaz de transmitir informações para e entre uma equipe de desenvolvimento é através de conversa face a face;
- Software funcionando é a medida primária de progresso;
- Os processos ágeis promovem desenvolvimento sustentável. Os patrocinadores, desenvolvedores e usuários devem ser capazes de manter um ritmo constante indefinidamente;
- Contínua atenção à excelência técnica e bom design aumenta a agilidade;
- Simplicidade - a arte de maximizar a quantidade de trabalho não realizado - é essencial.
- As melhores arquiteturas, requisitos e designs emergem de equipes auto-organizáveis;
- Em intervalos regulares, a equipe reflete sobre como se tornar mais eficaz e então refina e ajusta seu comportamento de acordo.

Diante dos valores e princípios apontados no manifesto ágil, a agilidade pode ser vista como a capacidade de uma organização reagir a mudanças em seu ambiente mais rapidamente do que o ritmo dessas mudanças. Essa abordagem simplificada e objetiva é apontada e utilizada por Luna et al. (2014), como mais adequada no contexto de governança ágil.

Agilidade no nível do negócio exige flexibilidade, capacidade de resposta e adaptabilidade, que deve ser aplicado em combinação com a capacidade de gerência, alinhamento estratégico e envolvimento entre as áreas incluídas, especialmente em ambientes competitivos (LUNA et al., 2014).

Ramlaoui, Semma e Dachry (2015) trazem outra definição, mas na mesma linha, apontando agilidade como a capacidade que as organizações apresentam, de forma dinâmica, para sentir a necessidade de mudança a partir de fontes internas e externas e realizar essas mudanças rotineiramente sem a queda de seu desempenho.

Gregory et al. (2016) apontam que qualquer pessoa que esteja envolvida direta ou indiretamente em ações ágeis na organização podem ser enquadradas como profissionais ágeis usufruindo dos benefícios, bem como, dos possíveis malefícios ou desafios que esta abordagem acarreta.

Antes de tratar de governança ágil é importante refletir que a abordagem ágil, segundo Gregory et al. (2016), pode ser inserida em ações específicas, dentre elas destaca-se o desenvolvimento de software ágil, mas também pode ser inserida em contexto mais amplos, organizacionais. Nesta última opção está inserida a abordagem de governança ágil. A governança ágil propõe a aplicação de agilidade sobre o sistema de gestão e governança organizacional tornando-o competitivo como um todo (LUNA et al., 2014).

Ao apontar a junção da área de governança com os conceitos ágeis, a princípio, pode parecer uma junção de áreas opostas, em alguns casos rivais, visto que a governança prega mecanismos de controle, responsabilidade, processos, auditoria e autoridade, enquanto a agilidade transmite a ideia de informalidade, simplicidade, experimentação e praticidade. No entanto, se a meta da empresa é conseguir agilidade nos negócios, esta não pode ser alcançada sem compromisso de todos os setores da organização, que por sua vez não pode ser alcançada sem governança (LUNA et al., 2014).

A aparente incoerência entre as áreas de agilidade e governança pode ter sido um dos pontos que resultaram na baixa quantidade de trabalhos na área de governança ágil. Esse contexto é refletido na revisão sistemática realizada por Luna et al. (2014), que afirma não ter encontrado outras revisões sistemáticas relacionando as capacidades ágeis com a área de governança, sendo seu trabalho, publicado em 2014, a primeira consolidação na área.

O estudo de Luna et al. (2014) elencou 167 estudos relacionados direta ou indiretamente com o domínio de governança ágil proposto, classificando-os em quatro áreas: engenharia de software, corporativo, industrial (de produção) e multidisciplinar, apontando que os primeiros estudos, mesmo que incipientes, começam a surgir apenas a partir

de 1996. Já no Brasil, Marques e Mota (2013) apontam os primeiros trabalhos sobre governança de TIC em 1999.

Mesmo sabendo que os estudos têm limitações, bem como, por motivos diversos, podem ter deixado de inserir alguns trabalhos, fica evidenciado quanto a área é recente e carece de estudos. Corroborando com este assunto, vale ressaltar o estudo de Marques e Mota (2013) que aborda um estudo bibliométrico em periódicos brasileiros sobre a governança de TIC e, mesmo abordando 81 artigos, não é citado no trabalho o conceito ou estudos em governança ágil, evidenciando, novamente, a incipiência na área ao nem ser citado o termo no levantamento.

Portanto, apenas nos últimos anos é que se começa a ver um comum entendimento sobre as definições e desafios na área de governança ágil. Em outras palavras, como expõem Luna et al. (2014), isto implica que executivos, pesquisadores e profissionais até pouco tempo atrás não tinham uma referência unificada para obter uma visão geral sobre este domínio. Fato corroborado por Gregory et al. (2016) ao apontar as dificuldades da aplicação de ações ágeis em ambiente não ágeis, sendo desafiador a aplicação de métodos ágeis em áreas que não foram amplamente pesquisadas, como a de governança.

Almeida Neto et al. (2015b) também ressaltam a incipiência da área de governança ágil em TIC, apontando que diversas iniciativas e apoios são encontrados para a área de desenvolvimento de software (sejam ágeis ou tradicionais), bem como iniciativas semelhantes podem ser vistas para a evolução da maturidade na governança em TIC tradicional, porém ainda não foi possível perceber as mesmas iniciativas para o contexto de governança ágil em TIC.

Luna et al. (2014) afirmam que a primeira definição de governança ágil é datada de 2007 e tem foco no desenvolvimento ágil de software. Em 2009 apresentou-se a definição de governança ágil dentro do escopo de governança de desenvolvimento de software. Em 2010 é apresentada a primeira definição de governança ágil focada em governança de TIC, sendo tratada como um processo de definição e implementação da infraestrutura de TIC que suporta e apoia os objetivos de negócios estratégicos da organização, sendo propriedade conjunta das várias unidades de TIC e de negócios e instruído a dirigir todos os envolvidos na obtenção de diferencial competitivo estratégico através dos valores e princípios do manifesto ágil Luna et al. (2010).

Por fim, Luna et al. (2014) apontam a quarta e última definição encontrada em seu levantamento para a área, abrangendo uma visão multidisciplinar, tratando-a como os meios pelos quais as vantagens competitivas estratégicas devem ser alcançadas e melhoradas no ambiente organizacional, sob uma abordagem ágil, a fim de proporcionar valor ao negócio de forma mais rápida, melhor e mais barata (LUNA; KRUCHTEN; MOURA, 2013), definição esta também utilizada por Almeida Neto et al. (2015b).

Posteriormente, Luna et al. (2016) lançou uma nova definição para governança ágil, apontando como a capacidade de uma organização de sentir, adaptar-se e responder às

mudanças em seu ambiente, de forma coordenada e sustentável, mais rápido do que a ritmo dessas mudanças.

Percebe-se, assim, que o conceito de governança ágil está ganhando atenção e evoluindo ao longo do tempo como um significado cada vez mais amplo e que pode ser encaixado em contextos diferentes. Este comportamento é coerente, tal como um domínio que está tomando forma, onde os autores começam a perceber a sua amplitude e as relações entre os diversos contextos onde os fenômenos se manifestam (LUNA et al., 2014).

Ramlaoui, Semma e Dachry (2015) também concordam com a necessidade de meios mais ágeis no ambiente corporativo, bem como com essa visão mais ampla dada à governança ágil ao citar que a governança de TIC é muitas vezes um conjunto muito rígido de regras e processos, evitando que a área de TIC possa evoluir e mudar junto com a necessidade da empresa e suas estratégias. Temas como mudanças rápidas na tecnologia, globalização e privacidade estão entre as características que a maioria das organizações atuais necessitam trabalhar. Para ter sucesso neste ambiente, os princípios da agilidade criam uma vantagem competitiva, ajudando não apenas na solução do problema atual como preconizando a empresa como inovadora, pensamento também defendido por Almeida Neto et al. (2015a) e Almeida Neto et al. (2015b).

Almeida Neto et al. (2015b) ainda reforçam que em diversos casos tentam justificar a burocracia dos processos de governança como algo essencial a própria organização. No entanto, quando as organizações tentam adotá-las, especialmente as que não possuem maiores conhecimentos na área, acabam se deparando com diversas dificuldades e, normalmente, tendo custos adicionais com a contratação de consultorias especializadas.

Luna et al. (2014) ainda esclarecem que a governança ágil não é uma substituta aos modelos convencionais, frameworks e métodos já existentes (por exemplo, ITIL e COBIT). A proposta é inserir uma nova visão para a governança. Para isso Luna et al. (2014), ratificado por Luna, Kruchten e Moura (2015) e Luna et al. (2016), propõem seis meta-princípios para um modelo de governança ágil prezando que:

- O nível de governança deve ser sempre adaptado ao contexto organizacional, sendo equilibrado, e ajustado, quando necessário para equilibrar os princípios de governança e agilidade;

- Deve ser orientado ao negócio. Neste conceito o negócio deve ser a razão para cada decisão e ação, ou seja, decisões de qualquer natureza devem ser feitas tendo em conta a estratégia do negócio;

- Deve ser focado nas pessoas, valorizando e incentivando cada pessoa a participar criativamente, onde as pessoas são um elemento chave da mudança e a força motriz nas organizações;

- Deve ter por base os ganhos rápidos, onde as vitórias rápidas devem ser celebradas e usadas para obter mais impulso e melhores resultados refletindo, cada pequeno ganho ou melhoria, em uma grande aceleração para a empresa no médio e longo prazo;
- Deve inserir uma abordagem sistemática e adaptativa, devendo tais características serem intrínsecas na forma de lidar com as mudanças e adaptações ao momento e estratégias atuais da organização. Considerando as mudanças como um componente natural do ambiente de negócio que tenta se adaptar aos novos fatores; e, por fim:
- Apresentar um design simples e com refinamento contínuos dos serviços e entregas. Ou seja, deve-se escolher sempre a alternativa mais simples e viável para o design de soluções, para que seja entregue rapidamente e que poderá ser melhorada posteriormente.

Tomando por base esses seis meta-princípios, Luna, Kruchten e Moura (2015) e Luna et al. (2016) propõem nove meta-valores para a governança ágil, sendo eles: Comportamento, Prática, Sustentabilidade, Competitividade, Transparência, Envolvimento das Pessoas, Sentir, Adaptar e Responder.

Inspirado em Beck et al. (2001), Luna, Kruchten e Moura (2015) e Luna et al. (2016) abordam tais meta-valores, comparando com a governança tradicional, da seguinte forma:

- Comportamento e prática do que processos e procedimentos.
- Alcançar a sustentabilidade e a competitividade do que ser auditada para estar em conformidade.
- Transparência e envolvimento das pessoas com a empresa do que monitoramento e controle.
- Sentir, adaptar e responder do que seguir um plano.

Finalmente, Luna et al. (2014) apontam em sua revisão que a governança ágil é uma nascente, um domínio amplo e multidisciplinar, com foco na melhoria do desempenho organizacional, mas que precisa ser mais intensivamente estudada. Desafios também citados por Almeida Neto et al. (2015b) e corroborado por Gregory et al. (2016) ao citar que é um desafio a implantação de ações ágeis em um ambiente não ágil, devendo ser tratado em uma visão multidisciplinar, pois pode abranger questões organizacionais, sociais, culturais e etc.

3.2.2 Governança de Segurança da Informação

Mendonça (2007) coloca que o profissional responsável pela área de segurança da informação, ao atingir níveis avançados de conhecimento na área de segurança da informação,

gestão e negócio, entende a segurança da informação de forma mais profunda, com maior maturidade, evoluindo para uma visão mais ampla, que emerge sob o rótulo de "governança da segurança da informação" (GARTNER , 2006, p.2 *apud* MENDONÇA, 2007, p. 67), tal conceito de governança também é defendido e explorado por Alexandria (2009).

Ferreira (2003) e Ramos et al. (2008) corroboram a linha de pensamento citada e sugerem que esse profissional esteja em um departamento ligado diretamente com a diretoria ou presidência da corporação para que o mesmo tenha poder de decisão. Manoel (2014) segue a mesma linha ao colocar que a governança de segurança da informação é uma parte da governança de TIC, podendo haver sobreposição entre as duas. Mas se a governança de TIC não existir, não é um impeditivo para as ações da GSI. Nesta última situação, a governança de segurança da informação deverá estar subordinada ao presidente da instituição ou ao maior escalão tomador de decisão.

A ISO/IEC 27.0014 (ABNT, 2013c) aponta que a governança de segurança da informação deve ter como objetivo:

- Alinhar os objetivos de negócio com a estratégia da Segurança da Informação;
- Garantir que os riscos da informação sejam elucidados e encaminhados aos responsáveis;
- Aditar valor para o negócio, para a alta direção e para as partes interessadas.

Tais objetivos apontados pela ISO/IEC 27.014 (ABNT, 2013c) são corroborados e detalhados por Manoel (2014) que complementa a temática ao inserir que a GSI atuando para obtenção de tais objetivos e aplicada de forma eficiente resulta:

- Abordagem mais ágil para a tomada de decisões na área de segurança da informação;
- Apresentação para a alta direção e demais envolvidos a real situação da segurança da informação corporativa;
- Direcionamentos para investimentos mais eficientes e eficazes em segurança da informação;
- Encaminhamento da organização ao atendimento e conformidade com requisitos externos (legais, regulamentares ou contratuais).

Diante da responsabilidade sobre a segurança da informação, sabendo que suas ações e decisões podem influenciar toda a corporação e, em diversos casos, não tendo pessoas realmente qualificadas para o cargo, Ferreira (2003), Ramos (2007), Ramos et al. (2008) e Sêmola (2013), entre outros, propõem a criação de comitês corporativos de segurança. O comitê corporativo, além do Chief Information Security Officer (CISO), se constitui de diversos outros executivos dos vários departamentos da empresa, formando, assim, visões distintas que representam toda a empresa. Seu principal papel é organizar, concentrar

e planejar as ações estratégicas de segurança da informação, sendo um início para uma correta GSI.

Em sua composição podem existir parceiros externos, por exemplo, especialistas em segurança como consultores. Porém, devido à criticidade das informações e decisões a serem tomadas pelo grupo, pode ser um risco a participação de terceiros, necessitando cuidados (CEZAR; CAVUSOGLU; RAGHUNATHAN, 2013). Sobre este ponto, Ramos (2007, p. 52) cita que "são inegáveis os riscos na escolha e contrato destas empresas, pois afinal são ativos importantes que as organizações estarão disponibilizando para elas, sendo necessária uma atenção especial às cláusulas de responsabilidade de ambas as partes".

Diante da crescente necessidade de se ter pessoas em posições estratégicas na corporação com conhecimento de segurança da informação, o que nem sempre ocorre, e da dificuldade de formação de tais especialistas, por ser uma área multidisciplinar, extensa e volátil, é comum encontrar a segurança da informação corporativa e as ações da GSI ainda defasadas e sem o correto entendimento das ameaças e desafios inerentes à área.

No caso de se ter uma área de segurança da informação adequada e implementada a GSI poderá se obter uma maior compreensão deste novo ambiente e traçar metas alternativas na tentativa de estabelecer um ambiente mais seguro nas corporações contra tais ameaças, visto que um dos grandes desafios da segurança da informação é a dificuldade de conhecer e mensurar os riscos, vulnerabilidades e ameaças existentes para, então, se ter uma maior gerência do ambiente, como cita Anderson e Moore (2006), corroborado por Mahopo, Abdullah e Mujinga (2015), que ainda adicionam que a gestão de riscos de segurança de TIC vem ganhando atenção considerável na última década devido ao colapso de algumas grandes organizações no mundo.

Uma das formas de se buscar a governança de segurança da informação é o alinhamento da área de segurança da informação ao negócio através de uma análise mais profunda da própria área de segurança da informação e dos riscos envolvidos, como aborda Thomas (2015) que defende, para isso, a utilização das extensões do COBIT 5 para segurança da informação (ISACA, 2012b) e para risco (ISACA, 2013).

Além do COBIT e da ISO/IEC 27.014, podemos citar outras ações na tentativa de se prover uma melhor governança na área da segurança da informação, como Mahopo, Abdullah e Mujinga (2015) que ao correlacionar as propostas da OCTAVE[14], ISO/IEC 27.001 e 27.002, COBIT, ITIL e Information Security Forum Standard of Good Practice (ISF SOGP)[15], criaram uma abordagem qualitativa própria para gerenciamento de risco de segurança de TIC.

Porém a simples implantação de modelos ou frameworks, por melhor que sejam, não tem tido êxito total. Os ataques e exploração de vulnerabilidades estão aparecendo em maior quantidade e diversidade, bem como explorando vulnerabilidades humanas. Por-

[14] OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation - https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051

[15] ISF SoGP - Information Security Forum Standard of Good Practice - https://www.securityforum.org/

tanto, é fundamental ampliar a governança de segurança de TIC para incluir o fator humano em análises e avaliações de riscos corporativos. Para fazer isso de maneira eficiente, é crucial compreender e mensurar o risco real, bem como propor contramedidas eficazes e personalizadas para mitigá-lo (PURICELLI, 2015).

Puricelli (2015) reforça o assunto ao apontar que as atuais abordagens de segurança e gestão de riscos de TI tendem a subestimar, ou até ignorar, o fator humano nos modelos de avaliação, ferramentas, processos e estrutura jurídica. É fundamental desenvolver uma estratégia que inclua esse risco específico relacionado ao fator humano nos processos de governança de segurança de TIC.

Mesmo não sendo algo fácil, como aponta Puricelli (2015) ao afirmar que envolver os funcionários em uma avaliação é uma abordagem relativamente inovadora, além de ser considerada arriscada, alguns trabalhos, como o presente, buscam caminhos para alcançá-la.

Mouton, Malan e Venter (2013) ressaltam que a abordagem para a área de segurança da informação incluindo pessoas no ambiente corporativo deve envolver todas as partes interessadas relevantes, como os departamentos responsáveis pelos recursos humanos, de comunicação e jurídico, para explanar sobre as ameaças, alinhar os objetivos, definir o escopo da avaliação e obter o comprometimento de todos. Além dos pontos citados, existem muitas outras questões e requisitos éticos que precisam ser levados em consideração ao realizar uma avaliação do fator humano no ambiente corporativo. O que mais uma vez remete a necessidade de uma visão de governança, seja de TIC ou de segurança da informação, holística e alinhada ao negócio como um todo e não apenas em áreas ou setores pontuais, como abordam Fernandes e De Abreu (2014), Manoel (2014) e De Haes e Grembergen (2016).

Por fim, Manoel (2014) aponta que uma correta aplicação da governança de segurança da informação visa um tratamento mais ágil na área. Fato também apontado, em escala maior (governança de TIC) por Fernandes e De Abreu (2014). O que reforça a necessidade dos arcabouços utilizados serem mais simples e rápidos para auxílio das tomadas de decisões, convergindo com o pensamento proposto pela governança ágil.

3.3 Modelos de Maturidade

Maturidade pode ser vista como o desenvolvimento de sistemas e processos que tem natureza repetitiva e, por sua repetição, aumenta a sua probabilidade de sucesso (KERZNER, 2017). Prado e Oliveira (2018) afirmam que, de maneira geral, existe relação direta entre maturidade e indicadores de desempenho. Ou seja, quanto maior a maturidade:

- Maior o sucesso total e menor o fracasso;
- Menor o atraso;

- Menor o estouro de custos;
- Maior o percentual de execução do escopo previsto.

Além disso, quanto maior a maturidade maior a percepção, pela alta administração, do valor da área para agregar valor à organização (PRADO; OLIVEIRA, 2018).

Neste contexto, um modelo de maturidade pode ser entendido como uma estrutura conceitual, composta por processos bem estabelecidos, por meio do qual uma organização desenvolve-se de modo sistêmico a fim de atingir um estado futuro desejado (ALMEIDA NETO, 2015; ALMEIDA NETO et al., 2015b). Funcionando como um guia para a organização, de tal maneira que a empresa possa localizar onde está e como está "espelhando-se" nele para, em seguida, realizar um plano para que possa chegar à algum ponto melhor do que o atual, na busca da excelência (MAYER; FAGUNDES, 2008). Vale ressaltar que, para esta tese de doutorado, será adotado o termo modelo de maturidade para referenciar modelos de estágios (englobando maturidade e/ou capacidade), assim como ocorreu em Almeida Neto (2015).

Um modelo de maturidade seria, então, um mecanismo capaz de quantificar numericamente a capacidade de uma organização em determinada área. Por outro lado, espera-se também de um modelo de maturidade que ele seja capaz de auxiliar no estabelecimento de um plano de crescimento para a maturidade da organização na área em questão (PRADO, 2018). Podendo ser visto, também, como um conjunto de características, atributos, indicadores ou padrões que representam a capacidade e a progressão em uma determinada disciplina. O conteúdo do modelo tipicamente exemplifica as melhores práticas e pode incorporar padrões ou outros códigos de prática da disciplina (REA-GUAMAN et al., 2017).

Para Gomes et al. (2016), um modelo de maturidade tem por objetivo auxiliar na melhoria contínua, por meio de processos, para que possam ser implementadas as melhores práticas. Prado et al. (2016) afirmam que via um modelo de maturidade aplicado corretamente na área de TIC os pontos de melhoria são entendidos e explicados de uma forma melhor; bem como mostra o alinhamento aos objetivos estratégicos da organização, a dependência da empresa à área de TIC e elenca as fraquezas e virtudes dentro da área, podendo até se refletir em pontos fortes e fracos da própria empresa como um todo.

Almeida Neto et al. (2015b) corroboram ao apontar que um nível de maturidade é uma etapa evolucionária definida na melhoria de processos onde cada nível estabiliza uma parte importante dos processos organizacionais e que a partir do diagnóstico de um nível de maturidade de uma organização, torna-se possível prever seu desempenho futuro dentro de determinada área.

Pensamento semelhante é exposto por Cordeiro (2017) ao afirmar que 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.

Fato corroborado por Nery Júnior, Moura e Teixeira Filho (2018), ao inserir que a função do modelo de maturidade é avaliar e identificar em qual nível de maturidade a organização se encontra e depois aplicar o plano de crescimento para se chegar a excelência.

Depois de identificar os processos e controles críticos, o uso de um modelo de maturidade permite a identificação de lacunas que representam risco e como mostrá-las a equipe de gestão. Com base nesta análise, planos de ação podem ser avaliados e desenvolvidos para a melhoria dos processos e controles considerados deficientes até o nível de desenvolvimento desejado (ISACA, 2012a; JIRASEK, 2012), fato ratificado em Rigon et al. (2014).

Para aferir a área e traçar um caminho para se alcançar o nível desejado pela organização, como mencionado, os modelos normalmente trabalham de duas formas: a representação contínua e a representação por estágios (SILVA et al., 2016).

> "Na representação contínua, uma organização pode optar por melhorar o desempenho de uma única área de processo que esteja relacionada a um determinado problema ou pode trabalhar em diversas áreas independentes que estejam alinhadas aos objetivos de negócio da organização.
>
> Do contrário da representação contínua, a representação por estágios oferece um caminho sistemático, estruturado e uniforme, baseado em um conjunto de áreas de processos associados em níveis de maturidade. Quando uma organização atinge um nível de maturidade, considera-se que seus processos alcançaram uma determinada capacidade, ou seja, possuem mecanismos que garantem a repetição sucessiva de bons resultados. A melhoria contínua dos processos da organização é obtida por meio de passos evolutivos entre os cinco níveis de maturidade do modelo, definidos e numerados" (SILVA et al., 2016, p. 127).

Ciente da relevância apontada e dos benefício que um modelo de maturidade pode trazer, vários órgãos, por exemplo, a Organização para Cooperação e Desenvolvimento Econômico (OCDE)[16], o Instituto Brasileiro de Governança Corporativa (IBGC)[17], a Comissão de Valores Mobiliários (CVM)[18], e B3 (Brasil Bolsa Balcão)[19] produziram recomendações de boas práticas de governança corporativa nas quais temas como transparência, gestão de risco e controles são abordados, todos fazendo algum tipo de referência à maturidade dentro de sua área de atuação (GONÇALVES; GASPAR; CARDOSO, 2016), o que entrelaça estas áreas.

Rigon e Westphall (2011) também ressaltam a importância de um modelo de maturidade e avaliação para a área de segurança da informação ao afirmar que ter uma PSI implantada na empresa não garante a total segurança da informação, sendo necessário medir o nível de maturidade da segurança através de um método de medição e um conjunto de controles que tratem a segurança da informação de forma abrangente. Desta

[16] OCDE - Organização para Cooperação e Desenvolvimento Econômico - http://www.oecd.org
[17] IBGC - Instituto Brasileiro de Governança Corporativa - https://www.ibgc.org.br/
[18] CVM - Comissão de Valores Mobiliários - http://www.cvm.gov.br/
[19] B3 - Brasil Bolsa Balcão, surgiu da fusão da Bolsa de Valores, Mercadorias e Futuros de São Paulo (BM&FBOVESPA) com a Central de Custódia e de Liquidação Financeira de Títulos (CETIP) - http://www.b3.com.br

forma, avaliando o estado atual da segurança, os gestores poderão tomar decisões precisas para melhorar os processos e controles internos da organização.

Um modelo de maturidade de segurança deve fornecer um guia para um programa de segurança completo. Ele também define a ordem em que os elementos de segurança devem ser implementados, incentiva o uso de padrões de melhores práticas e fornece um meio para comparar programas de segurança, como aborda o The Open Group (2017) e Chapin e Akridge (2005 *apud* RIGON et al., 2014). Fato corroborado por Silva e Barros (2017) ao afirmar que um modelo de maturidade deve ter objetivo de auxiliar as empresas na avaliação da segurança da informação. Para a avaliação, o modelo de maturidade apontará o estágio atual, bem como deixa claro o caminho para se chegar a níveis mais avançados.

Não é de agora que se sabe a necessidade das empresas implementarem a gestão de risco de forma consistente e sistematizada. Porém, mesmo sendo necessário, os estudos na área são recentes, como pode ser percebido em Mayer e Fagundes (2008) que afirmavam, em 2008, não se ter um modelo de maturidade voltado à Gestão de Riscos em Segurança da Informação (GRSI) que meça ou avalie o nível de maturidade desse processo dentro das organizações conforme os requisitos de um Sistema de Gestão de Segurança da Informação e, portanto, aplicável a empresas de diferentes portes e segmentos de mercado. Fato que aos poucos vem sido mitigado com publicações na área em períodos mais recentes, como afirmam Silva, Menezes e Costa (2012).

Entre as pesquisas relacionadas ao uso de modelos com a finalidade de aferir a maturidade da segurança da informação no ambiente corporativo e como forma de evidenciar a evolução das publicações, mencionada por Silva, Menezes e Costa (2012), pode-se destacar: Leem, Kim e Lee (2005), Lessing (2008), Park et al. (2008), Woodhouse (2008), Saleh (2011b), Cholez e Girard (2014), Rigon et al. (2014), Muthukrishnan e Palaniappan (2016) e Silva e Barros (2017).

Diversas abordagens para gestão ou maturidade existem no mercado, como citam Karokola, Kowalski e Yngström (2011). Mais específicas para a área de segurança, podemos citar, conforme classificação de Rigon et al. (2014): Orientadas a Processo: COBIT e ITIL; Orientadas a Controle: ISO/IEC 27.001; Orientadas a Produtos: como a ISO/IEC 15.408; Orientadas a Gerenciamento de Risco: como OCTAVE e ISO 27.005; e, por fim, Orientadas a Melhores Práticas: como ISO/IEC 27.002. Sendo o ITIL e o COBIT os mais utilizados para governança de TIC (GONÇALVES; GASPAR; CARDOSO, 2016).

Vale ressaltar que esses modelos, normas, frameworks ou padrões não são, em sua grande maioria, excludentes. Pelo contrário, muitas vezes são apoiados ou embasados por outros. Como é o caso do Open Information Security Management Maturity Model (O-ISM3)[20], um modelo que visa mensurar a maturidade da gestão da segurança da informação (THE OPEN GROUP, 2017) e fundamenta-se no CMMI, ITIL, ISO 9.000 e ISO 17.799/27.001 (RIGON et al., 2014).

[20] O-ISM3 - Open Information Security Management Maturity Model - https://www.ism3.com/

Gomes et al. (2016) afirmam que quando um modelo de maturidade é utilizado baseado em algum modelo de melhores práticas, esses modelos alcançam uma medição de maturidade com resultados consideráveis e embasados, por exemplo, como ocorre com o COBIT Manegement Guidelines[21] e o Process Maturity Framework (PMF)[22]. Mesmo pensamento é abordado por Radanliev et al. (2018), ao analisar as melhores práticas existentes visando nortear os princípios de segurança aplicáveis no conceito da Internet das coisa.

Também é o caso do modelo de avaliação cíclica de maturidade da segurança da informação proposto por Rigon et al. (2014) que é derivado, entre outros conceitos e embasamentos, da ISO/IEC 27.002, ISO/IEC 27.005 e do COBIT. Bem como os estudos de Gomes et al. (2016) e Park et al. (2008) que trazem resultados de modelos de maturidade baseados no ITIL.

Nesta mesma linha, também cabe citar como exemplo de modelo de maturidade o MAnGve Maturity Model (M3) apresentado por Almeida Neto e Moura (2014) e Almeida Neto et al. (2015b). O M3 aborda os aspectos de maturidade para a área de governança ágil, sendo influenciados por uma série de normas, modelos e frameworks anteriores, entre eles o CMMI e o COBIT.

Janssen (2008) propõe um instrumento de avaliação da maturidade dos processos de segurança da informação, neste caso sendo baseado no ambiente de três instituições hospitalares, sendo fundamentado na ISO/IEC 27.002. Mayer e Fagundes (2008) apresentam a proposta de um modelo para avaliar o nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação, tendo por base, direta ou indiretamente, o CMMI, COBIT, Modelo de Maturidade em Gerência de Projetos (MMGP)[23] e o Organizational Project Management Maturity Model (OPM3)[24] vigentes na época. Por fim, podemos citar Gonçalves, Gaspar e Cardoso (2016) que verificaram o nível de maturidade de 107 empresas brasileiras a partir de questionário baseado no COBIT.

Importante também ressaltar o Cybersecurity Framework (CSF)[25], framework do National Institute of Standards and Technology (NIST) que, mesmo não trazendo um modelo de maturidade, é um documento importante para a área de segurança da informação. O framework consiste em padrões, diretrizes e melhores práticas para gerenciar riscos relacionados à segurança cibernética na tentativa de promover a proteção e a resiliência da infraestrutura crítica e de outros setores importantes para o Governo dos EUA.

Diante do apresentado, verifica-se que inicialmente não se tinham guias para a implan-

[21] COBIT Manegement Guidelines - https://www.isaca.org/Knowledge-Center/Academia/Pages/A-Management-Guideline-Implementing-COBIT-5.aspx

[22] PMF - Process Maturity Framework é descrito no Apêndice do V3 ITIL Service Design Book

[23] MMGP - Modelo de Maturidade em Gerencia de Projetos - http://www.maturityresearch.com/novosite/index_br.html

[24] OPM3 - Organizational Project Management Maturity Model- https://www.pmi.org/pmbok-guide-standards/foundational/organizational-pm-maturity-model-opm3-third-edition

[25] NIST - CSF: Framework for Improving Critical Infrastructure Cybersecurity, https://www.nist.gov/cyberframework

tação da segurança da informação, maturidade e governança. Passou-se para um segundo estágio, com os primeiros modelos aparecendo e, em seguida, ao ponto de termos um conjunto de modelos, guias, frameworks ou documentos de melhores práticas concorrentes ou complementares.

Ciente da limitação e escopo do presente trabalho, torna-se necessário a apresentação dos principais modelos de maturidades que norteiam a área.

Para Rigon et al. (2014) os dois modelos de maturidades mais importantes para a área de maturidade em segurança da informação são o COBIT e o Open Information Security Management Maturity Model (O-ISM3).

Rea-Guaman et al. (2017) elencou como mais citados os modelos: Systems Security Engineering Capability Maturity Model (SSE-CMM)[26], Cybersecurity Capability Maturity Model (C2M2)[27], National Initiative for Cybersecurity Education – Capability Maturity Model (NICE-CMM)[28], COBIT, além de também citar o O-ISM3.

Já Cordeiro (2017) detalhou em seu trabalho a ISO/IEC 21827 (SSE-CMM), o O-ISM3 e o COBIT. Enquanto De Lima (2017) apresentou o COBIT e o Capability Maturity Model (CMM). Por fim, Alencar et al. (2018b) e Alencar et al. (2018c) apontaram, após o mapeamento realizado, que as principais normas, padrão, modelo, framework, documento, metodologia ou teoria utilizado pelos autores para implantação e avaliação da governança, gestão ou maturidade da segurança da informação corporativa são: as normas ISO/IEC da família de segurança e o COBIT.

Os modelos mais citados podem ser visto, de forma sintética, no Quadro 4. Não foram exibidos no quadro os modelos citados por Rea-Guaman et al. (2017) focados em cybersegurança, por ser citado apenas por esses autores e não ser a real área de interesse da presente pesquisa.

Quadro 4 – Modelos de Maturidade mais Utilizados

	O-ISM3	**COBIT**	**SSE-CMM**	**C2M2**	**NICE-CMM**	**CMM** [1]
Rigon et al. (2014)	x	x				
Rea-Guaman et al. (2017)	x	x	x	x	x	
Cordeiro (2017)	x	x	x			
De Lima (2017)		x				x
Alencar et al. (2018b, 2018c)		x				

[1] Acredita-se que a forma mais atualizada de comparar seria com o CMMI (Capability Maturity Model Integration). Porém, por ser a representação de uma RSL, foi apresentado exatamente como o autor do trabalho citado o exibiu em seu trabalho.

[26] SSE-CMM - Systems Security Engineering Capability Maturity Model - https://www.iso.org/standard/44716.html

[27] C2M2 - Cybersecurity Capability Maturity Model - https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0

[28] NICE-CMM - National Initiative for Cybersecurity Education – Capability Maturity Model - https://www.nist.gov/itl/applied-cybersecurity/nice

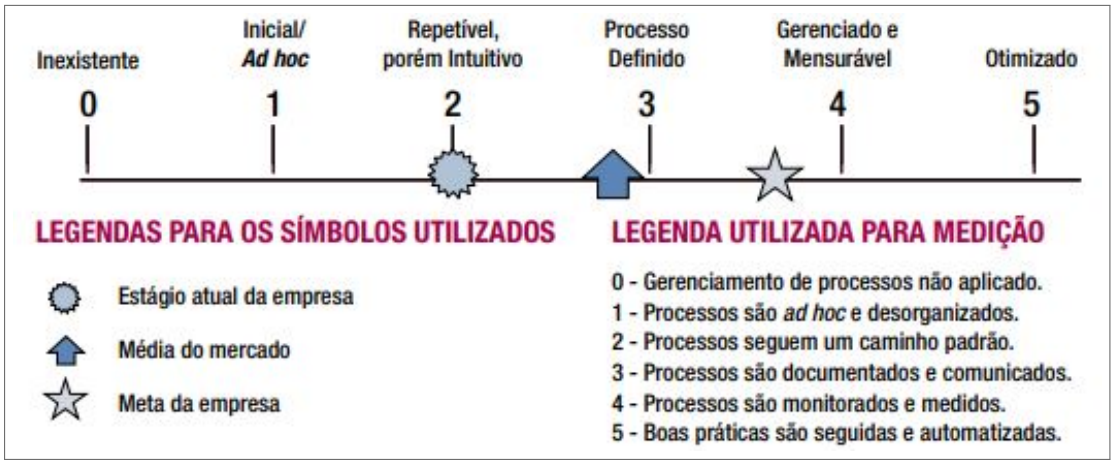
Os modelos mais citados no levantamento realizado terão um maior detalhamento a seguir, são eles: COBIT (citado por todos), O-ISM3 (com três referências) e o SSE-CMM (com duas citações).

3.3.1 COBIT

Em complemento ao que já foi detalhado sobre o COBIT, em especial na abordagem realizada na seção de governança de TIC, esta seção focará na avaliação da maturidade proposta pelo modelo.

De acordo com Fernandes e De Abreu (2014), sendo ratificado por Prado et al. (2016), o modelo de maturidade padrão do COBIT foi derivado do Capability Maturity Model for Software (SW-CMM) e estabelece para cada processo de TIC níveis de maturidade para que a organização possa ser medida, avaliada e comparada, conforme exibido na Figura 9.

Figura 9 – Representação Gráfica dos Modelos de Maturidade - COBIT 4.1



Fonte: ITGI (2007, p. 20)

Os níveis de maturidade do COBIT 4.1, exibidos na Figura 9, destinam-se a descrever possíveis estados dos processos de TI (STAMBUL; RAZALI, 2011), produzindo um perfil de maturidade de uma determinada organização ISACA (2012a). A definição de cada nível, de acordo com ITGI (2007) e ISACA (2012a), pode ser vista no Quadro 5.

Para tratar a maturidade, o COBIT apresenta um conjunto de indicadores obtidos pelo consenso de especialistas, porém mais focados nos controles de atividades do que em sua execução. Esses controles ajudam a otimizar o investimento em TIC, garantir a prestação de serviços e fornecer uma medida para julgar e permitir a comparação (RIGON et al., 2014).

Almeida Neto (2015) afirma que é papel da organização analisar e apontar o grau de maturidade que a empresa se encontra e o grau de maturidade que deseja alcançar, de acordo com a estratégia de TIC organizacional.

Quadro 5 – Níveis de Maturidade Conforme o COBIT

Nível	Nome	Descrição
0	**Inexistente**	Falta completa de qualquer processo identificável. Não existindo a consciência da necessidade de controles. A organização nem sequer reconhece que existe um problema a ser tratado.
1	**Inicial**	Há evidências de que a organização tenha reconhecido a existência de problemas que deveriam ser tratados. Existem processos, porém ad hoc. Normalmente são aplicados isoladamente ou tratados a cada caso. De forma geral, o gerenciamento ainda é desorganizado.
2	**Repetível**	Os processos seguem procedimentos similares e são seguidos por diferentes pessoas que executam a mesma tarefa, normalmente ações que estavam no Nível 1 e deram certo ou foram bem aceitas. Não existe treinamento formal ou comunicação dos procedimentos padrões, sendo a responsabilidade ainda individual. Existe um alto grau de confiança no conhecimento dos indivíduos, sendo provável a ocorrência de erros.
3	**Definido**	Neste nível os procedimentos já estão padronizados e documentados, bem como comunicados e treinados. Em qualquer etapa é possível acontecer erros ou desvios, mas, a partir deste estágio, os erros não são vistos com frequência. Seguir esses processos é obrigatório. No entanto, é improvável que os desvio sejam detectados. Os procedimentos não são sofisticados, mas existe formalização das práticas existentes;
4	**Gerenciado**	Após a melhoria da execução (nível 3), é possível monitorar e medir a conformidade com os procedimentos, bem como agir nos processos que aparentemente não funcionam corretamente. Os processos estão sobre aperfeiçoamento constante e fornecem boas práticas. Ferramenta de automação é usada de forma limitada e fragmentada.
5	**Otimizado**	Os processos estão refinados ao nível das melhores práticas, baseados em resultados de aperfeiçoamento contínuo e modelagem de maturidade com outras organizações. A TIC é usada de forma integrada para automatizar fluxos de trabalho, fornecendo ferramentas para aperfeiçoar a qualidade e eficiência, e fazendo com que a empresa, quando necessário, se adapte rapidamente.

Fonte: ITGI (2007) e ISACA (2012a)

> "Existem casos onde os marcadores de auto avaliação, os quais refletem onde a organização se encontra segundo sua maturidade e onde ela tem intenção de chegar, ficam separados por um "gap" que reflete o esforço necessário para atingir esta meta estratégica. Visando apoiar que esta meta possa ser alcançada, este "gap" acaba sendo descrito de maneira mais detalhada para posteriormente servir de insumo para uma análise mais apurada. Esta análise resulta no planejamento de projetos que possibilitem que a organização atinja suas metas estratégicas para segurança e controle da TIC" (ALMEIDA NETO, 2015, p. 57).

Prado et al. (2016) ainda comentam que o COBIT, para medir um processo, utiliza dois tipos de indicadores:

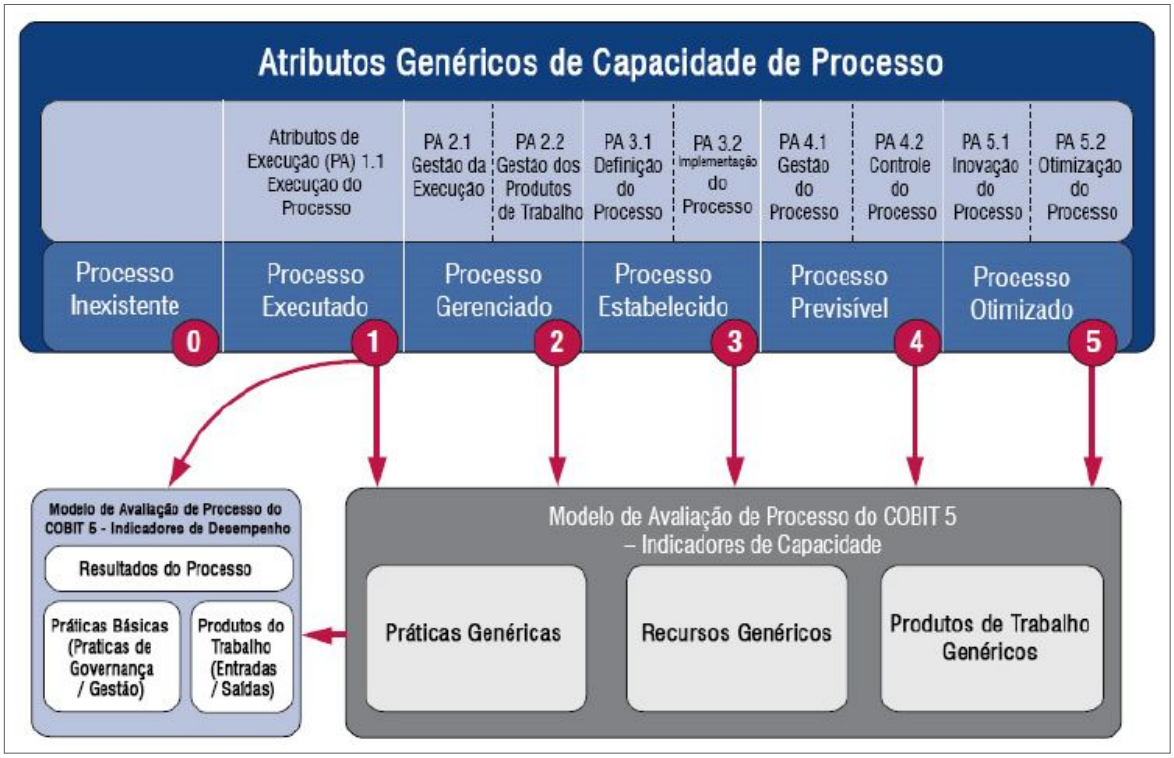
- Medições de resultados (outcome measures), que indica se um processo de TI atingiu

os objetivos de negócios, e também é conhecido como lag indicators;

- Indicadores de desempenho (performance indicators), que indica o quanto os processos de TIC estão sendo bem executados no atendimento aos objetivos do negócio. Sendo conhecido como lead indicators.

No COBIT 5, baseado na ISO/IEC 15.504, não há mais um modelo de maturidade específico. O mesmo trabalha com uma abordagem da avaliação da capacidade de processo ISACA (2012a), conforme exibido na Figura 10. Este modelo fornece meios para medir o desempenho dos processos de governança e gestão especificados no modelo de referência do COBIT 5 (ALMEIDA NETO, 2015).

Figura 10 – Modelo de Capacidade de Processo - COBIT 5



Fonte: ISACA (2012a, p. 44)

Os atributos de maturidade do COBIT 4.1 e os atributos de capacidade de processo do COBIT 5 não são idênticos. Eles sobrepõem-se e mapeiam até certa medida (ISACA, 2012a). As organizações que utilizam a abordagem dos atributos do modelo de maturidade do COBIT 4.1 podem reutilizar os atuais dados da sua avaliação e reclassificá-los segundo as avaliações de atributos do COBIT 5 (ISACA, 2012a).

3.3.2 O-ISM3

O segundo modelo de maturidade para segurança da informação mais citado no levantamento da literatura realizado foi o Open Information Security Management Maturity

Model (O-ISM3). O O-ISM3 é um padrão que trata, essencialmente, da maturidade dos sistemas de gerenciamento da segurança da informação, para qualquer tipo de organização (THE OPEN GROUP, 2017).

A segunda versão do O-ISM3 aponta como objetivos deste normativo (THE OPEN GROUP, 2017):

- Fornecer uma abordagem para criar Sistemas de Gerenciamento de Segurança da Informação (SGSIs) que estejam totalmente alinhados com as necessidades da missão e em conformidade com o negócio;
- Fornecer uma abordagem que se aplique a qualquer organização, independentemente do tamanho, contexto e recursos;
- Permitir que as organizações priorizem e otimizem seus investimentos em segurança da informação;
- Permitir a melhoria contínua dos SGSIs usando métricas;
- Permitir a terceirização de processos de segurança verificada e controlada por métricas.

O seu modelo de maturidade oferece aos gerentes, auditores e organizações uma abordagem para avaliar, especificar, implementar, mensurar e melhorar o SGSI. Para isso define cinco níveis: não definido, definido, gerenciado, controlado e otimizado (THE OPEN GROUP, 2011) e se fundamenta nas boas práticas de vários padrões como o CMMI, ITIL, ISO/IEC 9000 e ISO/IEC 17.799 e 27.001 (RIGON et al., 2014). Sendo, desta forma, passível de ser utilizado em conjunto e compatível com os padrões citados (CORDEIRO, 2017).

Os cinco níveis de maturidade para os processos de segurança da informação, definidos pelo O-ISM3, podem ser definidos como (CORDEIRO, 2017, p. 46):

- 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 executadas quando necessário. As práticas não são formalmente aprovadas, acompanhadas e documentadas;
- Nível 2 – Definido: Os requisitos básicos para a área de controle são planejados, implementados e repetíveis;
- Nível 3 - Gerenciado: A principal distinção do Nível 2, Definido, é que além de ser repetitivo os processos utilizados são mais maduros, documentados, aprovados e implementados 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.

O O-ISM3 define a capacidade em termos de métricas e práticas de gerenciamento. Exigindo a vinculação dos objetivos e metas de segurança da informação aos objetivos de negócios. Define um número abrangente, porém controlável, de processos de segurança da informação. E seus níveis de maturidade ajudam as organizações a escolher a escala do SGSI mais apropriada às suas necessidades (THE OPEN GROUP, 2017).

Embora muitas abordagens de gerenciamento da segurança da informação considerem a avaliação de risco como um primeiro estágio necessário, o O-ISM3 não exige uma abordagem baseada em avaliação de risco. Porém o modelo permite sua utilização a qualquer momento (THE OPEN GROUP, 2017).

The Open Group (2017) ainda aponta que, em alguns casos, uma empresa pode decidir que não é necessário fazer uma avaliação de risco formal para decidir se precisa de um controle de segurança. Por exemplo, os controles podem ser escolhidos com base em (THE OPEN GROUP, 2017):

- Senso comum;
- Melhores práticas (senhas);
- Aprendendo com incidentes (melhores firewalls ou Antivírus);
- Uma análise de vulnerabilidade ou ameaça especificamente focada.

Desta forma, por não abordar a ISO/IEC 27.005 ou outro modelo para risco, o O-ISM3 não mede o risco ou a segurança diretamente (KAROKOLA; KOWALSKI; YNGSTRÖM, 2011).

Por fim, Rea-Guaman et al. (2017) apontam características relevantes no O-ISM3:

- Gerência por métricas de segurança da informação;
- Ajuda a manter a organização em um nível aceitável de risco;
- Adaptação a organizações pequenas e grandes;
- Amplamente usado e adaptável a necessidades específicas. Por exemplo, segurança cibernética.

3.3.3 Systems Security Engineering Capability Maturity Model (SSE-CMM)

O Modelo de maturidade de capacidade de engenharia de segurança de sistemas, Systems Security Engineering Capability Maturity Model (SSE-CMM) foi o terceiro modelo

mais citado no levantamento da literatura realizado. É um dos padrões mais amplamente utilizados internacionalmente em relação à definição e implementação de processos de segurança, pois define em detalhes os processos que devem ser levados em conta em qualquer organização que deseje implementar um processo de segurança da informação (REA-GUAMAN et al., 2017).

Segundo a ISSEA (2018) o SSE-CMM descreve as características essenciais do processo de engenharia de segurança de uma organização que devem existir para garantir uma boa engenharia de segurança. O modelo destina-se a ser utilizado como (ISSEA, 2018):

- Ferramenta para as organizações avaliarem as práticas de engenharia de segurança e definirem melhorias para as mesmas.
- Mecanismo padrão para os clientes avaliarem a capacidade de engenharia de segurança de um provedor.
- Base para organização de avaliação de engenharia de segurança (por exemplo, certificadores de sistema e avaliadores de produto) para estabelecer evidências baseadas em capacidade da organização (como um ingrediente para garantia de segurança do sistema ou projeto). O SSE-CMM aborda atividades de engenharia de segurança que abrangem todo o produto confiável ou o seguro ciclo de vida do sistema, incluindo definição de conceito, análise de requisitos, projeto, desenvolvimento, integração, instalação, operações, manutenção e desfazimento. O SSE-CMM aplica-se a desenvolvedores de produtos seguros, desenvolvedores e integradores de sistemas seguros e organizações que fornecem serviços de segurança e engenharia de segurança. A SSE-CMM aplica-se a todos os tipos e tamanhos de organizações de engenharia de segurança, como comercial, governamental e acadêmica.

Para fins deste modelo, uma organização de engenharia de segurança é definida como o grupo de pessoas, tanto os gerentes quanto a equipe técnica, que tem a responsabilidade de implementar o processo de engenharia de segurança (REGULWAR; GULHANE; JAWANDHIYA, 2010).

A norma 21.827 desenvolvida pela ISO/IEC foi criada em alinhamento com o SSE-CMM, desenvolvido pela "International Systems Security Engineering Association - ISSEA (CORDEIRO, 2017; REA-GUAMAN et al., 2017). De acordo com a norma ISO/IEC 21.827, 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 (CORDEIRO, 2017).

O modelo SSE-CMM é baseado e adota grande parte da estrutura do SEI-CMM. Enquanto o SEI-CMM tem como alvo os aspectos gerenciais e organizacionais de uma corporação, o SSE-CMM é direcionado aos aspectos da organização de engenharia de segurança dentro de uma organização maior (REGULWAR; GULHANE; JAWANDHIYA, 2010).

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 (CORDEIRO, 2017).

A ISO/IEC 21827:2008 define seis níveis de maturidade para os processos de segurança da organização. Uma descrição mais detalhada de cada nível de maturidade pode ser observada a seguir (SSE-CMM PROJECT, 2003; CORDEIRO, 2017):

- 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.

Regulwar, Gulhane e Jawandhiya (2010) apresentaram, em seu trabalho, um framework para maturidade em segurança da informação, de cinco níveis de maturidade, baseado no SSE-CMM. Segundo Regulwar, Gulhane e Jawandhiya (2010) o SSE-CMM representa as práticas mais importantes envolvidas na execução de engenharia de segurança.

Após a apresentação dos diversos estudos sobre a área de maturidade, conceituando-a e demostrando exemplos, o presente trabalho prossegue adentrando mais profundamente na área de segurança onde será apresentada a família de normas ISO/IEC 27.000.

3.4 Família de Normas ISO/IEC 27.000

A família 27.000 da ISO/IEC é o aglomerado de normas, sendo a maioria de segurança da informação, por isso, muitas vezes é chamada de família de normas ISO da Segurança da Informação. Cada uma das normas ou relatórios técnicos com sua finalidade específica e voltada a uma área da segurança conforme detalhadas abaixo, de acordo com Palma (2016), ISO27k (2016) e ISO (2017).

ISO/IEC 27.000:2016: é uma norma generalista que fornece uma visão geral dos sistemas de gestão de segurança da informação e define termos relacionados, criando um vocabulário ou glossário padrão às definições formais.

ISO/IEC 27.001:2013: a norma que define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI).

ISO/IEC 27.002:2013: é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.

ISO/IEC 27.003:2010: A ISO 27.003 contém um conjunto de diretrizes para a implementação do SGSI. Enquanto a ISO 27.001 disponibiliza apenas requisitos, aqui obtemos uma orientação detalhada.

ISO/IEC 27.004:2009: define métricas de medição para a gestão da segurança da informação. Pode ser uma importante aliada no momento de definirem-se metas de níveis de serviço para a segurança da informação, ou mesmo executar o check e act do SGSI.

ISO/IEC 27.005:2011: cobre a gestão de riscos em segurança da informação. Grande parte do escopo da ISO 27.005 pode ser interpretada como a sessão 4 da norma ISO 27.001 detalhada na perspectiva dos riscos.

ISO/IEC 27.006:2015: defini requisitos para organizações que trabalham com auditoria e certificação de sistemas de gestão de segurança da informação. Em outras palavras, os requisitos na perspectiva da empresa auditando o seu cliente, para validar um SGSI.

ISO/IEC 27.007:2011: aborda diretrizes para guiar a auditoria do sistema de gestão da segurança da informação. Ela deve ser usada junto com a ISO 27.006 assim como a ISO 27.002 deve ser usada em conjunto com a ISO 27.001.

ISO/IEC TR 27.008:2011: relatório técnico que complementa a ISO/IEC 27.007. Ele se concentra na auditoria dos controles de segurança da informação fornecendo diretrizes.

ISO/IEC 27.009:2016: norma que aponta aplicação da ISO 27.001 em setores específicos.

ISO/IEC 27.010:2015: aborda um guia para a comunicação em gestão da segurança da informação tanto no escopo da organização como fora dela (sobretudo entre empresas do mesmo setor).

ISO/IEC 27.011:2008: guia de gestão da segurança da informação para empresas de telecomunicações.

ISO/IEC 27.013:2016: trata-se de um guia para implementar a ISO 27.001 em uma organização de forma integrada com a ISO 20.000 (norma que atribui os requisitos para gestão de serviços de tecnologia da informação).

ISO/IEC 27.014:2013: técnicas para governança de segurança da informação. Este objetivo é buscado por tal norma através de uma especificação de como avaliar, dirigir, controlar e comunicar todas as práticas internas da empresa relacionadas à segurança da informação, de forma que sejam compreendidas e estejam alinhadas com necessidades da área de negócio.

ISO/IEC TR 27.015:2012: relatório técnico que aborda a gestão da segurança da informação para serviços financeiros. Pode ser interpretada como uma norma que fornece controles e diretrizes complementares a ISO 27.002 para empresas e departamentos deste segmento.

ISO/IEC TR 27.016:2014: o mesmo raciocínio da ISO 27.015, só que para o setor de economia.

ISO/IEC 27.017:2015: controles específicos para cloud computing.

ISO/IEC 27.018:2014: cobre especificamente a privacidade (PII - Personally Identifiable Information) para serviços em cloud computing. É uma norma que complementa a ISO 27.017.

ISO/IEC TR 27.019:2013: norma com controles específicos para indústria de energia.

ISO/IEC TR 27.023:2015: Mapeia as edições revisadas da ISO/IEC 27.001 e ISO/IEC 27.002, visando mostrar a relação de correspondência entre as versões revisadas.

ISO/IEC 27.031:2011: propõe um guia de princípios/conceitos por trás do papel da segurança da informação para TIC no sentido de garantir a continuidade dos negócios.

ISO/IEC 27.032:2012: aborda "Cybersecurity". Está em sua definição à preservação da confidencialidade, integridade e disponibilidade da informação em "Cyberspace".

ISO/IEC 27.033-1:2015: esta é uma das seis partes da norma 27.033. O conjunto de normas 27.033-1 a 27.033-6 são derivadas das cinco partes da norma de segurança em

redes: ISO/IEC 18.028. A ISO/IEC 27.033-1 trata sobre a introdução e conceitos gerais para segurança em redes. ISO/IEC 27.033-2:2012: guia para o planejamento, desenho, implementação e documentação da segurança em redes. ISO/IEC 27.033-3:2010: tem o objetivo de definir os riscos específicos, técnicas de projetos e controles relacionados à segurança em redes. ISO/IEC 27.033-4:2014: propõe uma visão geral e requisitos para identificação e análise de ameaças para a segurança da informação relacionadas a gateways de segurança da informação que compõem a arquitetura de segurança em redes. ISO/IEC 27.033-5:2013: protegendo a comunicação entre redes usando Virtual Private Networks (VPNs). ISO/IEC 27.033-6:2016: define riscos, técnicas de projeto e desenho e controles específicos para a segurança da informação em redes sem fio e rádio.

ISO/IEC 27.034-1:2011: segurança da informação em aplicações - parte 01. Nesta primeira parte, é definida e abordada uma introdução e conceitos. É complementada pela. ISO/IEC 27.034-2:2015: segurança da informação em aplicações - parte 02. A segunda parte trata sobre a organização normativa para segurança em aplicações.

ISO/IEC 27.035:2011: guia detalhado para a gestão de incidentes de segurança da informação, cobrindo o processo de mapeamento de eventos, incidentes e vulnerabilidades de segurança.

ISO/IEC 27.036-1:2014 e 27.026-2:2014: segurança da informação para o relacionamento com fornecedores. Oferece orientações sobre a avaliação e tratamento de riscos de segurança da informação envolvidos na aquisição de informações ou produtos relacionados com as TIC de outras organizações.

ISO/IEC 27.037:2012: orientações para a identificação, coleta, aquisição e preservação de evidências forenses digitais. Esta norma está focada na manutenção da integridade destas evidências.

ISO/IEC 27.038:2014: especificação para redação digital, tratando sobre requisitos para a redação e compartilhamento da informação digital de forma adequada, seja ela publicada internamente na organização ou a partes externas.

ISO/IEC 27.039:2015: guia para seleção, contratação, desenho, operação e administração de sistemas IDS (Intrusion Detection Systems).

ISO/IEC 27.040:2015: fornece orientação técnica para as organizações mitigar riscos no armazenamento de dados.

ISO/IEC 27.041:2015: fornece orientação sobre mecanismos para garantir que os métodos e processos utilizados na investigação de incidentes de segurança da informação são aptos.

ISO/IEC 27.042:2015: mais uma entre as normas forenses, sendo que esta prevê diretrizes para a análise e interpretação de evidências digitais.

ISO/IEC 27.043:2015: princípios e processo de investigação de incidentes da segurança da informação. Esta é mais uma norma voltada exclusivamente para gestão de incidentes de segurança, assim como a ISO 27.035.

ISO/IEC 27.789:2013: trata questões relativas a auditorias em sistemas e registros eletrônicos na área de saúde.

ISO/IEC 27.799:2016: aborda o gerenciamento de segurança da informação, baseado na ISO 27.002, específico para a área de saúde.

Como percebido existem alguns saltos na sequência de normas listadas na família ISO/IEC 27.000. Ressalta-se que alguns desses espaços estão vagos e outros não foram listados por não serem diretamente relacionados à área de Segurança da Informação, por exemplo as ISO's: 27.020:2010, 27.025:2010, 27.026:2011, 27.027:2014, 27.048:11 e 27.065:2011.

Por outro lado, podemos citar outras normas que tratam de segurança da informação, mas que não foram inseridas na família 27.000, como é o caso da norma ISO/IEC 15.408. Esta norma é dividida em três partes: ISO/IEC 15.408-1:2009, ISO/IEC 15.408-2:2008 e ISO/IEC 15.408-3:2008, e tratam de segurança para produtos de TI, mais diretamente como segurança lógica das aplicações e para o desenvolvimento de aplicações seguras.

Alencar et al. (2018b) e Alencar et al. (2018c) apontaram, após o mapeamento realizado, que as principais normas, padrão, modelo, framework, documento, metodologia ou teoria utilizado pelos autores para implantação e avaliação da governança, gestão ou maturidade da segurança da informação corporativa são as normas ISO/IEC 27.001, 27.002 e 27.005, além do COBIT, já apresentado.

Diante da importância de tais normas, as mesmas serão detalhadas abaixo. Como complemento, devido a correlação com a área de Governança de Segurança da Informação, a norma ISO/IEC 27.014 também será brevemente abordada.

3.4.1 ISO/IEC 27.001

A norma ABNT NBR ISO/IEC 27.001:2013, nomeada como: Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos, é um modelo internacional para a gestão da segurança da informação, sua versão atual foi publicada em 2013, é baseada na norma BS 7799 (British Standard), que surgiu na década de 90 por uma iniciativa da instituição inglesa para padronizar os processos de segurança da informação e melhorar a qualidade dos dados.

Esta norma aponta os requisitos básicos para a implantação de um Sistema de Gestão de Segurança da Informação (SGSI), assim como todo seu controle e gerenciamento (ABNT, 2013a). É a principal norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão da segurança da informação. Por isso, é conhecida como a única norma internacional que pode ser auditável e que define os requisitos para um SGSI.

A estrutura da norma é composta por onze seções, são elas:

- 0 Introdução;

- 1 Escopo;
- 2 Referências normativas;
- 3 Termos e definições;
- 4 Contexto da organização;
- 5 Liderança;
- 6 Planejamento;
- 7 Apoio;
- 8 Operação;
- 9 Avaliação do desempenho;
- 10 Melhoria.

Complementa a estrutura da norma o seu Anexo A, detalhado a seguir.

O SGSI proposto é um modelo focado em estabelecer, monitorar, rever, manter e melhorar um sistema de gestão da segurança da informação. É um código de práticas para segurança da informação. A sua declaração está estruturada em seções, cada seção tem uma série de controles que podem ser implementados, que vai depender do tamanho e necessidade de cada empresa. O Anexo A, da norma, detalha 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles que podem ser implementados (ABNT, 2013a).

As 14 seções apontadas no Anexo A da norma são (ABNT, 2013a):

a) Política de Segurança da Informação;

b) Organizando a Segurança da informação;

c) Segurança em Recursos Humanos;

d) Gestão de ativos;

e) Controle de Acesso;

f) Criptografia;

g) Segurança Física e do Ambiente;

h) Segurança nas Operações;

i) Segurança nas Comunicações;

j) Aquisição, Desenvolvimento e Manutenção de Sistemas;

k) Relacionamento na Cadeia de Suprimento;

l) Gestão de Incidentes de Segurança da Informação;

m) Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio;

n) Conformidade.

Fernandes e De Abreu (2014) comentam que esta norma internacional foi preparada para promover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar o sistema de gestão de segurança da informação, podendo ser usada visando avaliação da conformidade por partes interessadas internas e externas.

Conforme ABNT (2013a) os requisitos definidos nesta norma são genéricos e é pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza. Qualquer exclusão de algum de seus controles precisa ser criteriosa e justificada, e a aceitação de que os riscos associados, inerentes à retirada, foram aceitos pelas pessoas responsáveis precisa ser fornecida. A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.

Sobre esse assunto, Fontes (2011) elaborou uma base de dados com informações referentes a política de segurança da informação, analisando o que as empresas definem em sua PSI. O resultado desta análise esclareceu a realidade das organizações naquele período, como a organização enxergava a segurança da informação e como isto estava sendo tratado internamente, apontando para uma incorreta ou incompleta aplicação da norma por parte das empresas.

Para Beckers et al. (2013) a ISO/IEC 27.001 não está bem clara para as empresas que o implantam e até propõe uma análise das implantações para entender o motivo. Fato corroborado por Breier e Hudec (2012), que complementa afirmando ser necessário tornar mais legível a norma e propõe a construção de uma hierarquia dos processos da ISO/IEC. Fatos que corroboram com a indicação de Fontes (2011) e também citado por Silva e Barros (2017).

3.4.2 ISO/IEC 27.002

A norma em questão iniciou sua publicação como ISO/IEC 17.799, tendo sido homologada no Brasil em setembro de 2001, atualizada e, posteriormente, renomeada para ISO/IEC 27.002, ambos os eventos ocorridos em 2005. Em 2013 foi atualizada para a versão atual, nomeada como: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação (ABNT, 2013b).

Esta norma contempla cinco seções explicativas, são elas:

- 0 Introdução;

- 1 Escopo;
- 2 Referências normativas;
- 3 Termos e definições;
- 4 Estrutura desta Norma.

Após essas seções, a norma continua com mais quatorze seções, seguindo a mesma divisão do Anexo A da ISO/IEC 27.001 (ABNT, 2013a), 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles que podem ser implementados, sendo um detalhamento da sua implementação (ABNT, 2013b).

Tais normas (ISO/IEC 27.001 e 27.002) são tidas como os principais documentos de referência para elaboração de um SGSI, sendo a escolha de Silva Neto, Alencar e Queiroz (2015), bem como de Fontes (2011) ao pesquisar um padrão mínimo para elaboração e implantação de uma PSI.

Pode ser entendida como um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação. Sendo recomendável que a norma seja utilizada em conjunto com a ISO/IEC 27.001, mas pode ser também consultada de forma independente com fins de adoção das boas práticas. A identificação de quais controles devem ser implementados requer planejamento e atenção cuidadosa em nível de detalhes. Tendo, como um dos principais benefícios desse modelo, a prevenção contra perdas financeiras que a organização pode ter no caso de ocorrências de incidentes de segurança da informação (FERNANDES; DE ABREU, 2014).

Um sistema de gestão da segurança da informação bem-sucedido requer apoio de todos os funcionários da organização. Isto pode também exigir a participação de acionistas, fornecedores ou outras partes externas. Orientações de especialistas externos podem também ser necessárias (ALENCAR, 2011).

Ativos são foco de ameaças, tanto acidentais como deliberadas. Os ativos, por exemplo, processos corporativos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (bem como novas leis e regulamentações), podem criar novos riscos de segurança da informação, conforme enfoca a ABNT (2013b).

De um modo geral, a segurança da informação eficaz também garante à direção e outras partes interessadas que os ativos da organização estejam razoavelmente seguros e protegidos contra danos, agindo como um facilitador dos negócios (FERNANDES; DE ABREU, 2014).

Um ponto interessante da norma ISO/IEC 27.002 ABNT (2013b), atualmente em vigor, é a sua alteração de visão ao tratamento das pessoas (ALENCAR, 2008). Na atualização de 2005, entre outras alterações, mudou sua compreensão do aspecto humano ao modificar sua antiga seção 6.2.1 “Educação e treinamento em segurança da informação”,

divulgada na primeira edição (ISO/IEC 17799 de 2001), para a seção 8.2.2 "Conscientização, educação e treinamento em segurança da informação", divulgada na atualização da norma em 2005 (ISO/IEC 27.002 de 2005), nomenclatura e concepção que permanece na versão 2013 (ABNT, 2013b), atual.

3.4.3 ISO/IEC 27.005

A ISO/IEC 27.005 foi publicada em meados de 2008, tendo como foco a utilização de técnicas na Gestão de Riscos em Segurança da Informação (GRSI). Esta norma dará um suporte à organização para que faça a gestão de risco seguindo as técnicas que associam as combinações de probabilidade e consequência de determinados eventos indesejados causar-lhe perdas (ABNT, 2011).

No dia 17 de novembro de 2011, publicou uma revisão da norma que substitui a edição anterior, esta que ficaria conhecida como ABNT NBR ISO/IEC 27.005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos da Segurança da Informação. Foi desenvolvida para ajudar na implementação dos processos de segurança da informação, através do fornecimento de diretrizes para o processo de GRSI (GHAZOUANI et al., 2014).

Existem metodologias e normas que direcionam para um bom desenvolvimento de uma gestão de risco, onde cada uma fornece um conjunto de diretrizes distintas para o gerenciamento dos riscos e nos vários modelos de referência para gestão dos riscos que visam nortear as implementações necessárias, entre as primordiais, está a norma ISO/IEC 27.005:2011 (KONZEN, 2013).

A ISO/IEC 27.005 é a norma que fornece diretrizes e descreve um processo genérico para a organização na gestão de seus riscos de segurança da informação (PONTES, 2009). Os processos descritos nesta norma formam uma base para construção de metodologias para gestão de riscos, que direciona o que a organização deve fazer, mas não detalha suficientemente como executar as atividades, dificultando na organização ou em algum setor a sua implementação (KONZEN, 2013).

Segundo a presente norma (ABNT, 2011), os controles em segurança da informação incluem qualquer processo, política, procedimento, diretriz, prática ou estrutura organizacional, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modificam o risco da segurança da informação.

A ABNT NBR ISO 27.005 é aplicável a todos os tipos de organizações que pretendem gerir os riscos que possam comprometer qualquer uma das áreas ou princípios inerentes à segurança da informação da organização, sejam elas públicas ou privadas, bem como indiferente do tamanho ou porte financeiro (GHAZOUANI et al., 2014).

O risco de segurança da informação pode ser entendido como a possibilidade da ameaça causar problema explorando vulnerabilidades ao bem empresarial. Portanto precisa-se medir a consequência gerada pela combinação do evento e sua probabilidade de ocorrência (ABNT, 2011).

Risco também pode ser visualizado como a possibilidade de um determinado evento adverso afetar de forma negativa a capacidade de uma organização em alcançar seus objetivos de forma parcial ou total. Nesse contexto, o risco é considerado um evento indesejável (FERNANDES; DE ABREU, 2014).

Para entender melhor o risco, é importante compreender o conceito de ativo, ameaça, vulnerabilidade e consequência. Estes podem ser definidos, de forma sumária, como:

- Ativo: qualquer elemento, tangível ou não, que tenha valor para a organização, devendo, por isso, ser devidamente protegido. É todo elemento que manipula a informação, inclusive sua interação pelo seu emissor (SÊMOLA, 2013);
- Ameaça: são eventos que causam prejuízo a organização (ABNT, 2011);
- Vulnerabilidade: fragilidade de um ativo ou conjunto de ativos que possa ser explorado por uma ameaça, ou conjunto dela, tornando-se sensível aos ataques (SILVA, 2010). As vulnerabilidades sozinhas não provocam incidentes, porém estas irregularidades e brechas na segurança podem ser exploradas por um agente malicioso causador ou condicional favorável para um evento negativo (KONZEN, 2013);
- Consequência: está atrelada com as perdas operacionais relativa com a proteção de ativos, fazendo parte do indicador do valor operacional de cada ativo da organização, levando em consideração para determinação das consequências operacionais, para sua investigação e tempo de reparo, de trabalho perdido e o custo econômico para reparar prejuízo, reputação e imagem da empresa (ABNT, 2011).

Jirasek (2012) aponta que o gerenciamento de riscos é uma área que está em constante movimento para responder a novas ameaças, padrões e tecnologias. Diante disto, ele afirma a necessidade dos modelos, normas e frameworks de segurança não apenas para gerir a segurança da informação, mas para ajudar a explicar por que a segurança é importante, bem como justificar a manutenção, apoio e investimentos nesta área. Cabendo a área de segurança da informação não apenas escutar e se alinhar ao negócio, mas também educar os usuários e gestores sobre os assuntos de sua área. Neste contexto, o trabalho aponta a correlação da segurança entre os diversos setores da organização, os papéis da segurança da informação, bem como definindo que ações são aplicáveis ou quem são os responsáveis em cada nível hierárquico da organização.

Por fim, é importante ressaltar que frequentemente utilizam-se alguns mecanismos, modelos ou abordagens a fim de se avaliar, definir métricas e procedimentos para calcular os controles necessários para efetividade e eficácia de segurança da informação. Por outro lado, é importante salientar que, para avaliar controles e mecanismos de segurança, é preciso entender e calcular o Return on Investment (ROI), em português retorno sobre o investimento, ou, de forma mais específica, Return on Information Security Investment (ROSI), em português, retorno sobre o investimento de segurança da informação. Métodos

que envolvam ROI e ROSI, alinhados com a gestão de risco em segurança da informação, são formas de evidenciar o quanto a organização precisa investir em segurança para evitar os impactos na sua estrutura organizacional para proteger seus ativos (PONTES, 2009).

3.4.4 ISO/IEC 27.014

A ISO/IEC 27.014 foi publicada em abril de 2013, sendo publicada a versão traduzida para o português do Brasil, pela Associação Brasileira de Normas Técnicas (ABNT) em meados de 2014, nomeada de ABNT NBR ISO/IEC 27.014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de Segurança da Informação, com intuito de apresentar uma série de ações para Governança de Segurança da Informação (GSI) (ABNT, 2013c).

A ISO/IEC 27.014 (ABNT, 2013c) se debruça sobre a vasta área de governança de segurança da informação apontando orientações sobre conceitos e princípios para o referido tema, provendo às instituições, indiferente de tamanho ou porte, diretrizes para avaliar, dirigir, monitorar e divulgar as ações inerentes à área de segurança da informação.

Manoel (2014) corrobora com o tema e afirma que a ISO/IEC 27.014 não detalha quem e como ela deve ser implementada nas organizações, mas propõe um modelo de GSI que tem por finalidade buscar o alinhamento dos objetivos estratégicos do negócio com a estratégia de segurança da informação. Neste contexto é possível agregar mais valor às instituições, pois visa assegurar o levantamento e análise dos riscos da informação e o seu correto direcionamento aos responsáveis.

A ISO/IEC 27.014 (ABNT, 2013c) apresenta os princípios da governança de segurança da informação, definindo como as empresas devem utilizar a segurança da informação. De forma sucinta, os princípios são:

- Estabelecer a segurança da informação em toda a organização;
- Adotar uma abordagem baseada em riscos, onde recomenda-se a utilização em conjunto da ISO/IEC 27.005;
- Estabelecer e Alinhar os investimentos;
- Assegurar a conformidade com os requisitos internos e externos;
- Promover um ambiente positivo de segurança, incluindo um tratamento especial às pessoas;
- Analisar criticamente o desempenho e resultado das ações de segurança da informação em relação aos resultados de negócios.

Diante do exposto, a correta implementação da GSI visará que a alta direção da empresa tenha clareza sobre a segurança de suas informações, possibilitando investimentos

e uma abordagem rápida em relação aos riscos existentes, bem como a conformidade com os regulamentos, como aponta Manoel (2014). Corroborando com os conceitos debatidos na seção de governança de segurança da informação.

3.5 Trabalhos Correlatos e Principais Influenciadores

Além do COBIT, O-ISM3 e das normas ISO/IEC 27.001, 27.002 e 27.005, já explicitados neste Capítulo, um conjunto de trabalhos influenciaram diretamente esta pesquisa. Seja por ser uma pesquisa com temática correlata, pela metodologia utilizada, pela motivação ou justificativa apresentada pelos autores.

Por ser um trabalho multidisciplinar, abrangendo, principalmente, as áreas de segurança da informação, maturidade e governança, diversos trabalhos poderiam estar elencados nesta seção, inclusive a maioria dos trabalhos referenciados até o momento que, pelas próprias citações, já indicam um pouco de sua pesquisa, contribuição e correlação com o presente trabalho.

É importante mencionar que os estudos elencados nesta seção, detalhados a seguir, foram selecionados por representar as principais áreas correlatas ou pesquisas que mais influenciaram o presente estudo. Não sendo, em hipótese alguma, desmerecimento a outras publicações existentes, referenciadas ou não nesta tese.

Dentre alguns autores a se mencionar, podemos destacar as publicações de Alencar, Almeida Neto, Luna e Rigon.

As publicações na área de segurança da informação propostas por Alencar abordam o fator humano na segurança da informação (ALENCAR, 2008), posteriormente se vê um detalhamento maior, dentro do fator humano, apresentando estratégias para tratamento e mitigação das ameaças internas, mais precisamente os insiders (ALENCAR, 2011; ALENCAR; QUEIROZ; QUEIROZ, 2013a; ALENCAR; QUEIROZ; QUEIROZ, 2013b), e a utilização das pessoas com uma camada ativa da segurança da informação corporativa (ALENCAR; LIMA; FIRMO, 2013a; ALENCAR; LIMA; FIRMO, 2013b), ou seja, as pessoas atuando para auxiliar diretamente a aplicação e manutenção segurança da informação. Mais recentemente, em Silva Neto, Alencar e Queiroz (2015), foi abordado uma simplificação das ISO/IEC 27.001 e 27.002 como uma forma de se conseguir uma melhoria para a área de segurança da informação em Pequenas e Médias Empresas.

Ressalta-se que os questionários para levantamento de dados nesta tese (Apêndices B e C), foram baseados nas pesquisas de Alencar (ALENCAR, 2011; ALENCAR; QUEIROZ; QUEIROZ, 2013a; ALENCAR; QUEIROZ; QUEIROZ, 2013b; SILVA NETO; ALENCAR; QUEIROZ, 2015).

Luna e seus coautores podem ser vistos como precursores na área de governança ágil. Dentre os trabalhos mais recentes, podemos citar Luna et al. (2010) abordando a governança ágil e colocando uma quebra no paradigma atual de governança (tradicional

e formal). Em 2013 apontaram um modelo para gerenciamento da governança ágil em empresas (LUNA; KRUCHTEN; MOURA, 2013). Em 2014 lançaram uma revisão sistemática da área (LUNA et al., 2014), sendo apontada pelos autores como a primeira em governança ágil. Posteriormente Luna continuou propondo melhorias, adaptações e ajustes à proposta de governança ágil, não apenas em sua concepção, aplicação e forma de gerenciamento, como também alterando e ampliando a definição dada para a área Luna, Kruchten e Moura (2015), Luna et al. (2016).

Almeida Neto e seus coautores apontam uma série de artigos na área de governança ágil mais precisamente propondo um modelo de maturidade para governança ágil e diversas avaliações do mesmo. Entre os artigos do autor, podemos citar Almeida Neto e Moura (2014), um dos trabalhos que apresenta o MAnGve Maturity Model, o modelo criado pelos autores para aferir e gerenciar a maturidade em governança ágil, a avaliação do mesmo (ALMEIDA NETO et al., 2015a) e outra avaliação baseada na abordagem de grupo focal (ALMEIDA NETO et al., 2015b), culminando em sua tese de doutorado (ALMEIDA NETO, 2015).

Os conceitos de governança ágil apresentados nas pesquisas encabeçadas por Luna e Almeida Neto apoiaram o presente estudo com o arcabouço que viabiliza, de forma já comprovada, em especial pelos autores em questão, a implantação de políticas e estratégias mais flexíveis e ágeis no ambiente corporativo. Fato de interesse deste trabalho.

As diversas pesquisas de Rigon e seus coautores vêm contribuindo para a segurança da informação na área de maturidade em segurança da informação. Abordando a necessidade de melhor mensuração formal da segurança da informação, visto que diversos processos, serviços e sistemas atuais, por mais que sejam vastamente utilizados, não foram, em grande parte, concebidos para serem seguros. Com este pensamento, Rigon propõem um modelo de avaliação de maturidade da segurança da informação como um processo para gerir, a partir da medição de um conjunto de controles mais abrangentes, a segurança da informação. Para tal modelo foi inserido, entre outros, alguns pontos da ISO 27.002:2005 e tem a sua base de mensuração apoiada pela escala de COBIT. Este modelo pode ser visto em Rigon e Westphall (2011) e expandido em Rigon e Westphall (2013). Tal proposta, após um maior detalhamento, também é exposta em Rigon et al. (2014) como um modelo de avaliação cíclica da maturidade da segurança da informação que promete ser um processo de gestão para a melhoria contínua da segurança, sob a forma de um modelo genérico aplicável a todos os tipos de organizações, independentemente do tamanho ou do campo, usando todos os controles presentes na norma ISO/IEC 27.002.

Os quatro principais blocos e publicações supracitados, encabeçados por Alencar, Almeida Neto, Luna e Rigon, englobam, de forma geral, os principais temas deste trabalho multidisciplinar (governança, segurança da informação e maturidade), mas, para demonstrar outras visões da vastidão que estas áreas cobrem, um conjunto de trabalhos são detalhados a seguir.

Woodhouse (2008) descreve uma proposta teórica de um modelo de maturidade para avaliar o SGSI da corporação e, consequentemente, classificar a maturidade da empresa. A proposta de Woodhouse (2008) contempla nove níveis: -3 (Subversivo), -2 (Arrogante), -1 (Obstrutivo), 0 (Negligente), 1 (Funcional), 2 (Técnico), 3 (Operacional), 4 (Gerenciado) e 5 (Estratégico). O autor afirmou que a intenção do modelo proposto era de destacar o papel crítico que a cultura corporativa desempenha no processo de segurança da informação. Se limitando a apresentar a proposta, sem uma etapa de avaliação ou implantação e sem apresentar a forma de utilização ou medição para categorizar a empresa em determinado estágio.

Lessing (2008) estruturou um modelo genérico de maturidade de segurança da informação. Para isso o autor extraiu características de oito outros guias ou modelos de maturidade de segurança da indústria, entre eles o O-ISM3 e o SE-CMM. O modelo genérico de Lessing (2008) é divido em 5 níveis e para cada nível o mesmo elencou melhores práticas existentes nos oito documentos que utilizou como base. Neste modelo, as melhores práticas a serem abordadas em cada nível são expostas a seguir:

- Nível 1: Gestão de ativos, gestão da segurança, segurança física e ambiental e medição de desempenho da gestão da segurança.
- Nível 2: Necessidades e objetivos de controle, aplicações críticas de negócios, gestão da continuidade do negócio, organização e gestão da segurança da informação, medição do desempenho, gestão da segurança, gestão da segurança do pessoal, desenvolvimento de sistemas de informação e requisitos legais;
- Nível 3: Gerenciamento de segurança, desenvolvimento de sistemas de informação, gerenciamento de segurança e gerenciamento de conformidade.
- Nível 4: Gestão da segurança, gerenciamento de riscos e gerenciamento de conformidade.
- Nível 5: Continuidade do negócio, gerenciamento de conformidade, aplicações críticas de negócios, medição de desempenho, gerenciamento de segurança e a responsabilidade corporativa e criminal.

Segundo Lessing (2008), este trabalho não teve intenção de criar mais um modelo de maturidade de segurança, mas sim um modelo de condução de boas práticas podendo ser classificado como um modelo de maturidade.

Saleh (2011b) propõem um modelo de maturidade de segurança da informação para ser utilizado como uma ferramenta para avaliar a capacidade das organizações de alcançar objetivos de segurança da informação. O trabalho aponta quatro domínios que afetam a segurança da informação em uma organização: o gerenciamento dos serviços, a governança corporativa, a cultura organizacional e a arquitetura dos sistemas. Para abranger

esses pilares, o modelo de maturidade de Saleh (2011b) possui cinco níveis de conformidade: Nenhuma Conformidade, Conformidade Inicial, Conformidade Básica, Conformidade Aceitável e Conformidade Total. Tais níveis e formas de aplicação, segundo o autor, caracterizam o modelo como um sistema completo e de melhoria contínua.

Dimitriadis (2011) publicou um artigo sobre segurança da informação na ótica dos negócios, onde realizou um estudo de caso da segurança da informação em uma rede lotérica. Para isso, trabalhou na junção de modelos e normas, pois fez uso do Business Model for Information Security (BMIS), além de um estudo comparativo entre as ISO's 27.001 e 27.002, amplamente utilizado para a criação e implantação de uma política de segurança da informação, a fim de suprir necessidades relacionadas ao negócio e aos problemas da segurança da informação.

Karokola, Kowalski e Yngström (2011) descrevem uma proposta teórica de um modelo de maturidade de segurança da informação para serviços de governo eletrônico. Basicamente, o modelo baseia-se nos resultados da análise crítica de diversos outros modelos de maturidade. É concebido em cinco níveis de maturidade, com suas respectivas dimensões de controle, são eles: Nível 1 - indefinido, Nível 2 - definido, Nível 3 - gerenciado, Nível 4 - controlado e o Nível 5 – otimizado. O trabalho é teórico, sem demonstração de aplicação do mesmo, e está limitado à definição dos cinco níveis para avaliar a maturidade de um SGSI especificamente para serviços de governo eletrônico, sem apresentar um método para a medição da situação atual da segurança ou o acompanhamento e evolução da segurança e processos conexos.

Silva, Menezes e Costa (2012) propõem um modelo que identifica, avalia e define o status de cumprimento da política de segurança corporativa. Esse estudo se diferencia por apresentar um modelo teórico para avaliar o nível de segurança da informação em um ambiente organizacional com foco sobre os conhecimentos, atitudes e comportamento do usuário final, identificando o nível e origem da diferença entre as diretrizes de segurança da informação estabelecidas pela empresa e as práticas reais de seu pessoal interno, parceiros, terceiros e fornecedores. O modelo foi desenvolvido visando auxiliar o cumprimento dos objetivos e políticas estabelecidas para a gestão da segurança da informação pela direção e contribuir para a manutenção de um programa de treinamento eficaz, bem como a sensibilização para a segurança da informação. O modelo trabalha com 23 indicadores e seus valores são utilizados para informar o cumprimento da política de segurança da empresa através de três status: bom, regular e ruim.

Jirasek (2012) aponta que o gerenciamento de riscos é uma área que está em constante movimento para responder a novas ameaças, padrões e tecnologias. Diante disto, ele afirma a necessidade dos modelos, normas e frameworks de segurança não apenas para gerir a segurança da informação, mas para ajudar a explicar por que a segurança é importante, bem como justificar a manutenção, apoio e investimentos nesta área. Cabendo a área de segurança da informação não apenas escutar e se alinhar ao negócio, mas também

educar os usuários e gestores sobre os assuntos de sua área. Neste contexto, o trabalho aponta a correlação da segurança entre os diversos setores da organização, os papéis da segurança da informação, bem como definindo que ações são aplicáveis ou quem são os responsáveis em cada nível hierárquico da organização. Jirasek (2012) não cria um modelo novo, mas aponta, de forma prática, onde cada modelo, framework ou norma (ISO/IEC 27.001, ISO/IEC 27.005, COBIT, entre outros) devem atuar e a correlação entre eles.

Tariq, Haq e Iqbal (2013) demonstram a formulação de um meio para se obter um acordo de nível de serviço para computação em nuvem baseado em métricas de segurança tendo o COBIT como framework base. Neste trabalho, os autores abordam a importância da utilização de métricas para mensurar o nível de segurança dos serviços, fato que é bastante consolidado para a análise de desempenho e construção de pacotes e cobranças de serviços, porém pouco explorado na área de segurança. Por fim, os autores refletem que a mensuração baseada no COBIT é um grande avanço, mas carece de melhorias e interconexões com SLA baseados na ISO 27.001:2005 e na NIST SP 800-53, sendo essas vertentes para trabalhos futuros.

Cholez e Girard (2014) descrevem um framework de avaliação de maturidade em segurança da informação e melhoria de processos para a gestão da segurança da informação em pequenas e médias empresas validado na indústria. Na construção do modelo foram realizados seis estudos de casos em PMEs do país de Luxemburgo para realização de seus ajustes. Posteriormente, tornou-se um modelo de serviço comercial, sendo realizados mais sete estudos de caso. Para aplicar o modelo, Cholez e Girard (2014) realizaram entrevistas. O questionário utilizado é composto de duas seções. A primeira seção se concentrou no lado organizacional, enquanto a segunda concentrou-se nos aspectos operacionais. O questionário contém 27 perguntas abertas e é baseado nas ISO/IEC 27.001 e 27.002. A escala de maturidade e o método de avaliação são inspirados na série padrão em Avaliação de Processos: ISO/IEC 15.504. A norma ISO/IEC 15.504 define 6 níveis de maturidade (de "processo incompleto" a "processo de otimização"), porém pela baixa maturidade das PMEs analisadas pelos autores, a escala de maturidade vai do 0 até o nível 4, onde o nível 4 (mais alto) é compatível com o primeiro nível de capacidade da ISO/IEC 15.504. Além disso, um nível deve ser totalmente atingido para estar no próximo nível.

O estudo de Coelho, Fernandes Junior e Proença Junior (2014) teve como objetivo principal apresentar o modelo GAIA-MLIS para avaliação dos níveis de maturidade dos SGSI das organizações e apresentar seus pontos fortes e fracos. De forma empírica criou-se um modelo de avaliação de segurança da informação através de cinco áreas distintas: hardware, software, pessoas, instalações e informação, adaptadas das seções da norma ISO/IEC 27.002. O GAIA-MLIS possui cinco níveis de maturidade, indo do Nível 0 ao 4, para avaliar as cinco áreas. Sendo baseado nas recomendações do COBIT 5 e das normas ISO/IEC 27.001 e 27.002. A aplicação do modelo se dá através de um questionário com 30 perguntas baseado na ISO/IEC 27.002.

Puricelli (2015) abordou aspectos humanos na gestão e governança de segurança da informação. Mais precisamente, o quanto a engenharia social é subestimada na área e como é possível conseguir informações, indiferente do tamanho da empresa, bem como da idade, localização, departamento ou cargo do funcionário. Por meio de técnicas de phishing, Puricelli (2015) revelou que esses tipos de ataques funcionam muito bem. Nessas avaliações, um em cada três funcionários (34%) clicou no link em um e-mail de "phishing" enviado como teste pelo autor e um em cada cinco (21%) também inseriu credenciais da empresa no formulário do site enviado. Os resultados são ainda mais impressionantes quando correlacionados ao fator temporal. De acordo com os resultados do autor, uma campanha de "phishing" provoca um rápido aumento da taxa de sucesso do ataque nas fases iniciais, alcançando 50% de taxa de eficiência apenas nos primeiros 20 minutos. Isso significa que o período disponível para uma reação eficaz é muito curto. Em suma, este estudo reflete os desafios da área de segurança da informação, dentro deles, a influência dos aspectos humanos na governança da segurança da informação.

Mahopo, Abdullah e Mujinga (2015) ao correlacionar as propostas da OCTAVE, ISO/IEC 27.001 e 27.002, COBIT, ITIL e Information Security Forum Standard of Good Practice (ISF SoGP), criaram uma abordagem qualitativa própria para gerenciamento de risco de segurança de TIC (IT Security Risk Based - ITSRB), visando a sua aplicação, por parte das organizações, para responder melhor aos riscos de TIC. Um ponto a se destacar do trabalho é a sua divisão em quatro fases (modelo PDCA – Plan, Do, Check e Act) e para cada fase o trabalho apresenta uma tabela com o objetivo, a frequência, o público alvo, o modelo do processo, ferramentas e quem deve ser responsável, consultado, informado e o aprovador.

Já Muthukrishnan e Palaniappan (2016) definem um modelo de maturidade para segurança operacional. Tal modelo visa retratar a maturidade das métricas de segurança utilizadas, criando um índice de maturidade de métricas de segurança como forma de aferir a confiança da métrica utilizada. Segundo os autores, tem-se bastante dificuldade em se mensurar a segurança da informação, bem como, ao se conseguir demonstrar algum índice na empresa, o mesmo é bastante questionado pelo alto escalão por, normalmente, não ter métricas fundamentadas. Neste contexto, a pesquisa de Muthukrishnan e Palaniappan (2016) visa a identificação de elementos de segurança de qualidade para determinar as métricas de segurança operacional. Através de um scorecard, o modelo classifica a situação da empresa em cinco índices de maturidade (1 a 5) ordenados em três níveis de maturidades (Métricas Infantis, Métricas em Evolução e Métricas Amadurecidas). Os dois primeiros índices estão no nível de maturidade de métricas infantis, os Índices 3 e 4 se encaixam no nível de métricas em evolução e, por fim, o Índice 5 representa o último nível, métricas amadurecidas.

Neste contexto, Muthukrishnan e Palaniappan (2016) utilizam as seguintes métricas operacionais:

- Gerenciamento de Patch;
- Gerenciamento de Vulnerabilidades;
- Métricas Financeiras;
- Segurança de Aplicativos;
- Gestão da Mudança;
- Gerenciamento de Configurações;
- Gerenciamento de Incidentes.

O estudo de Gomes et al. (2016) cria um método para mensurar a maturidade da empresa e do gestor de TIC embasado no ITIL através de questionários. Dois tipos de questionários foram utilizados, um tipo para os colaboradores (analisando três dimensões: pessoas, processos e tecnologias) e outro para os gerentes (analisando outras três dimensões: visão e orientação, processos e cultura). O resultado encontrado foi que algumas empresas não tem nível de maturidade de gerência necessário para desempenhar a governança de TIC na empresa. Composição semelhante, por também ser apoiado no ITIL, desta vez visando aferir a maturidade da segurança da informação, é exposta por Park et al. (2008). Neste trabalho um conjunto de entrevistas são realizadas com pessoas que desempenham cargos pré-selecionados visando avaliar a segurança da informação através de nove domínios e 63 itens.

Prado et al. (2016) descrevem a implantação do framework COBIT em uma organização privada no setor de saúde na cidade de São Paulo, SP. Nesta aplicação, Prado et al. (2016) apontam alguns elementos facilitadores e outros inibidores ou dificultadores na aplicação do COBIT. Dentre os inibidores tem-se: a não adaptação ou falta de postura proativa dos colaboradores para as novas rotinas e mudanças propostas pelo COBIT; e a dificuldade na mudança organizacional e cultural, visto que transformar uma organização e seus colaboradores não é uma tarefa fácil, demanda tempo e perseverança para que todos entendam a necessidade e a importância da mudança, percebendo assim os benefícios. Já como facilitadores, Prado et al. (2016) inserem: o apoio da direção da empresa e do diretor de TIC como primordiais; a revisão dos processos de implantação atuais e a criação de uma gerência de mudança para avaliar os impactos das mudanças e uma gerência de configuração para melhor controle dos ativos de TIC; definição de acordo de níveis de serviço junto às áreas usuárias, definindo tempo de indisponibilidade dos sistemas ou processos a serem alterados. Entre os principais pontos de correlação do trabalho de Prado et al. (2016) com o presente estudo está a proposta de aplicação de apenas parte dos complexos modelos atuais, no caso de Prado et al. (2016) o COBIT, visão corroborada por Silva Neto, Alencar e Queiroz (2015) e uma das etapas propostas neste estudo.

Carcary et al. (2016) apresentam um framework para governança e gestão da segurança da informação. A estrutura de maturidade e capacidade apresentada ajuda as organizações a avaliar seu estado de maturidade e identificar áreas problemáticas. Aborda os aspectos técnicos, processuais e humanos da segurança da informação e fornece diretrizes para a implementação dos processos de governança e gerenciamento da segurança da informação na organização. Foi concebido após análise e suporte de especialistas, análise da literatura e documentos da área como os da família do COBIT, The Open Group, ISO/IEC 27.002, entre outros. O framework classifica a governança e gestão da segurança da informação em 6 categorias: governança, segurança técnica, gerenciamento dos recursos de segurança, controle dos riscos de segurança, administração dos dados de segurança e gestão da continuidade do negócio. Essas categorias são decompostas em 22 blocos de construção de capacidade e cada bloco de capacidade é analisado e categorizado em 5 níveis de maturidade, são eles: inicial, básico, intermediário, avançado e otimizado. Salienta-se que todos as seis categorias e os 22 blocos de capacidade são fixos e que não existe hierarquia ou priorização entre os mesmos.

O trabalho de Menezes et al. (2017) apresentou a metodologia PESEG, que é a adaptação da metodologia de Planejamento Estratégico de TIC (PETIC), incorporando a este artefato requisitos de segurança da informação baseados nas normas ISO/IEC 27.001, 27.002:2013 e 27.005. A metodologia criada auxilia no planejamento estratégico de segurança e afere a maturidade da segurança da informação através de quatro níveis: 0 - informal, 1 - mínimo, 2 - seguro, 3 - satisfatório e 4 - estado ideal. Sendo aplicada através de questionário, a metodologia PESEG foi testada em dois estudos de caso em empresas distintas.

Silva e Barros (2017) apresentam um modelo de Maturidade de Segurança da Informação baseado na norma ISO/IEC 27.001. Tendo por objetivo auxiliar as empresas de software a avaliarem sua situação com relação à segurança da informação. Os autores adaptaram os 114 controles da ISO/IEC em 35 itens que são analisados através de questionário. O modelo proposto é composto por cinco níveis de maturidade (Ad Hoc, Gerenciado, Definido, Gerenciado Quantitativamente e Otimizado) e foi avaliado por especialistas e, posteriormente, por empresas. De acordo com a soma das pontuações obtidas em cada uma das 35 perguntas do questionário as empresas são categorizadas em determinado nível de maturidade.

Por fim, ressalta-se a pesquisa de Proença e Borbinha (2018) que também criou um modelo de maturidade para segurança da informação. O modelo criado adota elementos estruturais, domínios e funções da melhor prática na ISO/IEC 27.001, tendo cinco níveis de maturidade: Inicial, Planejamento, Implementação, Monitoramento e Melhoria. Esses níveis de maturidade são baseados no ciclo PDCA usado dentro da ISO/IEC 27.001. Sendo baseado em um mapeamento para os controles da ISO/IEC 27.001, facilitando a compreensão para os usuários já acostumados com a norma. No modelo Proença e Borbinha

(2018) o nível inicial não tem critérios. O nível de planejamento tem dez critérios. O nível de Implementação tem oito critérios. O nível de Monitoramento tem dez critérios. E, por fim, o nível de Melhoria tem quatro critérios. Cada critério utilizado é correlacionado com um controle da ISO/IEC 27.001. Dando um nível de maturidade geral para a organização. O Modelo foi aplicado em cinco organizações como forma de avaliação.

Diante do exposto, percebe-se diversas iniciativas para se conseguir mensurar a maturidade na área de segurança da informação, sendo, de certa forma, trabalhos correlatos à presente pesquisa. Grande parte desses trabalhos utilizam, de forma estática, os controles da ISO/IEC 27.001 e 27.002 ou outro arcabouço já consolidado no mercado, de forma completa ou uma lista de itens para representá-los. Não existindo diferença de peso ou valor entre os controles escolhidos, ou seja, todos os controles selecionados são tratados com a mesma importância para aferir a maturidade da segurança da informação.

Utilizando-os como base, o presente trabalho pode ser visto como uma evolução dos modelos mencionados, se diferenciando, principalmente, por:

- Propor não apenas um modelo para mensuração, mas, também, um guia para implantação da segurança da informação através da priorização dos controles;
- Não trabalhar com uma base estática de controles, visto que, por mais que se comprove que seja a ideal neste momento, não se tem a mesma garantia que será a recomendada no futuro. Para suprir esta possível deficiência, a presente estratégia prioriza os controles de acordo com a importância apontada pelas empresas, ou seja, sendo possível atualizar a base de resposta e, consequentemente, a ordenação e divisão dos controles de acordo com as necessidades atuais do mercado de forma contínua;
- Apresentar uma visão modular que permite utilizar os diversos arcabouços existentes, facilitando sua implantação e utilização pelas empresas.

Tais características conferem a originalidade do trabalho ao se comparar com os demais encontrados na literatura.

3.6 Síntese do Capítulo

O presente capítulo tentou abordar as principais áreas e conceitos da segurança da informação inerentes ao estudo. Como um funil, iniciou-se detalhando temas essenciais para a segurança da informação (trinca essencial, evolução da segurança da informação e, por fim, princípios da segurança da informação), passou para a área de governança (de TIC, ágil e de segurança da informação), posteriormente tratou a área de Maturidade (enfatizando o COBIT, O-ISM3 e o SSE-CMM). Após a área de Maturidade, foram apresentadas as principais normas ISO/IEC para a área de segurança da informação (em

especial: ISO/IEC 27.001, 27.002, 27.005 e 27.014) e finalizando com a discussão sobre um conjunto de trabalhos correlatos ou de importância para a presente pesquisa.

Cabe destacar que a divisão de seções dentro do capítulo serviu como forma de organizar o tema pelo autor, mas percebe-se uma intersecção grande entre elas. Por exemplo, o COBIT é tratado nas seções de maturidade e governança. O SSE-CMM está sendo tratado como uma norma ISO, mas também é um modelo de maturidade. A norma ISO/IEC 27.0014 é abordada nas seções de governança e da família ISO 27.000.

Destaca-se, também, a publicação de dois artigos (ALENCAR et al., 2018b; ALENCAR et al., 2018c) como resultado da pesquisa para concepção da fundamentação teórica apresentada neste Capítulo.

Os assuntos, conceitos e trabalhos apresentados até o momento servem não apenas para demonstrar as pesquisas correlatas, mas também para fechar o embasamento teórico necessário para a compreensão da presente investigação, bem como justificar e evidenciar a importância deste trabalho de pesquisa.

Diante do exposto, acredita-se que ficou explícita a necessidade de evolução nas áreas propostas na presente pesquisa e de uma estratégia para transferência e aplicação desse conjunto de conhecimentos para o meio corporativo. Tal estratégia servirá não apenas para mitigar questões pontuais, mas também como forma de prover um ambiente mais seguro, auxiliando na priorização, implementação e avaliação da segurança da informação de forma holística e integrada.

Este Capítulo fecha a etapa inicial desta tese (introdução, método de pesquisa e fundamentação teórica). Nos próximos capítulos, etapa final da tese, serão apresentados os resultados, discussões e considerações.

4 ANÁLISES DESCRITIVA DOS DADOS

Visando compreender melhor e encontrar soluções para o problema exposto, assim como, cumprir os objetivos propostos para este estudo e dispostos no primeiro capítulo, foi realizada uma pesquisa com o intuito de analisar a visão técnica e estratégica da área de segurança da informação nos ambientes corporativos.

Diante disto, este capítulo apresentará a análise dividida por etapas, na mesma sequência apresentada nos questionários (Apêndices B e C). Primeiro, serão apresentadas informações sobre a amostra alcançada (Seção 4.1). Logo após, será exposta a análise descritiva dos ambientes pesquisados (Seção 4.2), abordando a importância da segurança da informação, ferramentas de segurança utilizadas, recursos humanos, estrutura organizacional e demais aspectos da segurança da informação corporativa. Até esta etapa todas as informações que serão apresentadas têm origem no Questionário 1 (Apêndice B) e serão comparadas com algumas outras pesquisas semelhantes, entre elas o trabalho de Alencar (2011). A pesquisa de Alencar (2011) também teve seus resultados divulgados em Alencar, Queiroz e Queiroz (2013a) e Alencar, Queiroz e Queiroz (2013b), sendo, portanto, um comparativo com esses dois trabalhos.

O trabalho de Alencar (2011) trata-se de uma pesquisa de mestrado em Ciência da Computação, na área de Segurança da Informação, cujo objetivo era: "analisar a situação atual da segurança da informação no ambiente corporativo do Recife e cidades circunvizinhas, tratadas no presente trabalho como Grande Recife, através do entendimento dos pontos vulneráveis relativos às ameaças internas" (ALENCAR, 2011, p. 17). O Questionário 1 (Apêndice B) desta tese foi baseado no questionário de Alencar (2011), diferenciando apenas as quatro últimas questões que foram adicionadas para esta pesquisa.

Alencar (2011) alcançou uma amostra de 34 empresas e constatou que, de uma forma geral, a segurança da informação tem um baixo nível de maturidade, não está alinhada ao negócio, exerce um papel simplório e visa à proteção para as ameaças externas. Sendo, não apenas um trabalho a se comparar com o presente, como também auxiliou a justificativa e motivação desta pesquisa doutoral.

Vale ressaltar, que o comparativo realizado é apenas dos resultados descobertos nesta pesquisa com os apresentados em pesquisa anteriores. Porém, a inferência acerca das melhorias ou prejuízos ao ambiente corporativo, além de outras generalizações não serão possíveis devido à diferença de amostras, região, período da pesquisa e aspectos metodológicos.

Continuando a análise, a Seção 4.3 apresentará a análise dos dados obtidos pelo Questionário 2 (Apêndice C), que aponta a ordenação dos controles da ISO/IEC 27.001 e 27.002. O capítulo é concluído com as considerações expostas na Seção 4.4.

Para um correto entendimento por parte do leitor, é importante ressaltar que todos os participantes desta pesquisa são tratados como "empresa". Indiferente de sua classificação, porte ou abrangência. Como já informado no Capítulo 2, referente ao método da pesquisa.

4.1 Amostra Alcançada

A pesquisa foi enviada para 517 empresas, das quais foram obtidas 248 respostas. Destas, 52 foram descartadas por não responderem completamente todas as questões não opcionais ou por conterem respostas visivelmente incoerentes como, por exemplo, afirmar que tem atividade fim na área de TIC e ser do setor primário. 39 respostas também foram descartadas pela configuração ou porte da empresa, visto que não se enquadravam nas características detalhadas, por exemplo não ser da área de TIC ou não ter uma área de TIC, conforme descrição da amostra no capítulo do método da pesquisa.

Desta forma, nesta pesquisa alcançou-se a amostra de 157 questionários válidos e de empresas distintas, acima das 156,25 exigidas para se obter 95,5% de nível de confiança e erro máximo (intervalo de confiança) de 8,0%, conforme descrição da amostra no Capítulo do método da pesquisa.

Todos os entrevistados eram funcionários ou sócios das empresas. Sendo que 59,24% (93 empresas) era o responsável pela área de segurança da informação ou trabalhavam exclusivamente ou prioritariamente com a área de segurança da informação, os demais respondentes eram da área de TIC ou o responsável por ela.

A amostra de empresas alcançadas abrange 94,90% de empresas sediadas no Brasil, atingindo todas as regiões, e 5,10% de empresas sediadas no exterior (Argentina, Estados Unidos, Inglaterra e Portugal). A localização das empresas que compuseram a amostra desta pesquisa é exibida na Figura 11. Sendo considerada a região metropolitana, quando delimitada, das cidades.

A quantidade de funcionários das empresas respondentes varia entre 15 a 12 mil. Enquanto a quantidade de computadores varia entre 17 computadores a 14 mil máquinas. Para um melhor entendimento da amostra pesquisada, tais dados e seu espalhamento são exibidos nos próximos gráficos (Figuras 12, 13 e 14).

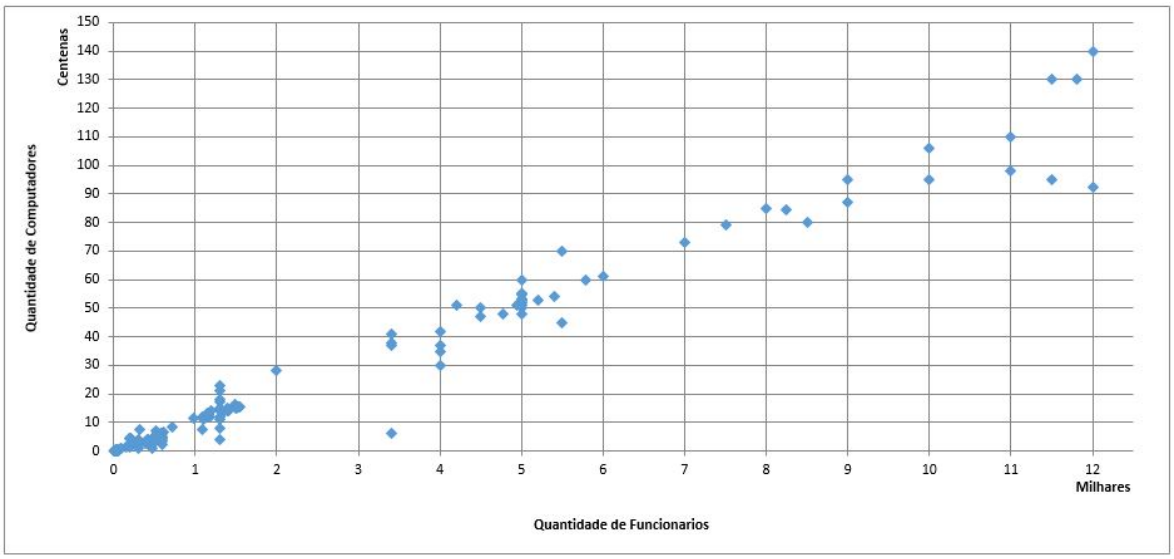
Dentre as empresas pesquisadas, 16,03% (25 empresas) têm a TIC como área fim.

Também foi analisada a atuação, economia e setor de atividade de cada empresa pesquisada. O maior grupo (33,12%) foi de empresas com abrangência de atuação nacional. No que tange a economia e setor de atividade, a maioria se classificou como privada (83,44%) e do setor terciário (82,17%), conforme demonstrado na Figura 15.

Figura 11 – Gráfico da Distribuição das Empresas por Cidade

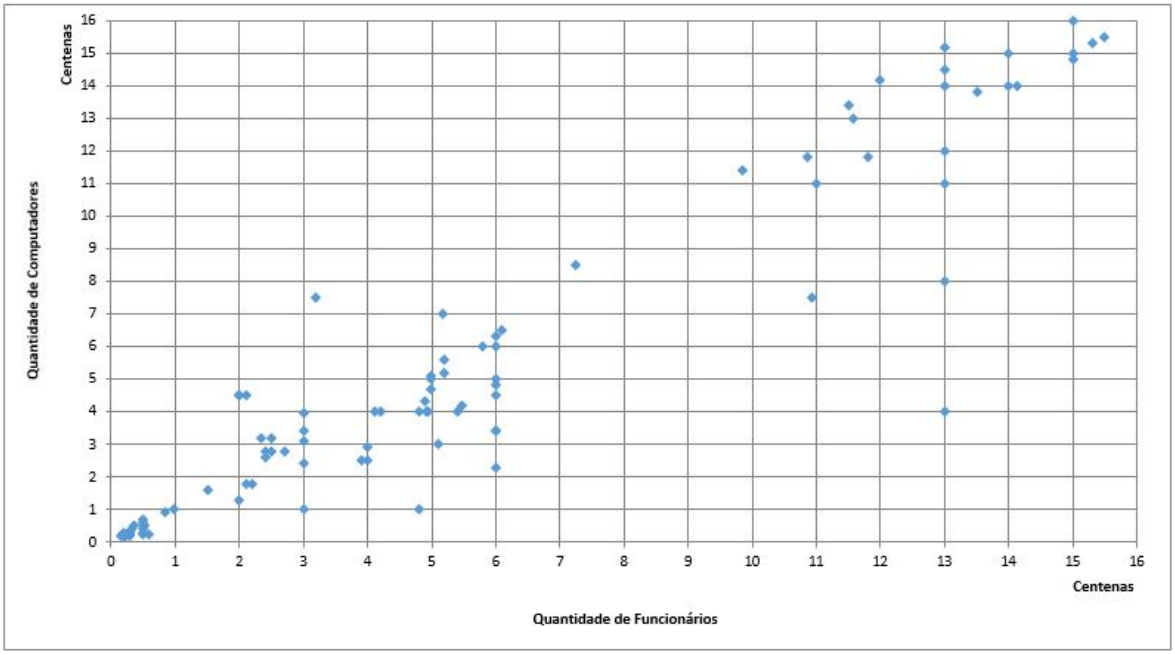
Fonte: autor.

Figura 12 – Gráfico da Dispersão da Amostra



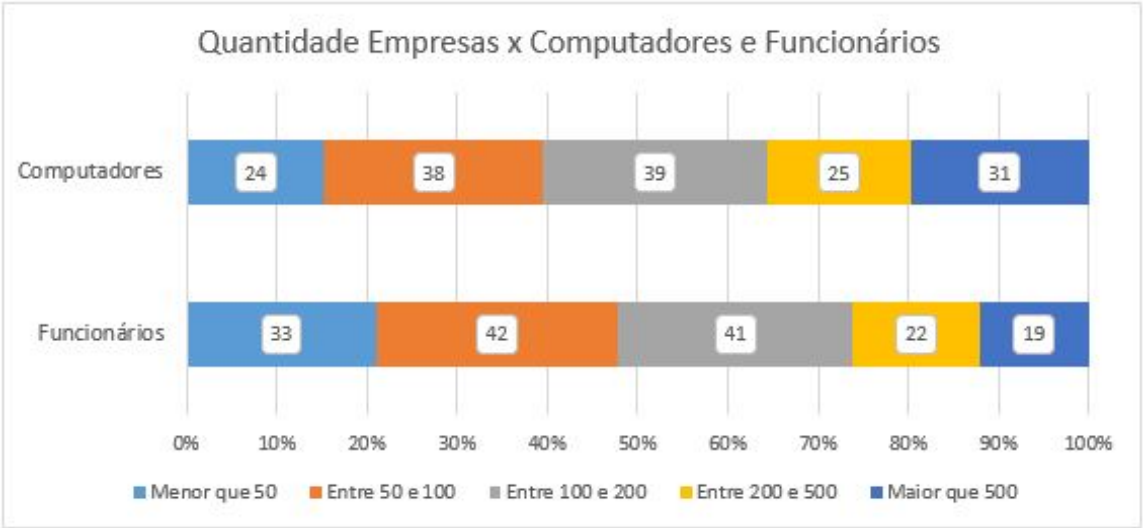
Fonte: autor.

Figura 13 – Gráfico da Dispersão da Amostra - Zoom da área mais populosa



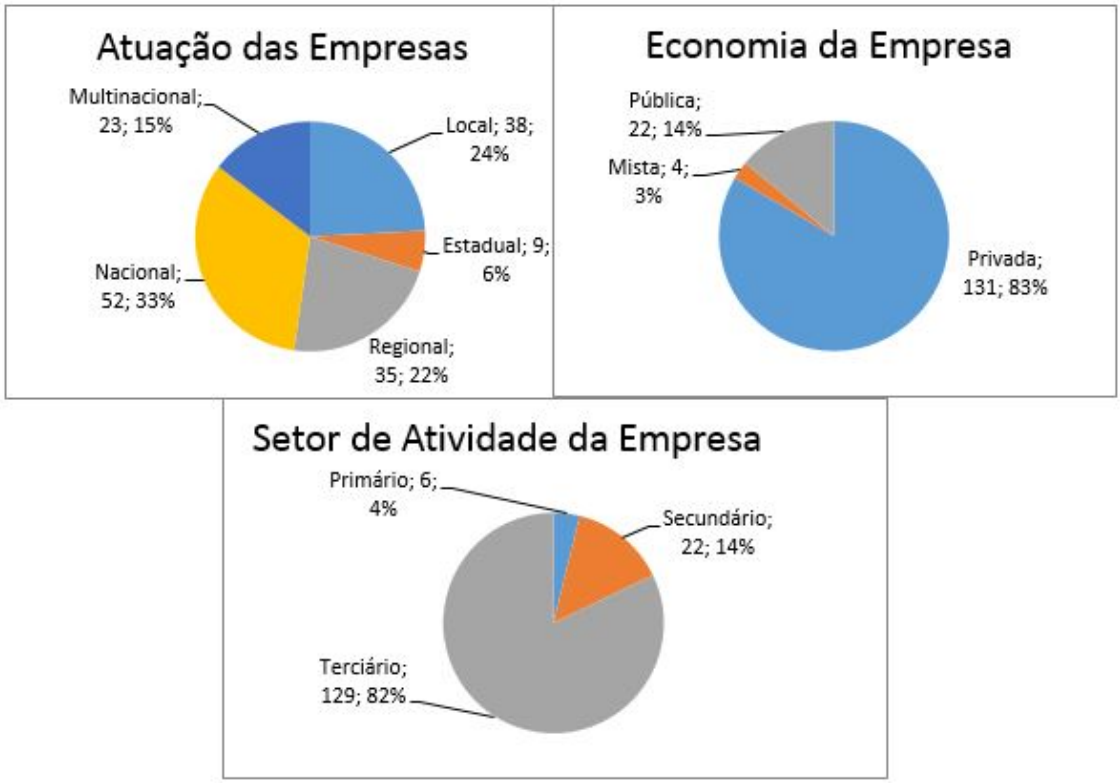
Fonte: autor.

Figura 14 – Gráfico da Proporção da Amostra



Fonte: autor.

Figura 15 – Gráficos da Atuação, Economia e Atividade da Amostra



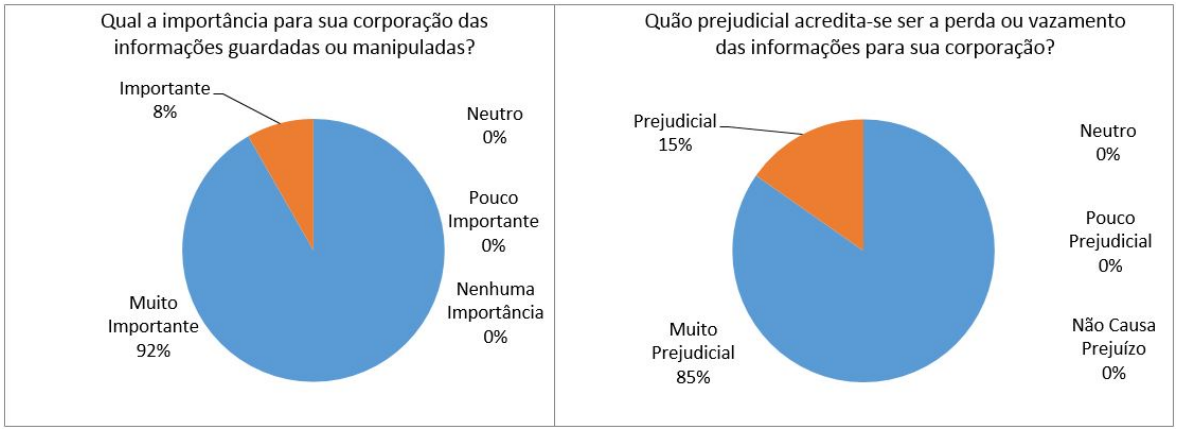
Fonte: autor.

4.2 Análise dos Aspectos de Segurança da Informação

4.2.1 Importância Estratégica da Informação

A pesquisa demonstrou que todas as empresas acreditam que as informações por elas guardadas ou manipuladas são importantes, sendo que 91,72% apontaram como muito importante. Apontando para o mesmo caminho, 84,71% acreditam que a perda ou vazamento das informações são muito prejudiciais para a corporação. Tais informações, que são demonstradas detalhadas na Figura 16, corroboram com o pensamento que já vem sendo afirmado na literatura da área, entre eles: Araújo (2009), Castells (2009), Ramos (2007) e Fontes (2012), no que tange à necessidade das informações pelas corporações na atual era da informação.

Figura 16 – Gráficos da Importância da Informação e Prejudicialidade do Vazamento



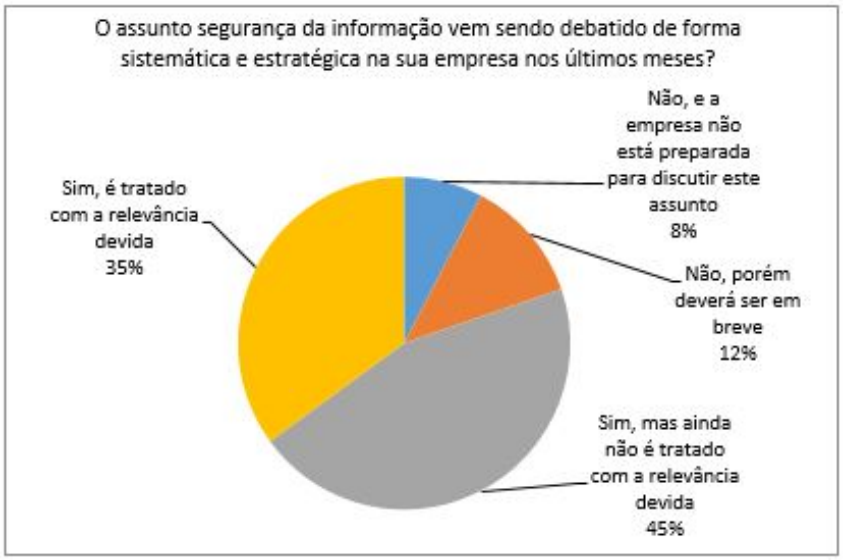
Fonte: autor.

Em Alencar (2011) também houveram respostas apenas nas categorias demonstradas na Figura 16, não havendo variação significante na importância da informação. Percebe-se uma evolução da quantidade de empresas que categorizaram como muito prejudicial o vazamento da informação, 76% (ALENCAR, 2011) para 84,71% na presente pesquisa.

Ao questionar se o assunto segurança da informação vem sendo debatido de forma sistemática e estratégica nas empresas nos últimos meses, a resposta mais mencionada (45,22%) foi de que o tema é tratado, mas ainda sem a devida relevância, enquanto 35,03% apontaram a situação ideal, ou seja, o tema é trado com a devida relevância. Importante apontar que, mesmo nos dias atuais e com a importância da informação apontada pelas empresas, 7,64% das empresas afirmaram que não estão tratando do referido tema nos últimos meses e nem se encontram preparadas para discutir tal assunto (Figura 17).

Uma discrepância significativa foi percebida entre os resultados apontados por Alencar (2011) e a pesquisa atual. Por um lado houve a melhoria da quantidade de empresas na pior situação (Não, e a empresa não está preparada para discutir este assunto), por outro

Figura 17 – Gráfico da Relevância do Assunto na Empresa



Fonte: autor.

lado houve uma redução na quantidade de empresas que apontara a resposta considerada como ideal (Tabela 1).

Tabela 1 – Relevância do Assunto Segurança da Informação na Empresa

Pergunta: O assunto segurança da informação vem sendo debatido de forma sistemática e estratégica na sua empresa nos últimos meses?	**Alencar (2011)**	**Pesquisa Atual**
Não, e a empresa não está preparada para discutir este assunto	9%	7,64%
Não, porém deverá ser em breve	9%	12,10%
Sim, mas ainda não é tratado com a relevância devida	38%	45,22%
Sim, é tratado com a relevância devida	44%	35,03%

No trabalho de Gabbay (2003) 71% dos entrevistados afirmaram que o assunto segurança da informação vem sendo discutido de forma sistemática nos últimos meses, porém a pesquisa tinha apenas a opção de sim ou não. Considerando as respostas demonstradas na Figura 17 apenas como sim ou não, têm-se 80,25% de respostas positivas, índice um pouco melhor que o citado por Gabbay (2003), mas ligeiramente abaixo dos 82% apontados por Alencar (2011).

Ao questionar as empresas sobre a existência de divulgação institucional e frequente sobre a segurança da informação na corporação, 36,94% das empresas responderam de forma positiva. Em sentido contrário das boas práticas relatadas nos capítulos anteriores, grande parte das empresas (63,06%) registrou que não existe divulgação institucional e frequente sobre segurança da informação na empresa.

Este número negativo tem uma representação ainda maior quando se questionou a existência de treinamentos periódicos ou processos de conscientização sobre segurança da

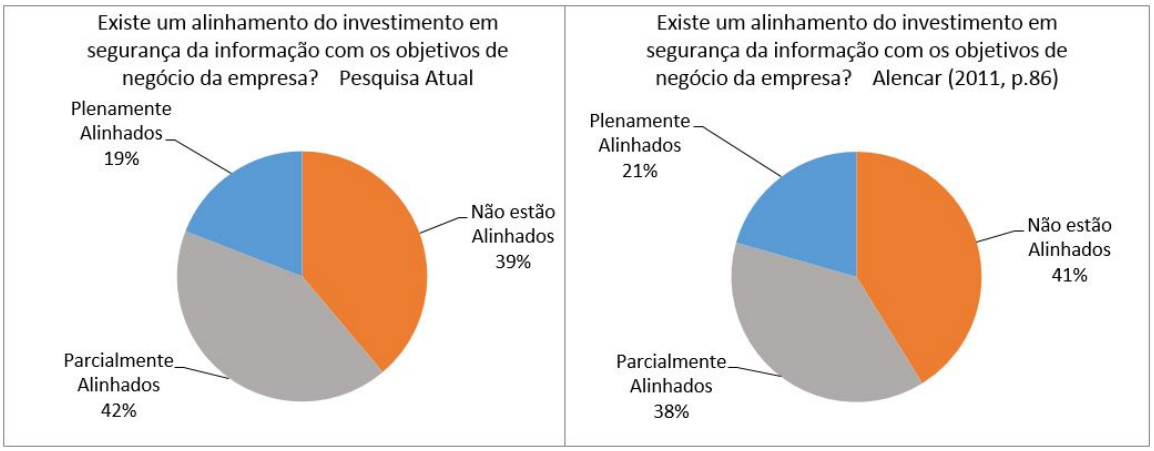
informação para os funcionários. Nesta opção, apenas 16,56% responderam positivamente.

Ciente que o ideal para a área de segurança da informação é que exista um processo formal e contínuo de divulgação, conscientização e treinamentos, os resultados apontados registram uma carência grande na área. Porém viu-se um pequeno avanço comparado com os resultados de Alencar (2011) que apontou respostas positivas nos percentuais de 35% e 15%, respectivamente para a existência de divulgação e de treinamentos.

Por fim, neste seção do questionário, foi perguntado sobre o alinhamento dos investimentos da segurança da informação.

Também indo contra o que fala a literatura já citada nas seções anteriores e que norteou o trabalho em sua fundamentação teórica, a pesquisa verificou que apenas 19,11% das empresas pesquisadas têm o investimento em segurança da informação plenamente alinhado com os objetivos de negócio da empresa, o que seria a situação ideal. Em comparação com a pesquisa de Alencar (2011) percebe-se um incremento na quantidade de empresas parcialmente alinhadas e diminuindo a quantidade de empresas nos extremos positivo e negativo (Figura 18).

Figura 18 – Gráficos do Alinhamento do Investimento de Segurança da Informação



Fonte: autor.

Nesta questão também foi possível observar uma discrepância, mostrando um ambiente menos alinhado, dos dados da Modulo (2006) que apresentaram 33% das empresas plenamente alinhadas, 40% parcialmente, 16% pouco e 11% não alinhadas.

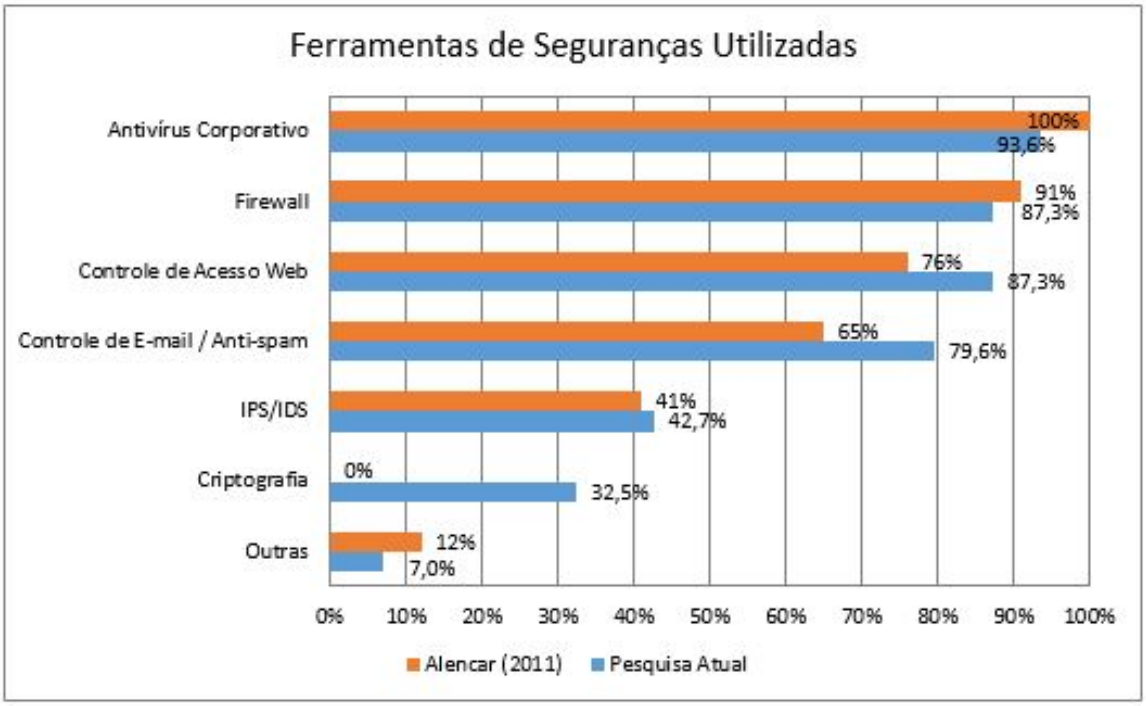
4.2.2 Ferramentas de Segurança da Informação nas Empresas

Com relação as ferramentas de segurança utilizadas pelas empresas, observa-se que os dados da atual pesquisa (com referência em 2017) apresentam melhorias significativas no contexto geral, ao se comprar com os dados de 2010 exposto em Alencar (2011). Havendo um pequeno decréscimo nas ferramentas mais tradicionais (Antivírus e Firewall) e melhorias consideráveis no uso de tecnologias para proteção web, e-mail e de criptografia.

Tais resultados são comparados na Figura 19, sendo exibido a pesquisa atual em azul e os dados de Alencar (2011) em vermelho.

Os itens das duas análises realizadas nesta seção (Figuras 19 e 20) extrapolam os 100% por ser possível a marcação de mais de uma resposta na mesma questão da pesquisa.

Figura 19 – Gráfico da Utilização de Ferramentas de Segurança da Informação



Fonte: autor.

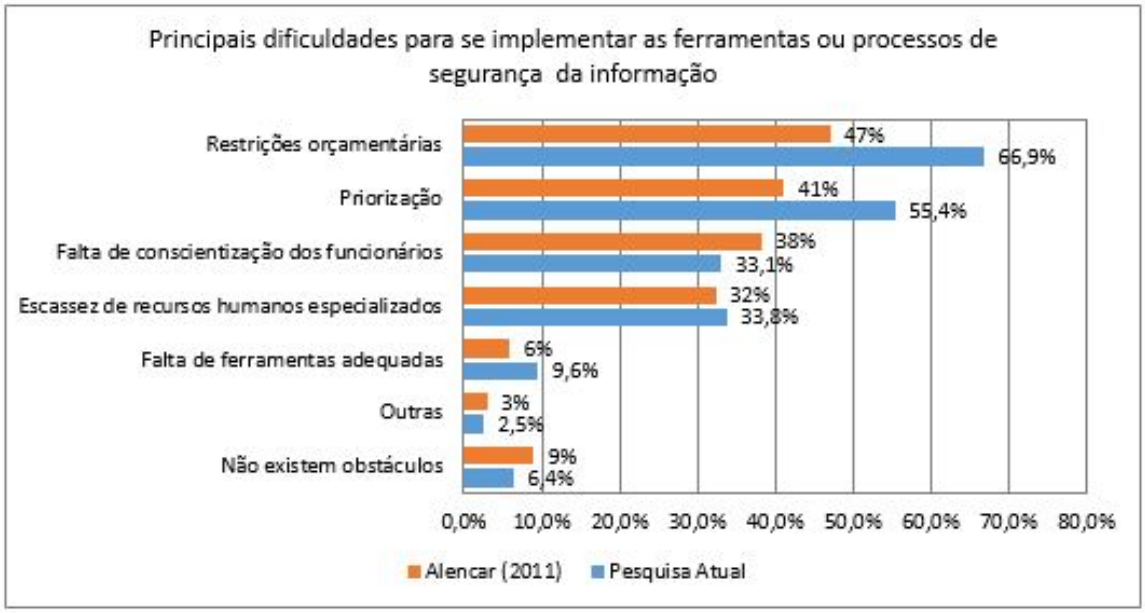
O item criptografia foi o que obteve um maior destaque entre a pesquisa de Alencar (2011) e a presente. Acredita-se que parte das respostas categorizadas como "Outras" em Alencar (2011) envolve a criptografia. Mesmo com essa possível configuração, que aumentaria o índice de 0% exposto na Figura 19, a maior evolução, ao se comparar com a pesquisa atual, continuaria sendo este item.

Algumas tendências do resultado atual podem ser observadas no trabalho de Silva Neto, Alencar e Queiroz (2015). Comparado com Alencar (2011), percebe-se a diminuição do uso de firewalls, aumento no uso de ferramentas anti-spam e aparecimento do uso de criptografia, com 31%. Fatos que corroboram com o estudo atual. Também verificou-se em Silva Neto, Alencar e Queiroz (2015) e na pesquisa atual, se comparadas com a pesquisa de Alencar (2011), uma maior utilização de controles de acesso web e de e-mail. Fatos que já eram esperados e podem ser visto como uma tendência natural, devido à migração contínua que se tem dos serviços para a web.

Ao questionar sobre as principais dificuldades para se implantar as ferramentas de segurança da informação na empresa, percebeu-se semelhanças quanto a ordem das dificuldades entre a pesquisa atual e de Alencar (2011), mas com percentuais bem diferentes,

como pode ser visto no gráfico a seguir (Figura 20). Tais áreas levantadas seguem um mesmo direcionamento dos resultados apresentados por Fazenda e Fagundes (2015).

Figura 20 – Gráfico das Principais Dificuldades para Implantação da Segurança da Informação



Fonte: autor.

O aumento de respostas apontando "Restrições orçamentárias" pode ser oriundo da diferença do estado econômico da nação em 2010 e 2017, período da pesquisa de Alencar (2011) e a atual. A mesma situação, e possivelmente a carência de recursos, pode ter orientado o aumento de respostas "Priorização". Em situações mais críticas de recursos, a área de segurança pode não ter recebido os mesmos investimentos do que áreas que possam aumentar os lucros, como marketing, por exemplo.

Outra possível explicação pode ser a falta de capacidade dos responsáveis pela área de segurança e pela área de TIC de debater e convencer os responsáveis pelos investimentos. Tal fato é corroborado pelo dados de alinhamento apresentados na Figura 18.

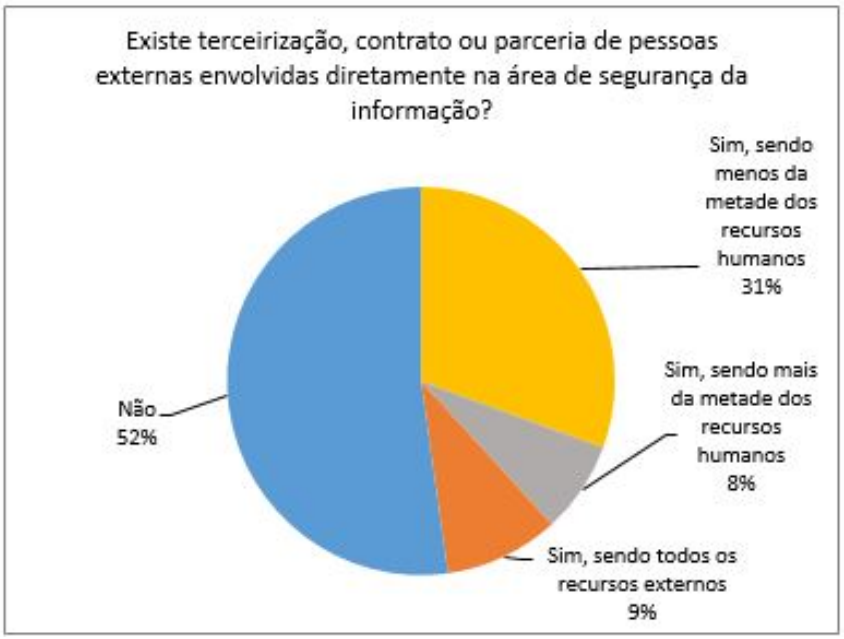
Porém, ambas as situações (crise nacional ou falta de convencimento) são apenas hipóteses e carecem de estudos para comprovação.

4.2.3 Recursos Humanos e Estrutura Organizacional

Analisando a organização setorial da segurança da informação e dos recursos humanos que tratam a mesma, a pesquisa revelou que em 50,95% das empresas existe uma área, departamento, unidade ou equipe formal dedicada à segurança da informação. Não havendo diferenças significativas para os 50% apontados por Alencar (2011). Porém, percebe-se uma melhoria dos dados mostrados pela Modulo (2006), onde 43% das companhias tinham um departamento de segurança da informação estruturado.

Também foi visto que 47,77% das empresas contam com pessoas externas envolvidas diretamente na área de segurança da informação, tais pessoas são oriundas de terceirização, contrato ou parcerias (Figura 21). Ponto com leve diminuição se comprado com Alencar (2011) (50%). Porém mantém uma tendência de queda, ao comparar com as respostas mais antigas da Modulo (2006), que apontavam 75% de algum tipo de terceirização em alguma atividade relacionada à segurança da Informação.

Figura 21 – Gráfico do Uso de Serviços Terceirizados na Segurança da Informação



Fonte: autor.

Os 75% apresentados em 2006 (MODULO, 2006), 50% em 2010 (ALENCAR, 2011) e 47,77% na pesquisa atual, apontam para uma diminuição nos últimos anos (2006-2017), nesta área, do serviço de terceirização. Tal fato pode ser resultado de uma melhoria da maturidade da área, dos profissionais e/ou das ferramentas, métodos e procedimentos. Porém, assim como detalhado em outros fatores, tal apontamento é apenas uma possível hipótese.

A área de segurança da informação é visto como crítica e sua terceirização pode gerar sérios problemas como relata Cezar, Cavusoglu e Raghunathan (2013) como, por exemplo, o conhecimento de senhas, acesso às configurações dos dispositivos de segurança e acesso à rede interna.

Foi possível verificar que apenas 21,65% dos responsáveis pela segurança da informação trabalham exclusivamente na área, novamente sem diferença do percentual apresentado por Alencar (2011) (21%). Sabendo que 50,95% das empresas alegaram ter um setor formal dedicado à segurança da informação, conforme citado no início desta seção, verifica-se que pouco mais de 40% dos responsáveis por esse setor trabalham exclusivamente para esta função. Ou seja, exclusivamente para prover a segurança da informação corporativa.

A pesquisa retratou que em 49,68% dos casos a equipe responsável pela segurança da informação tiveram capacitação ou formação relacionada aos conceitos gerais da área de segurança da informação (conceitos, políticas, normas, auditoria, criptografia, malwares) no último ano e em 49,04% das empresas tiveram capacitação ou formação nas ferramentas de segurança da informação utilizadas na empresa, também no último ano. Números bem abaixo dos apresentados em Alencar (2011), com 59% e 56%, respectivamente.

Percebeu-se também que 40,13% responderam que não tiveram capacitação ou formação no último ano em nenhuma área de segurança da informação pesquisada. Este número tinha sido de 29% em Alencar (2011).

Além dos números apontados serem mais baixos do que os de Alencar (2011), são bem mais baixos do que os apresentados pela pesquisa da Modulo (2006), que trazia 50% dos profissionais que lidam com segurança da informação parcialmente capacitados, 18% plenamente, 18% pouco capacitados e 14% sem capacitação ou treinamento. Assim como pelos dados exibidos por Gabbay (2003).

Ao solicitar aos participantes que colocassem uma nota entre 0 e 10 para mensurar o conhecimento da equipe responsável pela segurança da informação, obteve-se uma média de 6,3 (mediana 6) para os conhecimentos gerais em segurança da informação e média 6,7 (mediana 7) para o conhecimento da equipe nas ferramentas da área utilizadas. Em Alencar (2011) os resultados foram melhores, respectivamente, 6,9 e 7,3.

Ao analisar separadamente os grupos que afirmaram ter tido capacitação ou formação nas duas áreas em questão, a média sobe para 7,8 (mediana 8) nos conhecimentos gerais e média 8,1 (mediana 8) no conhecimento das ferramentas de segurança utilizadas. Resultados abaixo dos apresentados por Alencar (2011) para este mesmo grupo, 8,5 (mediana 8) e 8,7 (mediana 9), respectivamente.

No lado oposto, o grupo que respondeu que não teve capacitação ou formação em nenhuma das áreas, a média diminui para 5,1 (mediana 5) para os conhecimentos gerais e, para o conhecimento nas ferramentas de SI, média 5,9 (mediana 6). Resultados acima dos apresentados por Alencar (2011) para este mesmo grupo, 4,6 (mediana 5) e 5,3 (mediana 5), respectivamente.

Tal fato precisaria de maiores estudos para se comprovar o motivo da alteração dos resultados. Visto que, por ter uma amostra percentualmente menor de empresas que tiveram capacitação, seria normal ter uma nota média do conhecimento da equipe menor do que o número apontado por Alencar (2011). Fato que ocorreu.

Porém, ao analisar o grupo que teve capacitação nas duas áreas (conceitos gerais e ferramentas) a nota foi inferior aos dados de Alencar (2011). Por outro lado, o grupo que não teve capacitação em nenhuma das áreas teve nota superior aos dados de Alencar (2011).

Neste ponto pode ser colocada como hipótese a melhoria da formação e conhecimento dos profissionais na área de segurança. O que coloca a nota mínima (representada por

aqueles que não tiveram treinamentos) acima dos dados de 2010 de Alencar (2011). Por outro lado, o conhecimento dos mesmos, junto à complexidade da área pode fazer com que se tenha maior noção dos problemas e desafios da área, fazendo com que, mesmo os que receberam treinamento, não se sintam confortáveis para colocar uma nota maior ao mensurar seu conhecimento.

Finalizando a seção de recursos humanos do questionário, foi solicitado aos respondentes que marcassem todos os tipos de análises ou procedimentos utilizados e eliminatórios na seleção de colaboradores (funcionários, servidores, terceirizados, estagiários). Percebeu-se que, atualmente, as etapas mais tradicionais (exame médico, entrevista e análise de currículo) estão sendo realizadas, quase semelhantemente, na grande maioria das empresas (Tabela 2).

Tabela 2 – Análises e Procedimentos Utilizados na Seleção de Profissionais

Análise ou Procedimento	**Alencar (2011)**	**Pesquisa Atual**
Exame médico	85%	93,63%
Entrevista	71%	92,35%
Análise de currículo e documentos	71%	91,72%
Avaliação da conduta ética e moral	12%	19,11%
Antecedentes criminais	9%	7,64%
Exame psicotécnico	9%	7,0%

Porém, mesmo com o aumento de empresas que avaliam a conduta ética e moral, ainda são poucas as empresas que realizam análise dos antecedentes criminais e exame psicotécnico, ficando abaixo dos dados de Alencar (2011). As três análises aqui citadas poderiam detectar possíveis comportamentos ou características que indiquem se o profissional tem ou não o perfil desejado, como aborda o US CERT Program (2010) trazendo que 61% das empresas americanas pesquisadas afirmam verificar os antecedentes dos empregados ou contratados como uma forma de segurança da informação, inserindo estas análises como boas práticas.

4.2.4 Segurança da Informação Corporativa

Esta seção do questionário inicia perguntando sobre o que se espera dos problemas e ameaças relativos à segurança da informação nos próximos meses. Tal questionamento foi realizado quanto ao ambiente interno e ao externo (global) da empresa. Tais respostas são exibidas na Tabela 3.

Tal expectativa de aumento, principalmente no ambiente externo, corrobora com as tendências retratadas neste trabalho e com os dados da Modulo (2006) e do US CERT Program (2010), porém vai contra as expectativas dos entrevistados por Gabbay (2003), onde a maioria acreditava na diminuição dos problemas de segurança da informação.

Mesmo diminuindo, ao se comparar Alencar (2011) e a presente pesquisa, ainda é visível a dissensão na expectativa relativa ao aumento de problemas de segurança da in-

Tabela 3 – Expectativa de Problemas e Ameaças Relativos à Segurança da Informação

	Alencar (2011)		**Pesquisa Atual**	
	Amb. Interno	Amb. Externo	Amb. Interno	Amb. Externo
Aumentar os Problemas	41%	76%	59,87%	87,26%
Permanecer	32%	12%	32,48%	9,55%
Diminuir os Problemas	27%	12%	7,64%	3,18%

formação no ambiente interno e no ambiente global (externo). O que corrobora com o pensamento de Schneier (2007) que aborda a visão divergente das pessoas entre a segurança interna e externa, temendo, principalmente, o que é externo. Este fato é apontado por Schneier (2007) como sendo apenas uma crença social e sem fundamentos, visto que grande parte dos ataques, nas mais diversas áreas, tem participação de pessoas próximas, tais como funcionários, parentes, etc, ou seja, com grandes chances de ocorrer no ambiente interno.

A segurança da informação corporativa pode ser entendida como a união de uma estratégia e de ferramentas específicas que atendam aos anseios corporativos para a implantação e manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança da informação nunca está acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa. Para Alexandria (2009), a definição da política de segurança da informação é o primeiro passo para o reconhecimento da importância da segurança da informação para a organização e para seu tratamento adequado.

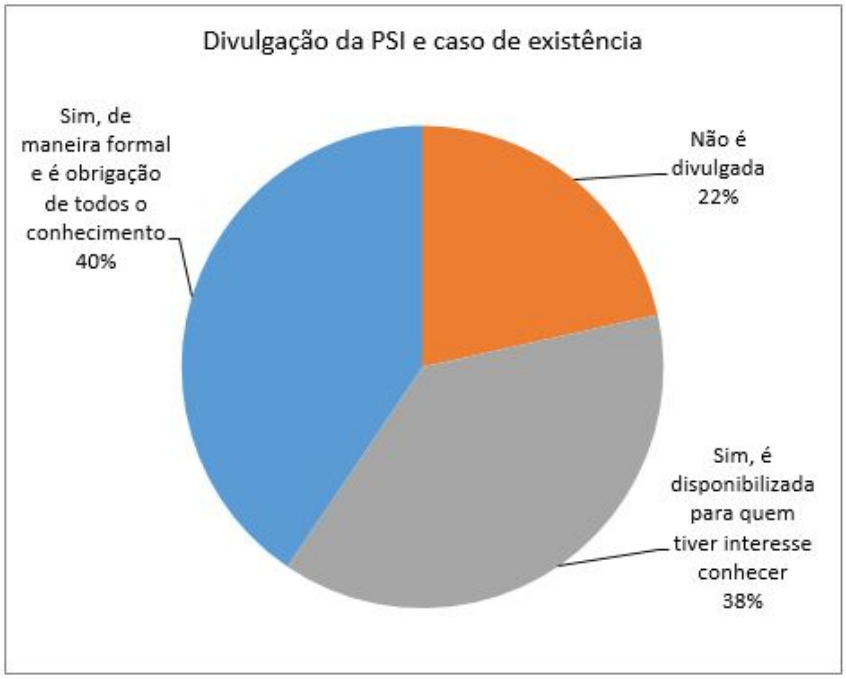
Sabendo da importância da política de segurança da informação para o ambiente tecnológica e informações das empresas, a pesquisa questionou sobre sua implementação. Percebeu-se uma grande melhora nos resultados de Alencar (2011), que apontavam para 50% das empresas que selecionaram uma das duas opções de implantação da PSI (formal ou informalmente), para 79,62%, nos mesmos aspectos, na pesquisa atual (Tabela 4). Porém ainda inferior aos resultados de Gabbay (2003), que apontou 82% das empresas com uma PSI implementada.

Tabela 4 – Implementação da PSI no Ambiente

PSI Implementada	**Alencar (2011)**	**Pesquisa Atual**
Sim, possui uma PSI formal implementada	35%	39,49%
Sim, possui uma PSI informal implementada	15%	40,13%
Não possui uma PSI implementada, mas está em processo de formulação ou implementação	35%	10,83%
Não possui nenhuma PSI nem previsão de implementação	15%	9,55%

Entre as empresas que já adotam uma PSI (formal ou informalmente), 40% afirmaram que existe uma divulgação formal da política e é obrigado o conhecimento por parte dos funcionários (Figura 22), sendo este o melhor caso para a segurança da informação.

Figura 22 – Gráfico da Divulgação da Política de Segurança da Informação



Fonte: autor.

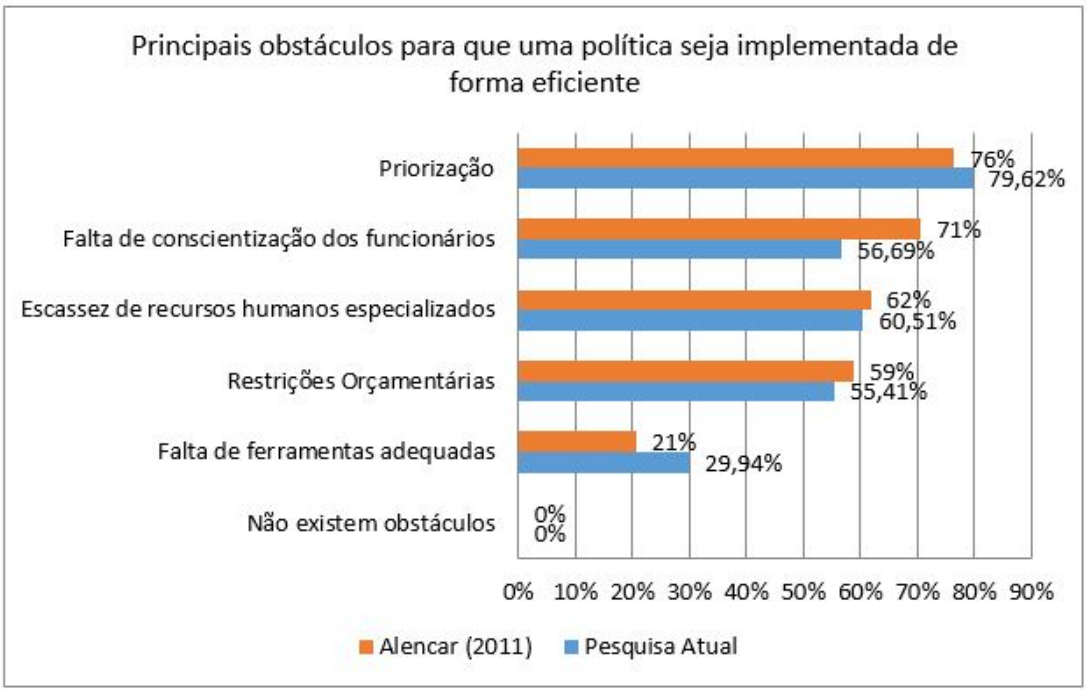
Neste ponto não se viu diferenças significativas ao se comparar com Alencar (2011). Por um lado houve uma melhora nos 24% que não divulgavam a PSI, por outro lado, houve redução de 1% daqueles que estavam na melhor situação (PSI divulgada de maneira formal).

Outro questionamento foi sobre os principais obstáculos citados pelos respondentes para que a PSI fosse implementada de forma eficiente. Analisando a pesquisa atual e a de Alencar (2011), percebe-se diferenças maiores entre as respostas dos itens: "Falta de conscientização dos funcionários" e "Falta de ferramentas". O que, aparentemente, verificou-se foi que a conscientização sobre a importância da PSI melhorou, mas isso não se reflete em priorização e ainda faltam ferramentas adequadas para implantação. Tais resultados são comparados na Figura 23.

Os resultados apontam uma convergência parcial com os resultados explanados por Gabbay (2003), onde as respostas que lideraram foram falta de conscientização dos funcionários (56%), falta de ferramentas adequadas (41%) e escassez de recursos humanos especializados (39%). Também segue um mesmo direcionamento apresentado por Fazenda e Fagundes (2015).

Ao questionar sobre as principais ameaças às informações nas empresas pesquisadas, os três itens mais indicados em Alencar (2011) estão diretamente ligados ao comportamento humano, sendo o primeiro e terceiro itens ligados, diretamente, ao comportamento das pessoas internas à empresa. Na presente pesquisa, ações com ligação aos usuários também se destacaram: Vazamento de Informações, Divulgação indevida de senhas, Uso

Figura 23 – Gráfico dos Principais Obstáculos para Implantação da PSI



Fonte: autor.

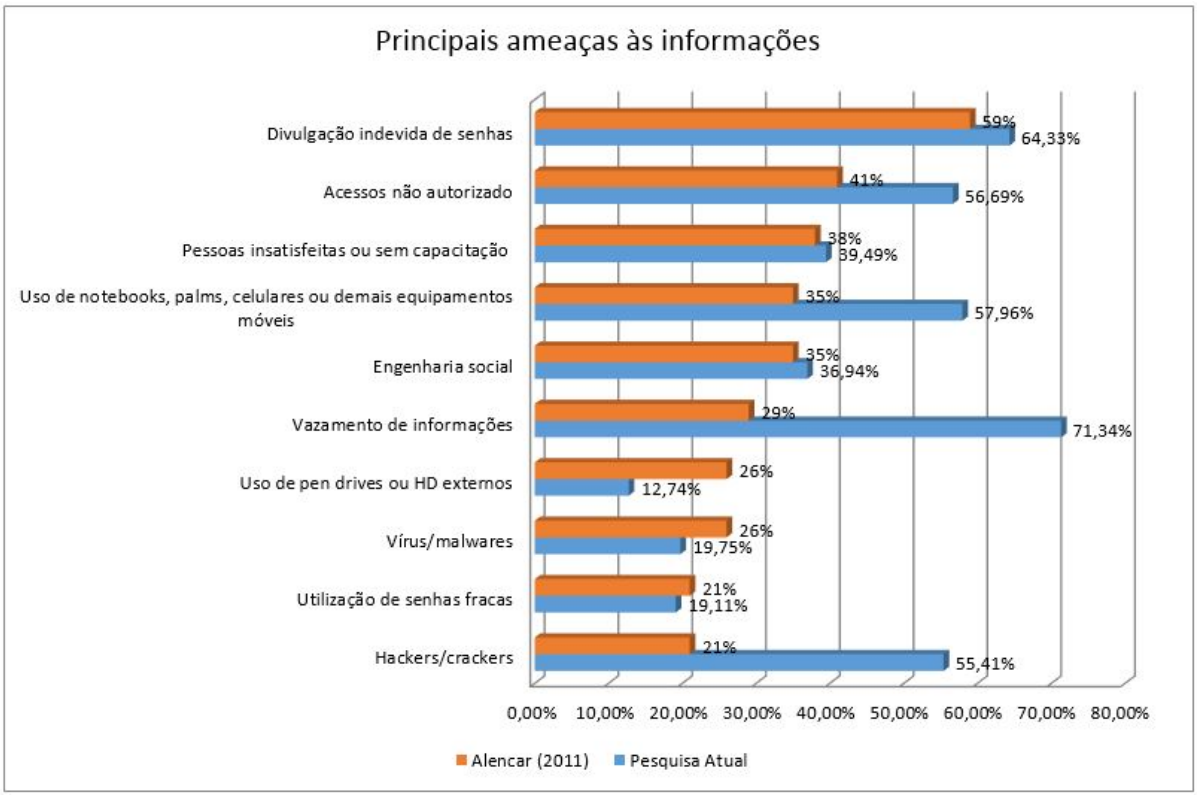
de dispositivos móveis. Além do grande aumento dos Hackers/Crackers como ameaça. Fatos que corroboram com Schneier (2007). Tais resultados são comparados no próximo gráfico (Figura 24).

Tais informações diferentes entre a pesquisa atual, a de Alencar (2011) e as demais pesquisas citadas neste trabalho e por Alencar (2011), mostram a dinamicidade e complexidade da área de segurança da informação e as particularidades de cada ambiente. Porém percebemos o desuso ou controle de algumas áreas, por exemplo, uso de pen drives ou HD externos (provavelmente não se tem o mesmo uso que em 2011 ou as empresas já tem controles para esta área) que podem ter migrados para uso em sistemas de compartilhamento na nuvem (neste caso, poderiam explicar o aumento do item vazamento das informações). Em um caminho oposto, percebeu-se a maior preocupação com os dispositivos móveis, provavelmente impulsionado pelo avanço dos smartphones.

As informações desta pesquisa neste quesito dão uma visão diferente das publicadas anteriormente Gabbay (2003), Modulo (2006), US CERT Program (2010) e Alencar (2011), que também não apontavam, entre si, correlações significantes. O que mostra a dinamicidade da área de segurança da informação e as particularidades de cada ambiente e período.

Ao requerer que selecionassem todos os métodos utilizados para segurança e controle de acesso aos meios tecnológicos e informações não públicas, 100% das empresas assinalaram o uso do método de usuário e senha, mesmo resultado encontrado em Alencar (2011). Mas alguns dados apresentam resultados melhores, como o uso de biometria (3,18%) e

Figura 24 – Gráfico das Principais Ameaças às Informações das Empresas



Fonte: autor.

certificado digital (23,57%), antes apontados por Alencar (2011), como 0% e 3%, respectivamente.

Mesmo o usuário e senha sendo um método tecnologicamente superado, ainda é o mais comum nas empresas, como a pesquisa comprovou, corroborando o estudo de Shay et al. (2010), porém a sua administração ainda não segue as melhores práticas. Ao pesquisar sobre a existência de procedimentos para checagem de privilégios dos usuários de redes, assim como procedimentos para bloquear a conta ou os privilégios imediatamente após não haver mais a necessidade, 29,30% afirmaram não existir tais recursos na sua empresa, 7,64% marcaram a opção indeciso e 63,06% concordaram com a existência (melhor situação). Nos resultados de Alencar (2011), tinha-se 32%, 12% e 56% respectivamente. Uma melhora significativa, mas longe de uma adesão de tal controle em massa, o que é considerado ideal para a área.

Percebeu-se também melhorias na adesão de senhas fortes, sem repetição e trocas periódicas. A pesquisa de Alencar (2011) apontou que 65% das empresas utilizavam deste recurso. Na pesquisa atual o número saltou para 73,25% das empresas que utilizam o recurso. 22,29% afirmaram não utilizar e 4,46% não souberam responder e marcaram a opção indeciso.

Já no panorama americano mostrado pelo US CERT Program (2010) 80% das empresas afirmam utilizar uma política de gerenciamento de usuário e senha que envolvem os

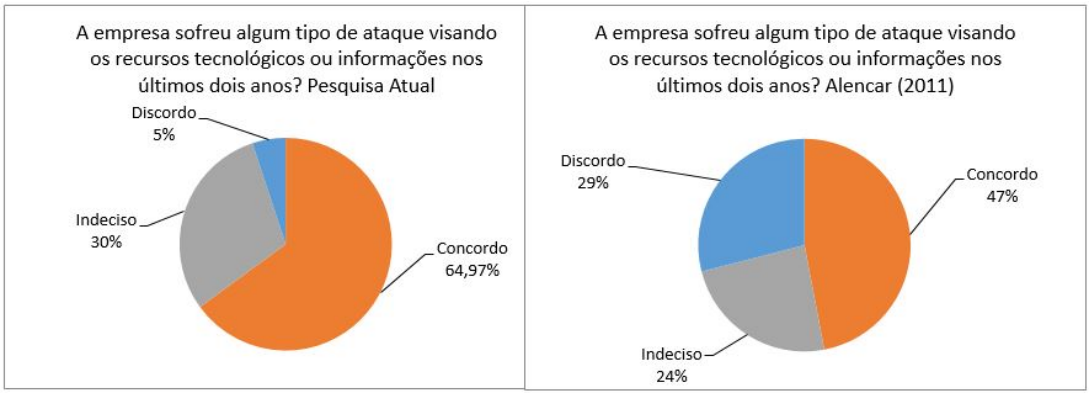
últimos dois itens debatidos.

Verificou-se também que, em 65,60% das empresas pesquisadas, não existe política de classificação e proteção às informações. Com relação à existência de níveis de controles ou políticas diferenciadas para acessar informações mais críticas, 44,59% da amostra afirmou não haver. Ambos os itens não mostraram alterações significativas aos 68% e 47%, respectivamente, apresentados por Alencar (2011).

Outro ponto levantado é que a ação de concordar, ao entrar na empresa, com algum tipo de termo de compromisso ou documento relativo à confidencialidade das senhas e informações internas ainda não é uma prática realmente difundida, sendo realizada por 40,13% das empresas, ante 50% de Alencar (2011) e 61% no mercado americano (US CERT PROGRAM, 2010).

Sabendo do valor que as informações têm no mercado atual, do aumento da capacidade de exploração de vulnerabilidades por parte dos atacantes e tendo como alvo o ambiente com vulnerabilidades, como esta e outras pesquisas vêm demonstrando, é de se esperar que as empresas venham sofrendo ataques ao seu ambiente computacional, fato que foi comprovado com o aumento dos dados da pesquisa atual (Figura 25) comparada com a de Alencar (2011) e com o trabalho de Gabbay (2003) que apontou: 45% das empresas sofreram ataques, 33% não sofreram e 21% não souberam responder.

Figura 25 – Gráfico dos Ataques Sofridos



Fonte: autor.

Dentre as empresas que afirmaram ter sofrido algum tipo de ataque (102) questionou-se sobre a descoberta da vulnerabilidade explorada, bem como da descoberta da origem do ataque. Percebeu-se uma diminuição de 7,84% daquelas que conseguiram descobrir a vulnerabilidade explorada em comparação com a pesquisa de Alencar (2011), enquanto a quantidade de empresas que conseguiram descobrir a origem do ataque obteve resultados semelhantes (Tabela 5).

Ressalta-se também o aumento significativo, nas duas situações, das empresas que responderam que não conseguiram detectar.

Tabela 5 – Descobertas de Vulnerabilidades Exploradas e Origem dos Ataques

	Alencar (2011)	**Pesquisa Atual**
Descobriram as vulnerabilidades exploradas	50%	42,16%
Não conseguiram detectar	29%	50,98%
Não souberam informar	21%	7,84%
Descobriram a origem	34%	35,29%
Não conseguiram detectar	33%	51,96%
Não souberam informar	33%	12,75%

Uma análise superficial pode apontar para o aumento da quantidade de ataques nos anos de 2003 e 2010 para o atual, bem como da maior capacidade de percepção dos mesmos. Não se pode desprezar essas possibilidades. Porém, mais uma vez, deve-se considerar, também, outras hipóteses como a diferença entre as amostras e o avanço das tecnologias de detecção e auditoria. Por outro lado, as empresas podem não ter respondido "corretamente" estas perguntas, nesta e nas demais pesquisa, como forma de proteção, não se expondo como uma empresa vulnerável. Tanto ficando indecisa ou afirmando que não recebeu algum ataque (não apontando uma possível fragilidade), quanto apontando que conseguiu detectar a vulnerabilidade e a origem (como demonstração da qualidade da área de segurança da informação). Por fim, também é possível que as empresas que responderam não ter sofrido ataque, tenham sido atacadas e não conseguiram perceber. Porém, seria necessário um estudo mais aprofundado para avaliar tais hipóteses.

Continuando com o mesmo grupo de empresas que afirmaram ter sofrido algum tipo de ataque, foi questionado sobre as perdas sofridas. Percebeu-se o aumento das empresas que apontaram perdas operacionais e exposição de informações confidenciais ao se comparar com Alencar (2011). Fato que se alinhou com a pesquisa do US CERT Program (2010), que também apontou a perda operacional em primeiro lugar, seguida pelos prejuízos financeiros, danos à reputação e roubo de dados sensíveis.

Interessante destacar que na pesquisa de Alencar (2011) 13% afirmaram não ter havido perdas. Já na pesquisa atual, esse item apareceu zerado (Figura 26).

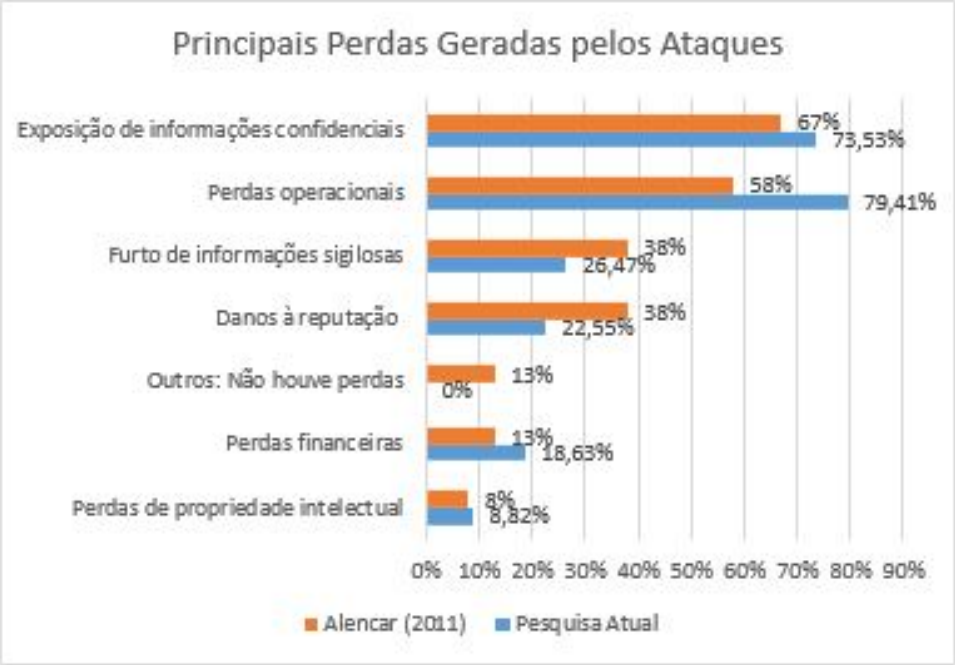
Porém, mesmo sabendo quais foram as possíveis perdas, 79,41% citaram que não foi possível mensurá-las. Índice superior aos 75% apontados por Alencar (2011) e 2,4 vezes superior aos 33% apresentados na pesquisa da Modulo (2006).

Como último questionamento as empresas que sofreram algum tipo de ataque nos últimos dois anos, questionou-se sobre a origem das pessoas envolvidas. O comparativo com a pesquisa de Alencar (2011) pode ser visto na Figura 27.

Percebe-se o aumento na quantidade de empresas que não conseguiram detectar. Uma hipótese para tal caso é o avanço das tecnologias de ataque, aperfeiçoando-se na capacidade de diminuir a rastreabilidade.

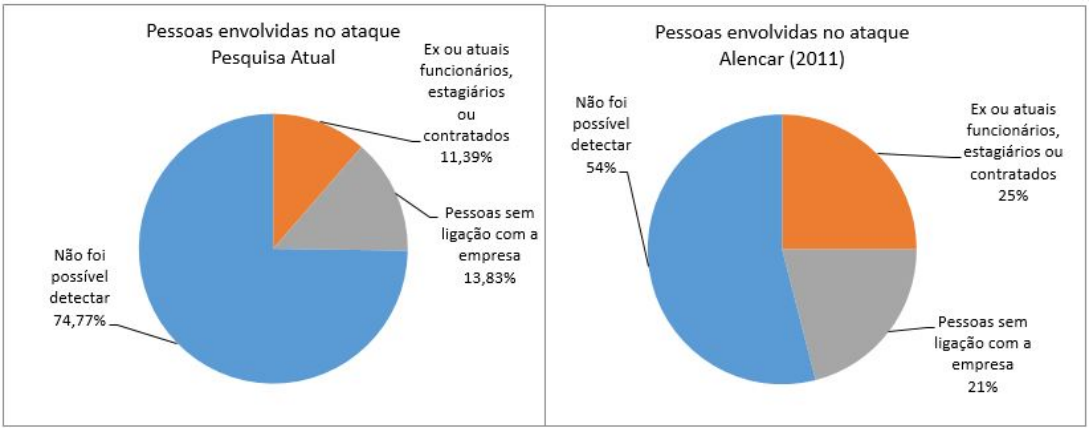
Quando foi possível detectar a origem, a quantidade de pessoas sem ligação com a empresa foi maior do que as consideradas insiders (pessoas com alguma ligação com a

Figura 26 – Gráfico dos Principais Perdas Geradas pelos Ataques



Fonte: autor.

Figura 27 – Gráfico das Origens das Pessoas Envolvidas nos Ataques



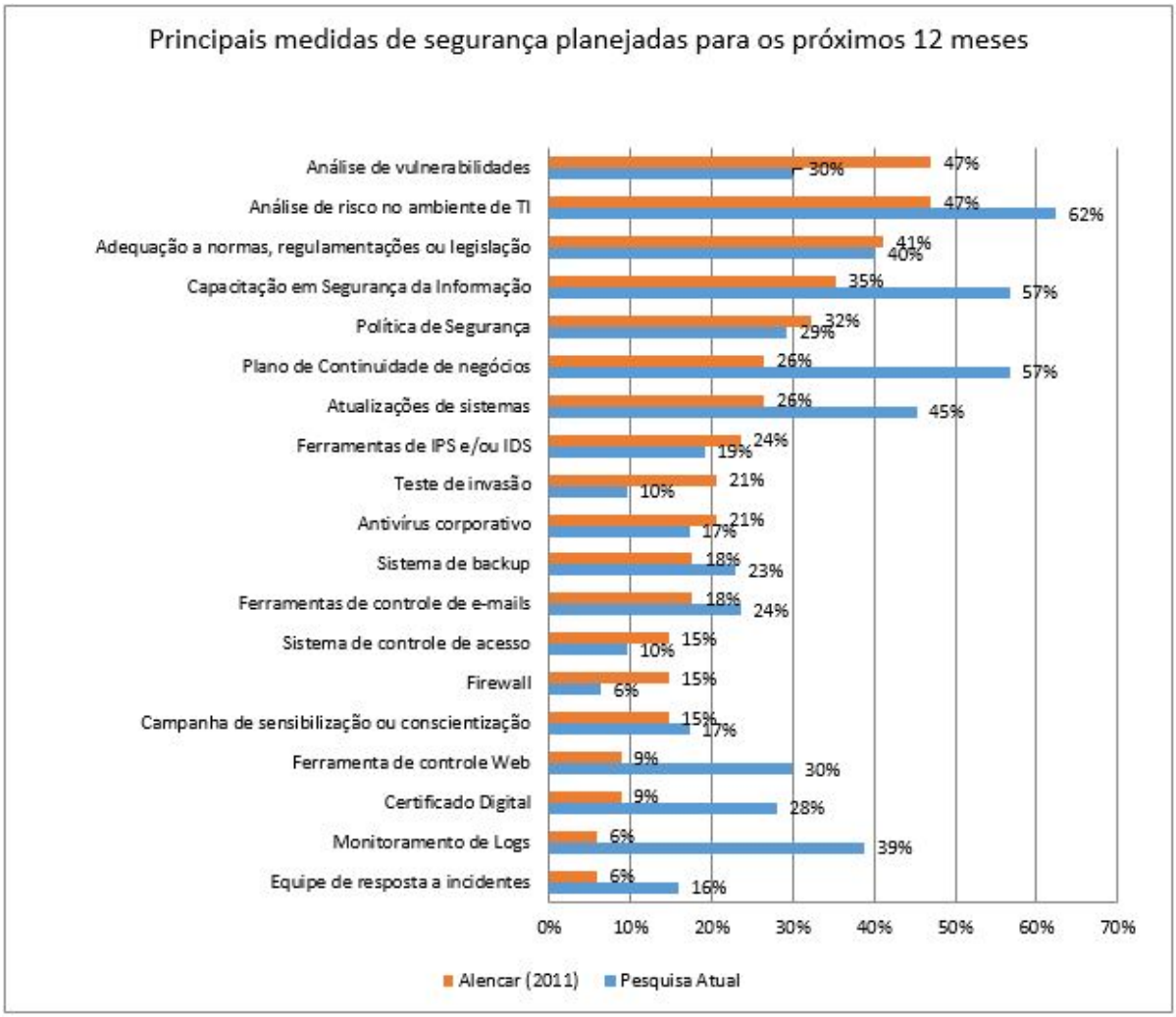
Fonte: autor.

empresa). Fato que foi o oposto dos resultados apresentados por Alencar (2011) e Modulo (2006). Porém ainda foi apontado 11,39% de insiders envolvidos, fato que não pode ser desprezado, como defende Schneier (2007).

Como último questionamento desta seção, perguntou-se sobre a existência de medidas de segurança planejadas para os próximos 12 meses. Todas as empresas apontaram algum tipo de medida, conforme exibido no gráfico a seguir (Figura 28).

Em algumas áreas viu-se um decréscimo na intenção de ações. Em destaque percentual observou-se: Firewall, Sistema de controle de acesso, Teste de invasão e Análises de

Figura 28 – Gráfico das Principais Medidas de Segurança da Informação para os Próximos 12 meses



Fonte: autor.

vulnerabilidade. Porém a pesquisa não abordou se tais áreas estão entrando em desuso, se a solução atual já antede ou se apenas não é prioridade para os próximos doze meses.

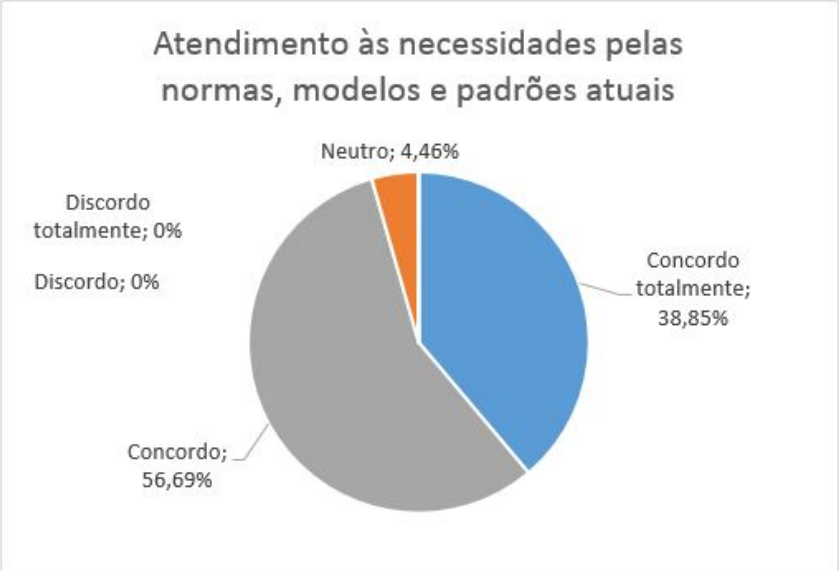
Porém, de uma forma geral, percebeu-se o aumento percentual das ações propostas nas empresas. As hipóteses são diversas para esse possível aumento. Por um lado pode ser oriundo de uma maior consciência dos problemas da área gerando, consequentemente, aumento das ações. Por outro lado, pode ser como tratamento de problemas ocorridos, ataques sofridos ou demanda reprimida na área.

4.2.5 Normas, Nível de Segurança e Desafios

Como complemento ao levantamento realizado, baseado em Alencar (2011), questionou-se se as normas, modelos e padrões atuais (por exemplo COBIT, ISO 27001, 27002, 27005, 27014, ITIL, etc) atendiam às necessidades da empresa. Nesta questão 95,54% das

empresas participantes da pesquisa apontaram “Concordo” ou “Concordo Totalmente”, conforme Figura 29.

Figura 29 – Gráfico do Atendimento às Necessidades Corporativas pelos Arcabouços Atuais



Fonte: autor.

Ciente que o arcabouço existente se adequa à grande maioria das empresas pesquisadas, mas que isso, de acordo com a literatura da área, não reflete na quantidade de empresas que realmente as aplica, questionou-se os motivos para a não utilização formal ou parcial do arcabouço existente na área. Neste caso, foram apontados vários motivos, destacando-se como principais categorias citadas:

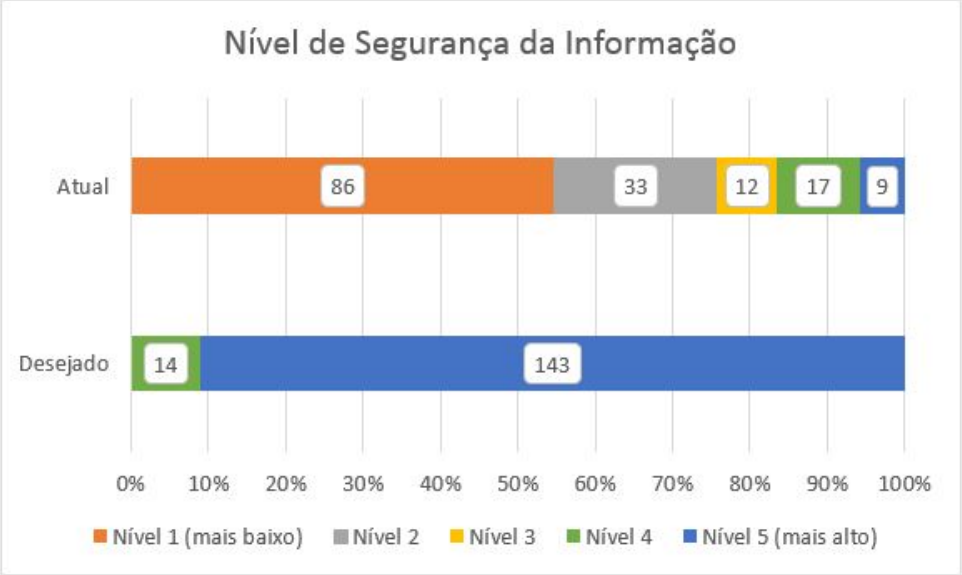
- Complexidade ou tamanho das normas (41,40%);
- Falta de apoio, definição ou priorização estratégica por parte do alto escalão (30,57%);
- Custos de implantação e gestão (21,65%);
- Falta de consciência, participação ou interesse de outras áreas envolvidas (19,74%);
- Acreditam que a aplicação parcial atende às necessidades da empresa (12,10%);
- Falta de conhecimento ou capacitação da equipe (11,46%).

Tais fatores levantados ratificam a situação e problemas expostos na fundamentação teórica, bem como corrobora com a justificativa do presente trabalho, com os dados expostos na Figura 20 e com o trabalho de Proença e Borbinha (2018) que aponta que os principais modelos de maturidades existentes não atendem, em sua completude, as atividades necessárias para aferir o nível de maturidade de segurança da informação conforme a ISO/IEC 27.001.

Outro ponto relevante também analisado é o desejo das empresas em alcançar patamares avançados no que tange a segurança da informação. Para isso foi solicitado às empresas que respondessem, de 1 a 5 (sendo 1 é o mais baixo nível de segurança e 5 é o mais alto), qual o nível de segurança desejado e qual o nível de segurança que acredita que a empresa estivesse no momento da realização da pesquisa.

Nas respostas, 91,08% (143 empresas) apontaram o desejo de estar no nível máximo (nível 5). Porém a situação real da empresa é bem diferente. Visto que, 54,8% desta mesma amostra, responderam que acreditam que se encontram no nível mínimo (nível 1), conforme Figura 30.

Figura 30 – Gráfico dos Níveis de Segurança da Informação Desejado e Estado Atual



Fonte: autor.

Ao analisar o gráfico (Figura 30) percebe-se a dificuldade em se alcançar níveis de excelência na área mesmo quando desejados. Bem como que ainda deverá ser ultrapassado um caminho longo para se atingir níveis aceitáveis na segurança da informação corporativa.

Fechando o questionário 1 (Apêndice B), questionou-se sobre quais eram os maiores problemas ou desafios de segurança da informação encontrados na empresa. Tal pergunta, de certa forma parecida com outras do questionário, foi inserida como uma pergunta de cobertura. Consistindo na revisita ao tema como uma tentativa de melhor detalhar ou captar as informações.

Como respostas, vários motivos foram apresentados, destacando-se como principais categorias citadas:

- Falta de apoio, definição ou priorização estratégica por parte do alto escalão (55,44%);
- Restrições orçamentárias (43,95%);

- Escassez de recursos humanos na área de segurança da informação (32,48%);
- Falta de consciência, conhecimento ou interesse por parte dos funcionários (26,75%);
- Falta de conhecimento ou capacitação da equipe de TIC em segurança da informação (19,11%).

Os resultados corroboram a pesquisa de Fazenda e Fagundes (2015) que analisaram os desafios para estabelecer e manter um SGSI no cenário brasileiro. Os autores apontaram a "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 à mudança" como principais desafios para esta área.

Ao analisar as repostas desta última pergunta, verificou-se que a cobertura feita coincide e corrobora com as informações apresentadas nas Figuras 20 e 23, bem como com a análise do questionamento sobre os motivos para a não utilização das normas, modelos ou padrões atuais que foi exibida nesta subseção. Diante disto, acredita-se que um dos objetivos deste questionário, que foi levantar os possíveis problemas ou obstáculos para a área, foi verificado e atendido.

4.3 Ordenação dos Controles ISO/IEC 27001 e 27002

Na análise dos dados coletados na segunda parte da pesquisa (Questionário 2 exibido no Apêndice C), foram inseridos os controles existentes no anexo da norma ISO/IEC 27.001, os mesmos da IS/IEC 27.002, e submetidos à avaliação das empresas através de uma escala de 1 (nenhuma importância) a 5 (muito importante), sendo a nota 3 categorizada como neutro na escala.

O índice de cada um dos 114 controles da norma (versão de 2013), são exibidos na Tabela 6, sendo ordenados de forma decrescente pela média do controle. O tamanho da amostra, como já citado, foi de 157 empresas.

Os controles são apresentados pelo mesmo código da norma ISO/IEC 27.001, ou seja, de A.5.1.1 até A.18.2.3. O controle relativo a cada um deles podem ser visto nas normas ISO/IEC 27.001 (ABNT, 2013a), 27.002 (ABNT, 2013b) e no Apêndice C.

Tabela 6 – Detalhamento dos Valores Obtidos para Cada Controle

Ordem	**Controle**	**Nota Mínima**	**Nota Máxima**	**Média**	**Mediana**	**Desvio-padrão**
1	**A.9.2.4**	3	5	4,47	4	0,67
2	**A.11.2.5**	2	5	4,41	4	0,72
3	**A.11.2.4**	3	5	4,21	4	0,68

Tabela 6 - continuação da página anterior

Ordem	Controle	Nota Mínima	Nota Máxima	Média	Mediana	Desvio-padrão
4	**A.9.2.3**	3	5	4,20	4	0,71
5	**A.5.1.1**	3	5	4,12	4	0,73
6	**A.9.1.2**	3	5	4,07	4	0,74
7	**A.11.1.5**	3	5	4,03	4	0,67
8	**A.9.4.4**	3	5	3,99	4	0,69
9	**A.15.1.3**	2	5	3,98	4	0,87
10	**A.11.2.6**	3	5	3,94	4	0,73
11	**A.9.2.5**	2	5	3,91	4	0,79
12	**A.18.1.5**	2	5	3,89	4	0,84
13	**A.6.1.1**	3	5	3,87	4	0,69
14	**A.8.2.1**	3	5	3,87	4	0,61
15	**A.18.1.1**	3	5	3,84	4	0,73
16	**A.18.1.4**	3	5	3,79	4	0,68
17	**A.8.1.2**	3	5	3,75	4	0,71
18	**A.6.1.5**	2	5	3,71	4	0,87
19	**A.7.2.1**	3	5	3,69	4	0,67
20	**A.9.4.2**	3	5	3,66	4	0,75
21	**A.11.2.7**	2	5	3,66	4	0,83
22	**A.6.2.2**	2	5	3,65	4	0,85
23	**A.9.2.1**	3	5	3,65	4	0,69
24	**A.18.1.3**	3	5	3,63	4	0,75
25	**A.13.1.3**	2	5	3,62	4	0,85
26	**A.7.1.1**	2	5	3,61	4	0,88
27	**A.12.6.2**	3	5	3,57	4	0,68
28	**A.8.2.3**	3	5	3,56	4	0,75
29	**A.18.1.2**	2	5	3,52	3	0,87
30	**A.8.1.3**	3	5	3,52	4	0,85
31	**A.12.5.1**	3	5	3,52	4	0,71
32	**A.5.1.2**	3	5	3,49	4	0,67
33	**A.6.2.1**	3	5	3,49	3	0,61

Tabela 6 - continuação da página anterior

Ordem	Controle	Nota Mínima	Nota Máxima	Média	Mediana	Desvio-padrão
34	**A.9.2.6**	3	5	3,49	3	0,72
35	**A.12.1.4**	3	5	3,49	4	0,64
36	**A.16.1.7**	3	5	3,49	3	0,69
37	**A.17.1.1**	3	5	3,49	3	0,72
38	**A.18.2.2**	3	5	3,49	4	0,71
39	**A.7.2.2**	3	5	3,48	3	0,73
40	**A.14.2.6**	3	5	3,48	3	0,77
41	**A.8.1.1**	3	5	3,47	3	0,71
42	**A.11.1.3**	3	5	3,47	3	0,67
43	**A.11.2.3**	3	5	3,47	3	0,78
44	**A.13.1.1**	3	5	3,47	3	0,68
45	**A.11.2.2**	3	5	3,46	3	0,72
46	**A.8.3.1**	3	5	3,44	3	0,70
47	**A.12.1.3**	3	5	3,40	3	0,79
48	**A.12.2.1**	3	5	3,40	3	0,69
49	**A.16.1.5**	3	5	3,39	3	0,67
50	**A.6.1.2**	3	5	3,38	3	0,72
51	**A.13.2.3**	3	5	3,38	3	0,78
52	**A.14.1.1**	3	5	3,37	3	0,77
53	**A.15.1.1**	3	5	3,37	3	0,78
54	**A.9.4.3**	3	5	3,32	3	0,68
55	**A.13.2.1**	3	5	3,30	3	0,71
56	**A.16.1.1**	3	5	3,27	3	0,70
57	**A.16.1.2**	3	5	3,25	3	0,50
58	**A.16.1.4**	3	5	3,25	3	0,68
59	**A.11.2.9**	3	5	3,22	3	0,69
60	**A.13.2.4**	3	5	3,22	3	0,68
61	**A.17.2.1**	3	5	3,22	3	0,69
62	**A.9.4.5**	3	5	3,21	3	0,71
63	**A.9.4.1**	2	5	3,20	3	0,69

Tabela 6 - continuação da página anterior

Ordem	Controle	Nota Mínima	Nota Máxima	Média	Mediana	Desvio-padrão
64	**A.12.1.1**	3	5	3,20	3	0,67
65	**A.13.1.2**	3	5	3,20	3	0,69
66	**A.16.1.3**	2	5	3,20	3	0,72
67	**A.8.1.4**	2	5	3,18	3	0,72
68	**A.12.7.1**	3	5	3,18	3	0,59
69	**A.8.2.2**	2	5	3,17	3	0,78
70	**A.18.2.3**	2	5	3,17	3	0,72
71	**A.11.2.1**	2	5	3,16	3	0,71
72	**A.9.3.1**	2	5	3,15	3	0,67
73	**A.18.2.1**	3	5	3,15	3	0,77
74	**A.9.1.1**	2	5	3,13	3	0,65
75	**A.14.2.9**	3	5	3,12	3	0,74
76	**A.14.2.5**	2	5	3,11	3	0,72
77	**A.12.3.1**	3	5	3,11	3	0,63
78	**A.11.1.2**	2	5	3,11	3	0,72
79	**A.11.1.1**	2	5	3,11	3	0,68
80	**A.7.2.3**	2	5	3,10	3	0,77
81	**A.12.6.1**	2	5	3,10	3	0,78
82	**A.15.1.2**	2	5	3,10	3	0,65
83	**A.12.1.2**	2	5	3,09	3	0,75
84	**A.12.4.1**	2	5	3,09	3	0,77
85	**A.14.1.2**	2	5	3,09	3	0,72
86	**A.14.1.3**	2	5	3,09	3	0,72
87	**A.15.2.1**	3	5	3,09	3	0,63
88	**A.6.1.3**	2	5	3,08	3	0,70
89	**A.10.1.1**	2	5	3,08	3	0,75
90	**A.14.2.3**	3	5	3,08	3	0,67
91	**A.14.2.2**	3	5	3,08	3	0,77
92	**A.17.1.3**	3	5	3,07	3	0,47
93	**A.9.2.2**	2	5	3,07	3	0,69

Tabela 6 - continuação da página anterior

Ordem	Controle	Nota Mínima	Nota Máxima	Média	Mediana	Desvio-padrão
94	**A.10.1.2**	3	5	3,07	3	0,55
95	**A.11.2.8**	2	5	3,07	3	0,69
96	**A.14.2.1**	2	5	3,07	3	0,75
97	**A.14.2.8**	3	5	3,07	3	0,72
98	**A.16.1.6**	3	5	3,06	3	0,64
99	**A.17.1.2**	3	5	3,06	3	0,51
100	**A.8.3.3**	3	5	3,05	3	0,49
101	**A.14.3.1**	3	5	3,05	3	0,71
102	**A.15.2.2**	2	5	3,04	3	0,72
103	**A.12.4.4**	3	5	3,03	3	0,70
104	**A.12.4.3**	2	5	3,02	3	0,71
105	**A.14.2.4**	2	5	3,02	3	0,68
106	**A.7.3.1**	2	5	3,01	3	0,77
107	**A.11.1.6**	2	5	3,01	3	0,69
108	**A.13.2.2**	2	5	3,01	3	0,68
109	**A.14.2.7**	2	5	3,01	3	0,75
110	**A.8.3.2**	2	5	3,00	3	0,69
111	**A.6.1.4**	2	5	2,99	3	0,71
112	**A.7.1.2**	2	5	2,99	3	0,65
113	**A.11.1.4**	2	5	2,98	3	0,66
114	**A.12.4.2**	2	5	2,98	3	0,70

Ordenando as respostas do questionário de forma cronológica de acordo com a obtenção das respostas, percebeu-se que, ao alcançar um grupo amostral com 121 empresas não houve mais alteração na ordenação dos controles.

Também percebeu-se que ao pegar grupos de 100 respostas (grupos de respostas testadas: 1-100, 11-110, 21-120, 31-130, 41-140 e 51-150), ordenados de forma cronológica de acordo com a obtenção das respostas, mesmo havendo algumas mudanças nas notas médias e pequenas alterações na ordenação dos controles, o grupo inicial dos 30 controles, exibidos na Tabela 6, permaneciam, praticamente inalterados. Em todos os grupos de 100 respostas testados, o seu conjunto inicial de 30 controles incorporava, ao menos, 27 dos 30 primeiros controles exibidos na Tabela 6.

Fatos que coincidem com o explanado pela lei da regularidade estatística, que afirma que um conjunto de n unidades tomadas ao acaso terá, provavelmente, características semelhantes a do grupo maior (GIL, 1999). Como também com a lei da permanência dos pequenos números, que aponta que os resultados de qualquer amostra da mesma magnitude, suficientemente numerosa e representativa da população deverão apontar resultados semelhantes (GIL, 1999).

Ciente que apenas as amostras do tipo probabilísticas são baseadas em tais leis (GIL, 1999), a verificação, mesmo que superficial, de sua possível aplicação na amostra utilizada do tipo não-probabilística, aponta para a relevância e consistência da amostra obtida.

4.4 Síntese do Capítulo

Esta etapa da pesquisa teve, como principal norte, o atendimento do objetivo específico:

"Compreender como a segurança da informação é tratada, nos diversos aspectos que abrangem essa área, no meio corporativo".

Para isso, foi feita a fotografia do ambiente através das respostas dos surveys. Os questionários foram respondidos por 248 empresas, resultando em 157 respostas válidas, alcançando empresas de toda a região do Brasil e quatro outros países (Argentina, Estados Unidos da América, Inglaterra e Portugal).

Como já era esperado na pesquisa, devido ao ambiente atual, relatos do noticiário e outros trabalho acadêmicos, a informação é de suma importância para as organizações e, consequentemente, cresceu a necessidade pela segurança das mesmas.

Os resultados, de uma forma geral, apontam que as empresas não estão totalmente adequadas ou preparadas no que tange à segurança da informação e têm um investimento mais forte nas ferramentas do que na construção de um ambiente propício para a segurança da informação. Para se alcançar o ambiente desejável, as empresas ainda carecem de ações e políticas para definições, alinhamento, capacitação e conscientização da segurança da informação.

Neste capítulo também buscou-se comparar os resultados obtidos com outros estudos. Tal ação visa nortear os resultados e apontar, de certa forma, se houve um crescimento, decréscimo, melhora ou piora em determinado aspecto.

Porém, como sugerido por diversas vezes, é importante ressaltar que essa análise é apenas de resultados, comparando dois ambientes de pesquisas diferentes. Devendo ser analisada com cuidado para apontamentos de tendências ou afirmações cabais devido, principalmente, ao período de realização de cada uma delas, à amostra, método utilizado, etc.

Por conta desta situação, qualquer explicação ou linha de tendência traçada deve ser vista apenas como hipóteses e que carecem de novos estudos para comprová-la. Que, mesmo sabendo da importância, não foi o objetivo deste trabalho.

5 EVOLUÇÃO DA ESTRATÉGIA PROPOSTA

Como já apresentado em seção específica, o presente trabalho tem um conjunto de objetivos que visa melhorias na área de segurança da informação, em especial nas áreas de priorização, maturidade e simplificação.

Seguindo a proposta metodológica e com base na fundamentação teórica estudada e no resultado do levantamento realizado, exposto no Capítulo 4, concebeu-se a estratégia proposta denominada Priorização e Maturidade em Segurança da Informação Adaptável (Primasia).

Porém, para se alcançar o modelo final da estratégia, Primasia, diversas etapas foram vencidas para conceber, aprimorar e avaliar o artefato.

Como etapa inicial, pensou-se em elencar os principais controles da norma ISO/IEC 27.001 e 27.002, simplificando-a. Tais controles serviram como proposta simplificada para uma Política de Segurança da Informação e, posteriormente, para um Sistema de Gestão de Segurança da Informação. Tal pensamento gerou a Versão 1 do artefato, detalhado na Seção 5.1.

Ciente que tal artefato não seria suficiente para contemplar todas as áreas propostas, projetou-se uma evolução para o mesmo. O artefato, agora em sua Versão 2, foi concebido como um possível modelo de maturidade. Neste modelo, o estágio inicial contempla os pontos de interesse tratados na versão anterior. A Versão 2 do artefato será exibida na Seção 5.2.

A Seção 5.3 demonstrará as melhorias implementadas chegando à Versão 3 do artefato. Essa versão a insere como uma estratégia para priorização e avaliação da maturidade da segurança da informação, contemplando todo o escopo proposto neste projeto para o artefato.

Na Seção 5.4 será apresentada a versão atual do artefato, denominado Estratégia Primasia, concebida como a evolução da Versão 3, através dos aprimoramentos sugeridos em sua avaliação.

Por fim o capítulo é concluído com as considerações expostas na Seção 5.5.

Para concepção dos artefatos foram utilizados o COBIT e as normas ISO/IEC 27.001, 27.002 e 27.005.

Poder-se-ia construir um artefato do zero, porém acredita-se que a adesão ao artefato e a sua implantação seria mais difícil, ponto que entra em conflito com os objetivos da pesquisa. Visto que já se tem dificuldades com os frameworks, modelos e normativos já consolidados no mercado, quanto mais em um possível novo “concorrente”. Ressalta-se também que a construção do modelo partindo do zero seria muito mais custoso.a Por

fim, um modelo baseado nas melhores práticas existentes torna-se mais robusto e alcança uma medição de maturidade com resultados consideráveis e embasados (GOMES et al., 2016). Bem como, é salutar para a área, a utilização da expertise de mais de um modelo existente, como ressalta Dimitriadis (2011), Karokola, Kowalski e Yngström (2011), Rigon et al. (2014), Mahopo, Abdullah e Mujinga (2015), entre outros trabalhos citados na fundamentação teórica.

O motivo da escolha do COBIT e das normas ISO/IEC 27.001, 27.002 e 27.005 foi embasado na literatura que os coloca como referências na área, conforme já mencionado no Capítulo 3. Entre os diversos trabalhos inseridos que destacam os arcabouços escolhidos, pode-se citar Albuquerque Junior e Santos (2014), Fernandes e De Abreu (2014), Prado et al. (2016), Gomes et al. (2016) e Rea-Guaman et al. (2017).

Mesmo embasado pela literatura existente para a escolha do arcabouço que alicerçaria a concepção dos artefatos, procurou-se ouvir o mercado sobre o atendimento das necessidades corporativas por tais documentos. Obtendo concordância de 95,54% das empresas participantes, conforme demonstrado anteriormente na Figura 29.

5.1 Versão 1 - Política de Segurança da Informação Simplificada

A primeira versão do artefato visava elencar os principais controles da norma ISO/IEC 27.001 e 27.002, simplificando-a. Tais controles serviram como uma proposta simplificada para uma PSI e, posteriormente, para um SGSI.

Para isso, foram analisadas as respostas obtidas no Questionário 2 (Apêndice C) e selecionados os controles que tiveram a média e mediana acima de três. Com base nos controles selecionados pelo crivo de média e mediana superior a três, foi analisada a existência de algum controle pré-requisito para algum controle selecionado. Caso isso ocorresse e o controle pré-requisito não estivesse na lista, o mesmo deveria ser inserido. Conforme método exposto na Figura 31.

Os pré-requisitos foram elencados com base na análise deste autor e, posteriormente, enviados aos especialistas para avaliação. Para verificar a condição de especialistas foi enviado um questionário (Apêndice D). Sendo obrigado o atendimento, no mínimo, dos itens descritos no Capítulo 2. Nesta etapa, o questionário, foi enviado para seis possíveis especialistas, cinco responderam e tiveram o perfil desejado, conforme Quadro 6, atendendo ao desenho metodológico.

Com o grupo de especialistas atendendo às condições propostas nesta pesquisa, foi enviado o questionário com a lista de 19 controles da norma ISO/IEC, que possivelmente necessitavam de pré-requisitos, para avaliação dos especialistas (Apêndice E). A lista de controles e pré-requisitos foi concebida pelo autor desta pesquisa.

Quadro 6 – Dados Especialistas - Avaliação pré-requistos

	Esp. 1	**Esp. 2**	**Esp. 3**	**Esp. 4**	**Esp. 5**
Experiência com TIC (anos)	25	27	12	15	31
Experiência com segurança (anos)	15	20	10	15	20
Trabalha em empresa de segurança	Sim	Não	Sim	Não	Não
Maior cargo assumido	Sócio-diretor	Diretor	Gerente de Produtos	Analista Sênior de Segurança	Sócio-diretor
Tempo no maior cargo (anos)	20	4	6	6	25
Maior titulação	Mestrado	Doutorado	Mestrado	Especialista	Especialista
Titulação em andamento	-	-	Doutorado	Mestrado	-
Titulação na área de segurança	Mestrado	Doutorado	Mestrado	Especialização	Especialização
Tem experiência com maturidade	Sim	Sim	Não	Sim	Sim
Quantidade de publicações acadêmicas	Mais que 7	Mais que 7	Mais que 7	Entre 1 e 3	0
Quantas delas em segurança	Mais que 7	Mais que 7	Mais que 7	Entre 1 e 3	0
Certificações na área de TIC	Entre 1 e 3	0	Entre 4 e 7	Mais que 7	Mais que 7
Quantas delas em segurança	Entre 1 e 3	0	Entre 1 e 3	Mais que 7	Mais que 7
Experiência no ensino em TIC	Palestrante e Professor em Graduação e Especialização	Palestra, Professor e Coordenador em Graduação, Mestrado e Doutorado	Palestra e Professor em Graduação e Especialização	Professor em Graduação e Especialização	Palestra e Professor em Graduação e Especialização
Experiência no ensino em segurança	Palestra e Professor em Graduação e Especialização	Palestra e Professor em Graduação, Mestrado e Doutorado	Palestra e Professor em Graduação e Especialização	Professor em Graduação e Especialização	Palestra e Professor em Graduação e Especialização
Tempo de experiência no ensino de TIC	15	25	4	10	20
Quanto deste tempo em segurança	15	20	3	8	15

As informações coletadas dos especialistas apontaram para a necessidade de manter treze controles, remover seis e inserir um controle, conforme Quadro 7.

Quadro 7 – Posição dos Especialistas Quanto aos Controles Pré-requisitos

Controle	Pré-requisito	Ação	Justificativas dos Especialistas
A.5.1.2	**A.5.1.1**	Manter	-
A.6.2.1	**A.5.1.1**	Excluir	Mesmo sendo uma boa prática a inclusão de tais itens na PSI concebida conforme o controle A.5.1.1, pode ser uma política ou normativo à parte.
A.6.2.2	**A.5.1.1**	Excluir	Mesmo sendo uma boa prática a inclusão de tais itens na PSI concebida conforme o controle A.5.1.1, pode ser uma política ou normativo à parte.
A.7.2.1	**A.7.1.2**	Excluir	Mesmo sendo uma boa prática a unificação em um documento concebido conforme o controle A.5.1.1, pode ser uma política ou normativo à parte.
A.7.2.3	**A.5.1.1**	Excluir	Mesmo sendo uma boa prática a unificação em um documento concebido conforme o controle A.5.1.1, pode ser uma política normativo ou legislação à parte.
A.8.1.2	**A.8.1.1**	Excluir	Mesmo sendo uma boa prática a realização de um inventário inicial concebido conforme o controle A.8.1.1, não é obrigatório a realização do mesmo para a identificação do proprietário.
A.8.2.2	**A.8.2.1**	Manter	-
A.8.2.3	**A.8.2.1**	Manter	-
A.8.3.1	**A.8.2.1**	Manter	-
A.9.1.2	**A.9.1.1**	Excluir	Mesmo sendo uma boa prática a definição dos acessos baseados em uma política concebida conforme o controle A.9.1.1. Procedimentos de autorização, até mesmo formal, podem ser feitos antes da política.
A.9.4.1	**A.9.1.1**	Manter	-
A.9.4.2	**A.9.1.1**	Incluir	Está na definição do controle “onde aplicável pela política de controle de acesso”. Portanto, caso seja realizada a ação do controle A.9.4.2 sem a política proposta no controle A.9.1.1, a mesma poderá prover melhorias na segurança, mas a ação não estará atendendo ao controle A.9.4.2.
A.11.1.2	**A.11.1.1**	Manter	-
A.12.4.2	**A.12.4.1**	Manter	-
A.17.1.2	**A.17.1.1**	Manter	-
A.17.1.3	**A.17.1.2**	Manter	-
A.18.1.2	**A.18.1.1**	Manter	-
A.18.1.3	**A.18.1.1**	Manter	-
A.18.1.4	**A.18.1.1**	Manter	-
A.18.1.5	**A.18.1.1**	Manter	-

Um nova rodada de questionamento foi enviada para os especialistas, em formato de questionário semelhante ao inicial (Apêndice E), porém inserindo os dados expostos no Quadro 7 e a lista ajustada, agora com 14 controles que, possivelmente, necessitam de

pré-requisitos. O formulário deste novo questionamento pode ser visto no Apêndice F.

No retorno desta segunda rodada, proposta ajustada, houve a concordância de todos os cinco especialistas, sendo então utilizados como pré-requisitos para esta pesquisa os 14 controles exibidos no Apêndice F e no Quadro 8.

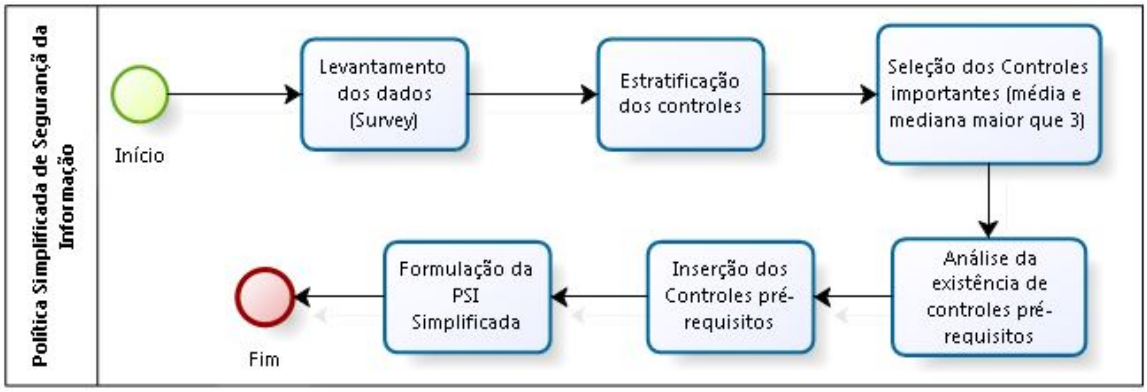
Quadro 8 – Resultado dos Controles com Pré-requisitos

Controle	**Título**	**Pré-requisito**	**Título**
A.5.1.2	Análise crítica das políticas para segurança da informação	A.5.1.1	Políticas para segurança da informação
A.8.2.2	Rótulos e tratamento da informação	A.8.2.1	Classificação da informação
A.8.2.3	Tratamento dos ativos	A.8.2.1	Classificação da informação
A.8.3.1	Gerenciamento de mídias removíveis	A.8.2.1	Classificação da informação
A.9.4.1	Restrição de acesso à informação	A.9.1.1	Política de controle de acesso
A.9.4.2	Procedimentos seguros de entrada no sistema (log-on)	A.9.1.1	Política de controle de acesso
A.11.1.2	Controles de entrada física	A.11.1.1	Perímetro de segurança física
A.12.4.2	Proteção das informações dos registros de eventos (logs)	A.12.4.1	Registros de eventos
A.17.1.2	Implementando a continuidade da segurança da informação	A.17.1.1	Planejando a continuidade da segurança da informação
A.17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação	A.17.1.2	Implementando a continuidade da segurança da informação
A.18.1.2	Direitos de propriedade intelectual	A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais
A.18.1.3	Proteção de registros	A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais
A.18.1.4	Proteção e privacidade de informações de identificação pessoal	A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais
A.18.1.5	Regulamentação de controles de criptografia	A.18.1.1	Identificação da legislação aplicável e de requisitos contratuais

Com o método desenhado (Figura 31), incluindo: levantamento de dados, seleção dos controles com média e mediana acima de três e inserção de controles pré-requisitos, conforme lista validada por especialistas, uma primeira versão desta proposta foi apresentada em Silva Neto, Alencar e Queiroz (2015) considerando apenas pequenas e médias empresas. Uma nova versão, abrangendo empresas de todos os portes, foi apresentada em Alencar, Tenorio Junior e Moura (2017a).

A versão descrita em Alencar, Tenorio Junior e Moura (2017a) culminou nos 31 controles a seguir:

Figura 31 – Processo de Criação de uma PSI Simplificada



Fonte: autor.

- A.5.1.1 Definição de Políticas de Segurança da Informação
- A.6.1.1 Definição das Responsabilidades
- A.6.1.5 Segurança da Informação considerada no gerenciamento de projetos
- A.6.2.2 Política e medidas em locais de trabalho remoto
- A.7.1.1 Verificação do Histórico para todos os candidatos ao emprego
- A.7.2.1 Funcionários e Terceiros praticando a Segurança da Informação
- A.8.1.2 Ativos com respectivos proprietários
- A.8.1.3 Regras para uso aceitável das informações
- A.8.2.1 Classificação da informação
- A.8.2.3 Procedimentos para o tratamento de ativos
- A.9.1.2 Perfil de acesso dos usuários
- A.9.2.1 Registro e cancelamento de usuários
- A.9.2.3 Direitos de acesso privilegiado sejam restritos e controlados
- A.9.2.4 Controle de concessão de informação de autenticação secreta
- A.9.2.5 Análise regular dos proprietários de ativos
- A.9.4.2 Procedimento seguro de entrada no sistema (log-on)
- A.9.4.4 Controle e restrições de programas utilitários
- A.11.1.5 Procedimentos para o trabalho em áreas seguras

- A.11.2.4 Manutenção correta dos equipamentos
- A.11.2.5 Não retirar equipamentos, informações ou softwares sem autorização
- A.11.2.6 Medidas de segurança para ativos fora da organização
- A.11.2.7 Análise de todos os equipamentos de mídias antes do descarte
- A.12.5.1 Controle de instalação de Software
- A.12.6.2 Regras e critérios para a instalação de software pelos usuários
- A.13.1.3 Segregação em redes de informação, usuários e serviços
- A.15.1.3 Requisitos para acordos com fornecedores relacionados a riscos
- A.18.1.1 Documentar todos os requisitos legais e contratuais
- A.18.1.2 Procedimentos apropriados legais e contratuais
- A.18.1.3 Proteção dos registros
- A.18.1.4 Privacidade e Proteção das informações quando aplicável
- A.18.1.5 Controles de criptografia usados em conformidade com a legislação

Quando se busca a certificação referente à norma ISO/IEC 27001, torna-se necessário abordar todos os 114 controles. Neste caso, o processo de seleção e priorização aqui proposto e apresentado em Silva Neto, Alencar e Queiroz (2015) e Alencar, Tenorio Junior e Moura (2017a) servirá como guia para se atingir o alvo e, ao mesmo tempo, fazendo com que o caminho seja traçado e percorrido inserindo inicialmente os controles considerados mais importantes. Desta forma, acredita-se que não apenas o objetivo de atender os controles para a certificação será realizado, como, também, a corporação começará a tratar os pontos mais importantes de imediato.

Porém, mesmo tendo aumentado ano após ano, o número de empresas que têm ativos no escopo com certificação ISO/IEC 27001 no Brasil é muito baixo, aproximadamente 100 empresas até o primeiro semestre de 2017 (DATACENTER DYNAMICS, 2017; MERKER, 2017). O que faz entender que a maioria das corporações não tem a necessidade, interesse ou recursos suficientes para aplicar ou tratar todos os controles e buscar a certificação. Neste aspecto, acredita-se que o processo em questão tenha mais valia, apontando os controles mais importantes e, consequentemente, direcionando os esforços para os que deverão ser implantados.

Tendo por base esses controles, o trabalho seguiu para a concepção de um modelo de maturidade. Mas, para isso, esta versão precisaria ser avaliada. Fato que ocorreu e é descrito a seguir.

5.1.1 Avaliação da Versão 1

Como método de avaliação desta versão, foram executadas três ações:

- Levantamento da aceitação com especialistas;
- Levantamento da aceitação com empresas;
- Submissão de artigos.

Cada uma das ações, por ordem cronológica de execução, são detalhas a seguir.

5.1.1.1 Levantamento da Aceitação com Especialistas

Com relação às duas etapas de levantamento propostas para avaliar o presente artefato, PSI simplificada, foram utilizados dois questionários exibidos no Apêndice G.

Na primeira etapa, enviou-se a proposta para seis especialistas na área de segurança da informação. Nesta ação obteve-se a resposta de cinco deles, sendo os mesmos que avaliaram os pré-requisitos da norma, conforme descrição do Quadro 6.

Ao questionar os especialistas se a versão apresentada abrangia os principais pontos para uma PSI, levando em consideração que esta embasará uma proposta de governança ágil de segurança da informação, todos responderam de forma positiva. Um dos especialistas ainda afirmou que cumprindo todos os 31 controles elencados, a empresa estaria em um patamar bastante elevado se comparado com o mercado.

5.1.1.2 Levantamento da Aceitação com Empresas

A segunda etapa da avaliação consistiu em enviar para as 157 empresas respondentes do primeiro survey o modelo simplificado proposto e um questionamento, a saber: se o mesmo atenderia às necessidades da empresa e se haveria o interesse da empresa em implantar este modelo simplificado. Foi solicitado que justificassem suas respostas (Apêndice G).

Dos 157 questionários enviados, 104 (66,24%) foram retornados. Destes, todos afirmaram que o modelo atendia às necessidades da empresa. Porém, 16 empresas (10,19% dos respondentes) afirmaram que, mesmo atendendo as necessidades da empresa, não o implantariam, visto que ainda o consideram muito complexo. As demais afirmaram ser viável a implantação de tal proposta na empresa.

Desta forma, acredita-se que a redução dos controles e a listagem feita tenham validade por atender às expectativas dos especialistas em segurança consultados, bem como a mais de 84% das empresas respondentes do questionário de avaliação.

5.1.1.3 Publicações de Artigos

Utilizou-se, também, como forma de avaliação a submissão de artigos. Como resultado, houveram duas publicações: Silva Neto, Alencar e Queiroz (2015) e Alencar, Tenorio Ju-

nior e Moura (2017a). Os retornos recebidos na fase de avaliação realizada pelos membros do comitê do programa, bem como, as apresentações dos trabalhos, auxiliaram não apenas à evolução do artefato apresentado como, também, as demais áreas da tese, em especial, a fundamentação teórica e método da pesquisa.

Percebeu-se, em especial, como ganhos com esta versão do artefato:

- A avaliação do grupo de controles pré-requisitos por especialistas;
- A avaliação das empresas e especialistas sobre o atendimento às necessidades da empresa utilizando um conjunto reduzido de controles;
- A aceitação dos artigos e, consequentemente, do artefato pela academia.

Porém, os ganhos elencados não eram suficientes para atender todos os objetivos propostos. Esta versão compõe a primeira parte da estratégia proposta (simplificação e priorização dos controles da ISO/IEC 27001 e 27002).

Diante desse fator e da busca contínua pela melhoria do artefato, incluindo as orientações deste projeto, revisitas à literatura, apresentações deste trabalho e debates com especialistas da área e com o grupo de pesquisa GP2 do CIn/UFPE, o artefato foi evoluído para a Versão 2, demonstrada a seguir.

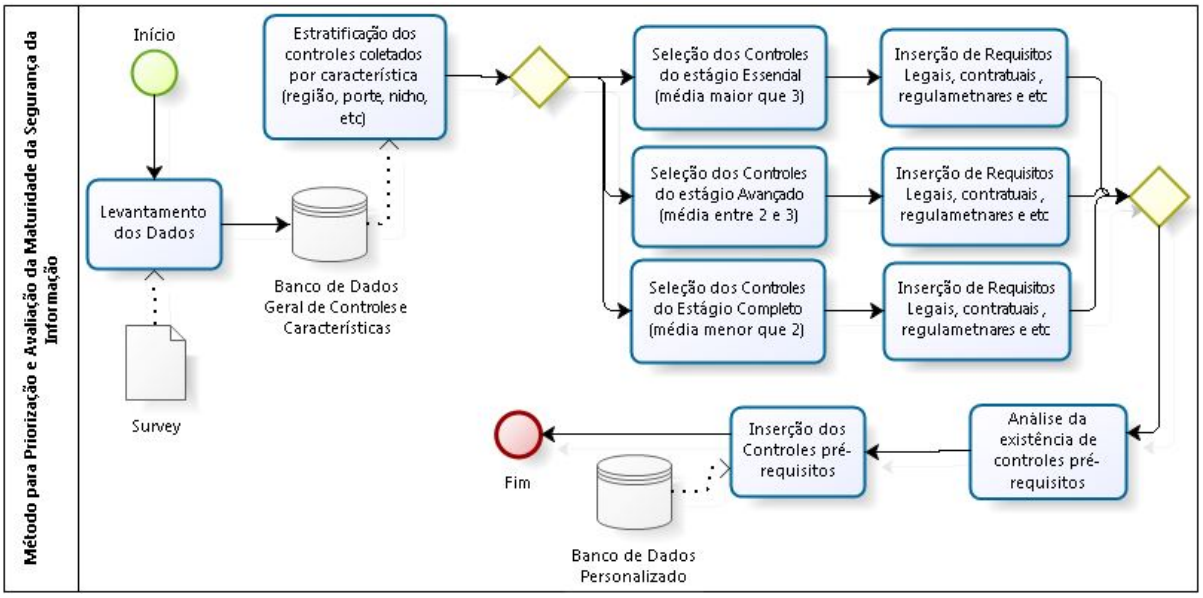
5.2 Versão 2 - Modelo de Avaliação da Maturidade e Priorização da Segurança da Informação

De modo mais amplo, o artefato proposto, agora em sua Versão 2, pode servir para aferir a maturidade da segurança da informação, além da elaboração de uma PSI simplificada e priorização dos controles, como demonstrado na Versão 1 do artefato. O detalhamento de processo proposto pode ser visto na Figura 32.

Os modelos de maturidade, como os já citados na fundamentação teórica, visam elencar fatores para categorizar as empresas em estágios. Por exemplo, utilizando os controles da ISO/IEC 27.002, como neste trabalho. Porém os mesmos são tratados de forma estática. Por exemplo, atendendo aos controles X, Y, Z a empresa está no nível 1; atendendo aos controles X, Y, Z, A, B, C, estará no nível 2. Ou pela forma de implementação de estágio, por exemplo o modelo do COBIT (ITGI, 2007; ISACA, 2012a), cuja descrição foi inserida no Quadro 5.

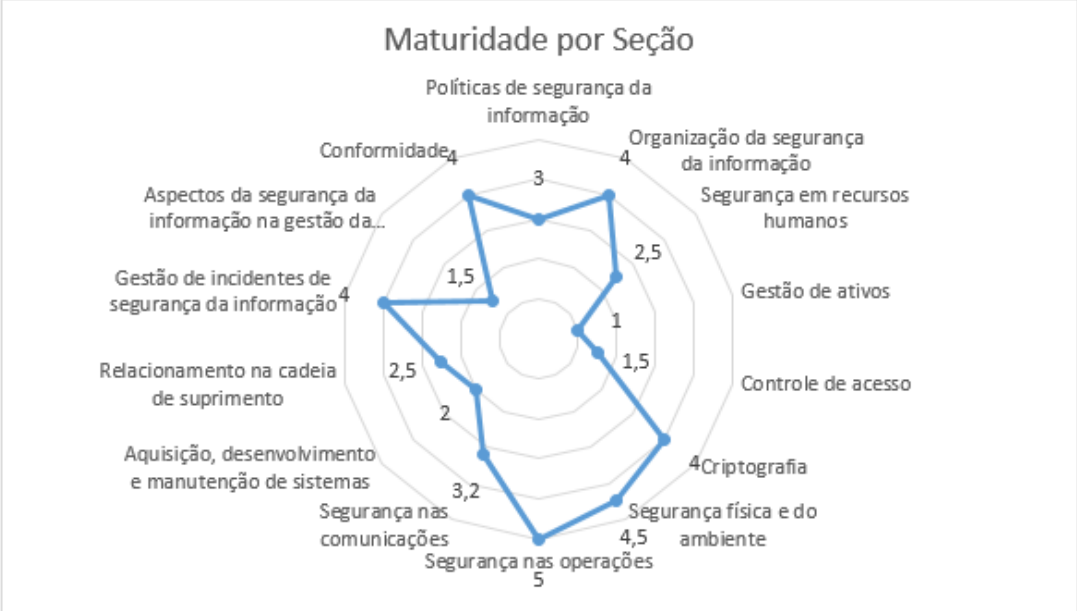
Então um conjunto de controles ou de processos podem ser definidos e analisados o seu grau de aplicação ou aderência para chegar ao nível de maturidade. Por exemplo, pegando os controles de cada seção da ISO/IEC 27.002 e retirando a média entre eles, como exemplificado na Figura 33. Bem como, pode se ter um nível geral de maturidade da empresa tirando a média da maturidade de cada seção. No exemplo da Figura 33, seria nível de maturidade global 3,05.

Figura 32 – Processo para Avaliação da Maturidade e Priorização da Segurança da Informação



Fonte: autor.

Figura 33 – Exemplo de Resultado de Maturidade por Seções da ISO/IEC 27.002



Fonte: autor.

Contudo, uma simples média dos controles pode transmitir uma visão turva para a empresa, visto que algumas indagações podem ser feitas, entre elas:

- Será que todos os controles têm a mesma importância para a empresa?
- Será que os controles selecionados, sejam todos ou não, tem a mesma importância

para todas as empresas?

- Será que os controles selecionados, todos ou não, terão a mesma validade em outros anos ou períodos?

A resposta é, provavelmente, não para todos os questionamentos. Devendo haver tratamento para todos eles.

Como forma de solucionar tal problema, bem como na tentativa de aprimorar os modelos existentes, a presente proposta poderá ser utilizada para criar um modelo de maturidade dinâmico.

O modelo dinâmico consiste em estratificar os controles de acordo com a importância dada pelas empresas. A medida que os questionários são aplicados e reaplicados no decorrer dos anos, os controles são ajustados para os novos estágios. Ou seja, o modelo é ajustado de acordo com a realidade dos respondentes sendo assim adaptável e dinâmico. Uma proposta é apresentada, como exemplo, no Quadro 9. Nele foram criados três estágios: Essencial, Avançado e Completo. Cada estágio é composto por um conjunto de controles. O primeiro, Essencial, revela os controles mais importantes, média maior do que três (M>3), e seus pré-requisitos. O segundo, Avançado, aponta os controles com média maior ou igual a dois e menor ou igual do que três ($2 \leq M \leq 3$) e seus pré-requisitos (caso não tenha sido inserido no estágio anterior). Por fim, o estágio Completo que contempla os controles com média abaixo de 2 (M<2), como fluxo mostrado na Figura 32. Desta forma, tem-se o estágio Essencial como o inicial, após atender este estágio pode-se buscar o Avançado e, por fim, após atender os dois estágios anteriores, o Completo que contempla os controles com menor índice de importância de acordo com as empresas. Assim, ao atender o estágio completo, a empresa terá atendido a todos os controles, neste caso do Anexo da ISO/IEC 27.001 e ISO/IEC 27.002.

Quadro 9 – Estratificação dos Controles de Acordo com sua Importância - Artefato Versão 2

Média do Controle	**M>3**	**$2 \leq M \leq 3$**	**M<2**
Estágio	Essencial	Avançado	Completo
Controles	A, B, C	X, Y, Z	G, H, I

Desse modo, temos um conjunto de controles ordenados, de acordo com a importância dada pelas empresas. Os controles são estratificados em três estágios e cada estágio tem os seis níveis do COBIT (Quadro 5). É verificado o nível de cada controle aplicável à empresa.

A empresa estará apta a passar de estágio quando todos os controles aplicáveis do estágio atual atingirem, ao menos, o nível 3 (processo definido). O nível de maturidade da empresa é expresso pelo nome do estágio em que ela se encontra (Essencial, Avançado ou

Completo) mais a média das notas de maturidade de cada controles do referido estágio, por exemplo (utilizando os dados do Quadro 9 e empresas fictícias):

- A Empresa A teve as seguintes notas de maturidades: Controle A=3, B=2, C=3, X=3, Y=2, Z=1, G=4, H=3, I=3. È analisado se todos os controles do primeiro estágio (Essencial) obtiveram, ao menos, nota 3. Neste caso, a empresa não atingiu devido ao controle B. Calcula-se a média dos controles do estágio que a empresa se encontra (A=3, B=2, C=3, média=2,33). Então a Empresa A encontra-se no nível de maturidade Essencial 2,33.

- A Empresa B teve as seguintes notas de maturidades: Controle A=5, B=2, C=5, X=3, Y=2, Z=1, G=4, H=3, I=3. È analisado se todos os controles do primeiro estágio (Essencial) obtiveram, ao menos, nota 3. Neste caso, a empresa não atingiu devido ao controle B. Calcula-se a média dos controles do estágio que a empresa se encontra (A=5, B=2, C=5, média=4). Então a Empresa B encontra-se no nível de maturidade Essencial 4.

- A Empresa C teve as seguintes notas de maturidades: Controle A=4, B=3, C=3, X=3, Y=2, Z=1, G=4, H=3, I=3. È analisado se todos os controles do primeiro estágio (Essencial) obtiveram, ao menos, nota 3. Neste caso, a empresa está apta a passar para o próximo estágio. È analisado se todos os controles do segundo estágio (Avançado) obtiveram, ao menos, nota 3. Neste caso, não atingiu devido aos controles Y e Z. Calcula-se a média dos controles do estágio que a empresa se encontra (X=3, Y=2, Z=1, média=2). Então a Empresa C encontra-se no nível de maturidade Avançado 2.

Em comparação entre as empresas, verifica-se que a empresa C se apresenta em melhores condições de maturidade, pois passou para o segundo estágio (Avançado) e atendendo a todos os controles principais, elencados no estágio Essencial. A pior empresa na comparação é a Empresa A, pois mesmo estando no mesmo estágio da Empresa B (Essencial) tem o nível de maturidade menor 2,33.

Esta solução permite a priorização dos controles, colocando pesos diferentes para que os controles mais importantes tenham maior relevância na aferição da maturidade da segurança da informação, visto que os que serão tratados inicialmente (no estágio Essencial) serão os selecionados como mais importante pelas próprias empresas. Bem como esses controles e os valores das médias utilizadas podem ser ajustados periodicamente, de forma a melhor representar as necessidades gerais ou de cada nicho específico.

Tal pensamento, de abordagem dinâmica, também pode ser facilmente adaptado para modelos já existentes, sendo um possível aperfeiçoamento para os mesmos.

5.2.1 Avaliação da Versão 2

Como método de avaliação desta versão, foram executadas duas ações:

- Levantamento da aceitação com especialistas;
- Submissão de artigo.

Cada uma das ações, por ordem cronológica de execução, são detalhas a seguir.

5.2.1.1 Levantamento da Aceitação com Especialistas

Com relação à etapa de levantamento proposta para avaliar o presente artefato, Modelo de Priorização e Maturidade, foi utilizado o questionário exibido no Apêndice H, concebido a partir do trabalho de Salah, Paige e Cairns (2014).

O questionário para avaliação do artefato foi enviado para 14 possíveis especialistas, sendo respondido por seis, conforme descrição apontada no Quadro 10.

A avaliação do artefato pelos especialistas, quanto aos critérios pesquisados, pode ser vista no Quadro 11. Pelas respostas percebeu-se a concordância dos especialistas ao modelo apresentado. Com exceção de um especialistas (E1) que discordou ao ser questionado se "Os níveis de maturidade são suficientes para representar todos os estágios de maturidade do domínio em questão". Bem como apontou como neutra (nem concordou, nem discordou) quando questionado se "Os controles são corretamente atribuídos ao seu respectivo nível de maturidade".

Tal fato pode ser justificado pela resposta dada a questão Q1 do mesmo documento. Ao ser questionado: "Você adicionaria algum nível ou estágio de maturidade?" o especialista E1 apontou a necessidade de inserir mais um nível:

E1: "Acredito que apenas 3 níveis não é adequado. Recomendo 4. Com 3, os estágios ficam muito densos, difícil de se atingir e desestimula".

Outro especialista (E4) também comentou nesta questão:

E4: "3 Estágios parece ser pouco, o mais habitual são 4 ou 5".

Os demais especialistas, quatro, não adicionaram alterações neste quesito.

Com relação à questão Q2, "Você atualizaria a descrição do nível de maturidade?", todos os seis concordaram com o modelo atual. Um especialistas inseriu que:

E1: "A utilização dos níveis do COBIT é interessante e uma prática já consolidada. Não cabendo alteração".

Com relação à questão Q3, "Você adicionaria algum controle?", houve uma resposta semelhante ao item anterior. Todos os seis concordaram com o modelo atual. Um especialistas inseriu que:

E1: "Foi utilizado os controles da ISO, mundialmente utilizados".

Quadro 10 – Dados Especialistas - Avaliação Artefato Versão 2

	Esp. 1	**Esp. 2**	**Esp. 3**	**Esp. 4**	**Esp. 5**	**Esp. 6**
Experiência com TIC (anos)	25	27	18	22	20	15
Experiência com segurança (anos)	15	20	6	18	10	15
Trabalha em empresa de segurança	Sim	Não	Sim	Sim	Não	Não
Maior cargo assumido	Sócio-diretor	Diretor	Diretor de Tecnologias	Diretor Técnico	Gerente de Segurança da Informação	Analista Sênior de Segurança
Tempo no maior cargo (anos)	20	4	6	12	7	6
Maior titulação	Mestrado	Doutorado	Especialização	Especialização	Mestrado	Especialista
Titulação em andamento	-	-	-	-	-	Mestrado
Titulação na área de segurança	Mestrado	Doutorado	Especialização	Especialização	Especialização	Especialização
Tem experiência com maturidade	Sim	Sim	Sim	Não	Sim	Sim
Quantidade de publicações acadêmicas	Mais que 7	Mais que 7	Entre 1 e 3	Entre 1 e 3	Entre 4 e 7	Entre 1 e 3
Quantas delas em segurança	Mais que 7	Mais que 7	Entre 1 e 3	Entre 1 e 3	Entre 4 e 7	Entre 1 e 3
Certificações na área de TIC	Entre 1 e 3	0	Entre 4 e 7	Mais que 7	Entre 4 e 7	Mais que 7
Quantas delas em segurança	Entre 1 e 3	0	Entre 1 e 3	Mais que 7	Entre 1 e 3	Mais que 7
Experiência no ensino em TIC	Palestrante e Professor em Graduação e Especialização	Palestrante, Professor e Coordenador em Graduação, Mestrado e Doutorado	Professor em Graduação	Palestrante em Graduação e Especialização	Professor em Especialização	Professor em Graduação e Especialização
Experiência no ensino em segurança	Palestrante e Professor em Graduação e Especialização	Palestrante e Professor em Graduação, Mestrado e Doutorado	Professor em Graduação	Palestrante em Graduação e Especialização	Professor em Especialização	Professor em Graduação e Especialização
Tempo de experiência no ensino de TIC	15	25	10	8	15	10
Quanto deste tempo em segurança	15	20	4	8	6	8

Quadro 11 – Avaliação dos Especialistas Artefato Versão 2

Critério	**Concordo Totalmente**	**Concordo**	**Neutro**	**Discordo**	**Discordo Totalmente**
Os níveis de maturidade são suficientes para representar todos os estágios de maturidade do domínio em questão	2	3		1	
Não há sobreposição detectada entre as descrições dos níveis de maturidade	6				
Os controles são relevantes para o domínio	6				
Os controles cobrem todos os aspectos impactantes / envolvidos no domínio	6				
Os controles são corretamente atribuídos ao seu respectivo nível de maturidade	3	2	1		
Os níveis de maturidade são compreensíveis	4	2			
As diretrizes de avaliação são compreensíveis	4	2			
O esquema de pontuação é fácil de usar	4	2			
As diretrizes de avaliação são fáceis de usar	3	3			
O modelo de maturidade é útil na realização de avaliações	5	1			
O modelo de maturidade é prático para uso na indústria	5	1			

Com relação às questões Q4, "Você removeria algum dos controles?", e Q5, "Você redefiniria / atualizaria algum dos controles?", todos os seis concordaram com o modelo atual e responderam não. Sem nenhum comentário posterior.

Com relação às questões Q6, Q7 e Q8, respectivamente: "Você sugeriria alguma atualização ou melhoria relacionada ao esquema de pontuação?", "Você sugeriria alguma atualização ou melhoria relacionada às diretrizes de avaliação?" e "O modelo poderia ser mais útil?", foram respondidos como "não" pelos seis especialistas. O especialista E1, mesmo não fazendo parte da questão em epígrafe, reforçou em todas os três questionamentos:

E1: "Inserir mais um estágio".

No questionamento Q8 um especialista complementou:

E2: "Poderia ser uma ferramenta web".

Com relação à questão Q9, "O modelo poderia ser mais prático?", cinco especialistas concordaram como o modelo apresentado, e um especialistas inseriu:

E5:"Teria que ver funcionando para indicar uma melhoria".

Por fim, foi apresentando a questão Q10, "Você tem mais alguma sugestão, crítica ou algo a comentar?", três respostas foram obtidas:

E1: "Deveria ter mais um estágio. O modelo também deviria incluir a gestão de riscos da empresa".

E3: "Bom".

E5: "A utilização do COBIT e da ISO é uma boa alternativa, como já os conhecemos facilita na implantação".

5.2.1.2 Publicação de Artigo

Utilizou-se, também, como forma de avaliação a submissão de artigo. Como resultado, houve uma publicação: Alencar e Moura (2018), ainda com resultados parciais, sem ter todas as repostas dos especialistas. O artigo foi aceito e o retorno recebido na fase de avaliação realizada pelos membros do comitê do programa referente ao trabalho Alencar e Moura (2018) foi de suma importância. Um dos avaliadores questionou o método utilizado para selecionar os controles em cada estágio de maturidade, utilizando apenas as médias das notas de cada controle aferida através do resultado do survey sobre os controles da ISO/IEC (Apêndice C). Neste caso, os controles com média maior do que três estariam no estágio essencial, média entre dois e três estariam no estágio avançado e os controles com média menor do que dois estaria no estágio completo, conforme descrito anteriormente.

Acontece que, conforme o avaliador apontou, a medida em que se sabe da importância de todos os controles, tende-se a ter, cada vez mais, empresas inserindo valores de importância maiores aos controles. Mesmo que não seja selecionada a nota cinco (máxima), é bem plausível que fosse inserida nota três ou quatro, podendo chegar ao ponto que todos os controles da norma em questão tenha média acima de três. Tal situação geraria um conjunto "simplificado" do mesmo tamanho da própria norma (114 controles) no estágio essencial (primeiro estágio) do modelo.

O questionamento levantado sobre a simples utilização de uma linha de base (média maior que três), que poderia não ser suficiente para o modelo, foi acatado. Não para a correção do artigo, que já tinha sido aceito e sem tempo hábil para um ajuste deste porte, mas para o caminho da pesquisa de doutorado. De fato, ao analisar a amostra alcançada por esse estudo, conforme Tabela 6, comprovou-se a hipótese. Apenas quatro controles, dos 114 da norma, não atingiram a média maior do que três.

Diante deste fator, das avaliações dos especialistas e da busca contínua pela melhoria do artefato, incluindo as orientações deste projeto, revisitas à literatura, apresentações deste trabalho e debates com especialistas da área e com o grupo de pesquisa GP2 do CIn/UFPE, o artefato foi evoluído para a Versão 3, demonstrada a seguir.

5.3 Versão 3 - Estratégia de Maturidade e Priorização da Segurança da Informação

Como uma evolução do artefato, a Versão 3 busca incorporar todas as ações que as versões anteriores já se propuseram e, ao mesmo tempo, evoluí-las de forma a atender as críticas levantadas nas avaliações.

Desta forma, a estratégia consiste, inicialmente, em classificar os 114 controles da ISO/IEC 27.001, conforme demonstrado na Versão 1 e também utilizado na Versão 2.

Após a resposta, em uma segunda fase, os controles serão classificados em quartis. Sendo esta uma das principais diferenças com relação à versão anterior. Trabalhou-se, neste momento, com quatro estágios e a divisão por percentual e não mais por uma linha base (média maior do que três para o primeiro nível, por exemplo).

Para isso, será calculada a média das notas de cada controle e ordenando-os. O primeiro quartil representa os 25% dos controles considerados mais importantes, enquanto o último quartil, apontará os 25% dos controles com menor nível de importância. Cada quartil é categorizado como "Estágio". Em uma situação ideal, os controles estariam distribuídos, conforme mostrado no Quadro 12.

Quadro 12 – Estratificação dos Controles de Acordo com sua Importância - Artefato Versão 3 - Divisão Teórica - Inicial

Média do Controle	**1º Quartil (maiores médias)**	**2º Quartil**	**3º Quartil**	**4º Quartil (menores médias)**
Estágio	Essencial	Intermediário	Avançado	Completo
Controles	29	28	29	28

Porém a divisão dos quartis pode não ser tão exata. Pois, assim como aconteceu nas versões anteriores, após a classificação dos controles, uma análise dos controles pré-requisitos é realizada e, caso o controle pré-requisito não esteja no mesmo estágio ou em um estágio anterior do que o controle que o tem como pré-requisito, o controle pré-requisito é inserido no referido estágio.

Um quartil também pode ter a quantidade de controles aumentadas caso exista empate nas notas dos últimos controles, sendo todos incorporados ao quartil. Por exemplo, se os controles das posições 27, 28, 29 e 30 tiverem a mesma média, todos serão incorporados ao 1º quartil, tendo, neste caso, o 1º quartil com 31 controles no lugar dos 29 iniciais (Quadro 12).

Assim como detalhado na Versão 2 do artefato, cada estágio é composto por um conjunto de controles, ordenados pelo nível de importância dado pelas empresas e a análise de seu pré-requisitos. Estes controles são avaliados e classificados de acordo com a definição dos seis níveis de maturidade do COBIT (Quadro 5), como exibido na Figura 34. Sendo verificado o nível de cada controle aplicável à empresa no estágio em questão.

Figura 34 – Estágios e Níveis de Maturidade - Artefato Versão 3

Fonte: autor.

Nesta proposta, a mensuração mais baixa dada a empresa é o Estágio Essencial e nível 1 (Inicial) ou Essencial 1. Já a mensuração mais alta é o quando se atinge o Estágio Completo e o Nível 5 (Otimizado) ou Completo 5.

Na Versão 2, a empresa estará apta a passar de estágio quando todos os controles aplicáveis do estágio atual atingirem, ao menos, o nível 3 (processo definido). Nesta versão, existem duas formas de aplicação. A primeira, para aferir a maturidade, utiliza a mesma nota 3 como linha de base para que os controles atinjam e, com isso, a empresa mude de estágio.

Após o levantamento e ordenação dos controles mais importantes, análise e, se necessário, inclusão dos controles pré-requisitos, entendimento dos quatro estágios e de seus cinco níveis deve ser visto o nível mínimo para se alcançar e estar apto a passar de estágio.

A definição do nível mínimo de maturidade para cada controle pode ser calculada de duas formas. Uma forma é elencar um padrão, por exemplo, todos os controles deverão alcançar, no mínimo, o nível 3 (definido). Uma outra opção, é realizar uma análise de risco de segurança da informação na empresa, como sugere a ISO/IEC 27005, e categorizar o nível mínimo de cada controle de acordo com a probabilidade e impacto do risco inerente à aplicação do referido controle.

Para esta estratégia, a probabilidade e o impacto serão categorizados como baixo, médio ou alto. Recebendo, respectivamente, o peso 1, 2 ou 3. Uma matriz é formada e o valor mínimo de maturidade a ser alcançado será a soma da nota da probabilidade e do impacto, conforme Figura 35.

Uma exceção é quando se atinge uma probabilidade e impacto altos, recebendo a nota 6 (3+3). Ciente que o modelo proposto aborda até o nível de Maturidade 5 (otimizado), os controles categorizados com nota 6 deverão atingir o Nível 5 (otimizado) e, por sua criticidade, deverão ser tratados, dentro de seu estágio, de forma prioritária pela empresa.

Desta forma, os controles nos quais ausências geram riscos com maior probabilidade e maior impacto deverão ser tratados de forma diferenciada, com um nível de maturidade

Figura 35 – Nível de Maturidade Mínimo de Acordo com o Impacto e Probabilidade

Probabilidade	Baixo (1)	Médio (2)	Alto (3)
Alta (3)	4 - Gerenciado	5 - Otimizado	6 - Otimizado
Média (2)	3 – Definido	4 - Gerenciado	5 - Otimizado
Baixa (1)	2 - Repetível	3 – Definido	4 - Gerenciado

Impacto

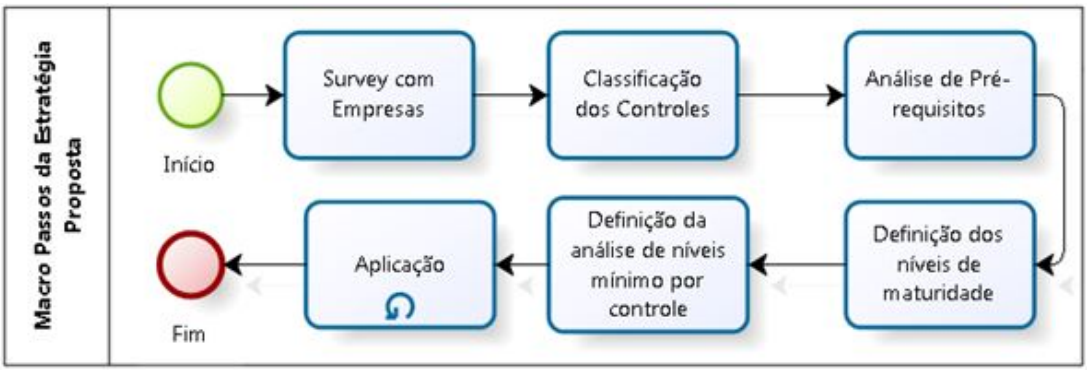
Fonte: autor.

superior.

Os controles não aplicáveis deverão ser devidamente justificados no relatório a ser apresentado no final da avaliação e terão como nível mínimo o 0 (inexistente) não sendo contabilizados na estratégia.

De forma sintetizada, os passos da estratégia proposta nesta Versão 3 do artefato, podem ser vistos na Figura 36.

Figura 36 – Macro Passos da Estratégia - Artefato Versão 3



Fonte: autor.

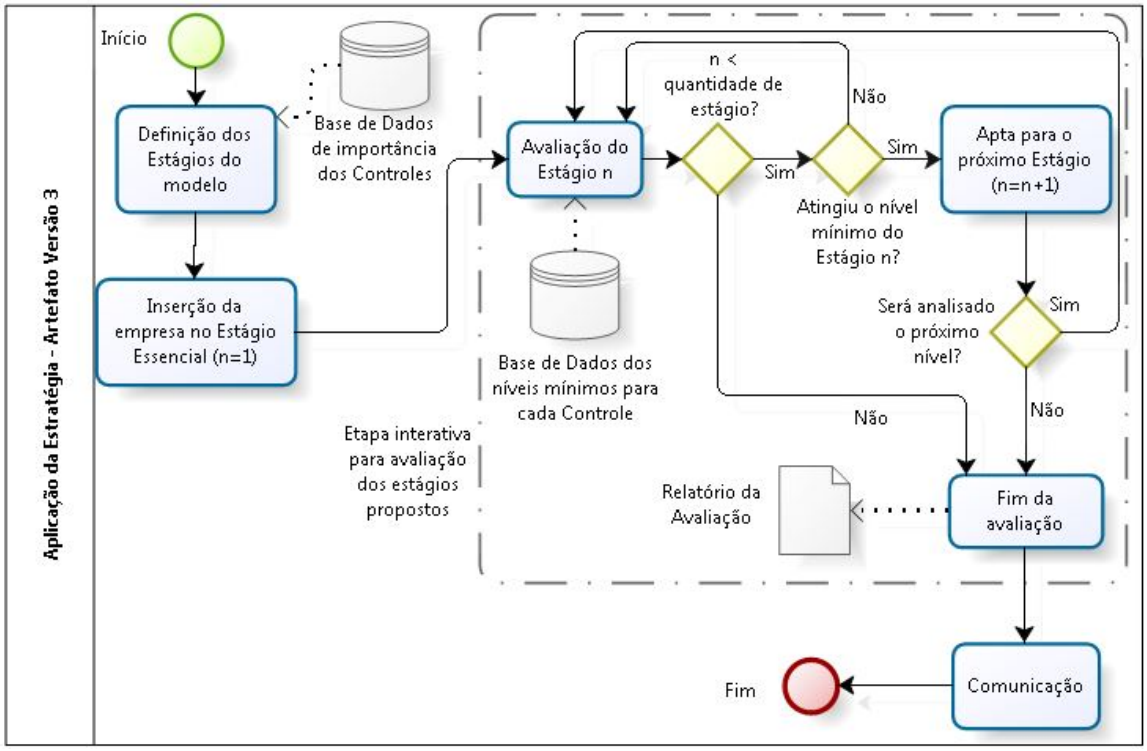
A fase de aplicação da estratégia consiste em analisar e aplicar cada controle ordenado nos estágios até o estágio pretendido, conforme Figura 37.

Portanto, a estratégia proposta pode ser aplicada de duas formas, denominadas de "Modelo de Maturidade Comparável" e de "Aplicação Independente". Torna-se necessário dividir essas formas de aplicação diante das duas possibilidades de se escolher o nível mínimo de cada controle que, consequentemente, direciona o esforço necessário para se alcançar o próximo estágio. As duas formas de aplicações são detalhadas a seguir.

5.3.1 Separação dos Controles por Quartis e Criação dos Estágios

Para verificar quais controles da ISO/IEC 27.001 e 27.002 são os mais importantes, foi realizada um survey, cujo resultado já foi exibido no Capítulo 4.

Figura 37 – Fase de Aplicação da Estratégia - Artefato Versão 3



Fonte: autor.

Com o levantamento feito, inicia-se, de fato, a construção dos estágios (quartis). Para isso as seguintes etapas devem ser realizadas:

i Ordenação dos controles de forma decrescente de acordo com a média das notas (Tabela 6);

ii Selecionar a quantidade de controles de cada estágio (Quadro 12);

iii Verificar possíveis empates nas últimas notas dos controles, inserindo-os no estágio anterior;

iv Verificar possíveis pré-requisitos dos controles (Quadro 8) e, caso o pré-requisito não esteja no estágio atual ou em algum anterior, inseri-lo no estágio atual.

Com base na média das notas respostas das empresas alcançadas, as etapas foram realizadas. A Tabela 6 demonstra o resultado da etapa i. A numeração dos controles está de acordo com a exibida no Anexo A da ISO/IEC 27.001.

O Quadro 13 demonstra o resultado da execução da etapa ii. Nesta etapa, o estágio Essencial recebe os controles nas posições 1 até 29, o estágio Intermediário recebe os controles nas posições 30 até 57, o estágio Avançado recebe os controles nas posições 58 até 86 e o estágio Completo recebe os controles nas posições 87 até 114.

Quadro 13 – Controles Separado por Estágio - Etapa ii

Estágio	**Quantidade de Controles**	**Controles**
Essencial	29	A.5.1.1, A.6.1.1, A.6.1.5, A.6.2.2, A.7.1.1, A.7.2.1, A.8.1.2, A.8.2.1, A.8.2.3, A.9.1.2, A.9.2.1, A.9.2.3, A.9.2.4, A.9.2.5, A.9.4.2, A.9.4.4, A.11.1.5, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.12.6.2, A.13.1.3, A.15.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 e A.18.1.5
Intermediário	28	A.5.1.2, A.6.1.2, A.6.2.1, A.7.2.2, A.8.1.1, A.8.1.3, A.8.3.1, A.9.2.6, A.9.4.3, A.11.1.3, A.11.2.2, A.11.2.3, A.12.1.3, A.12.1.4, A.12.2.1, A.12.5.1, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.1, A.14.2.6, A.15.1.1, A.16.1.1, A.16.1.2, A.16.1.5, A.16.1.7, A.17.1.1 e A.18.2.2
Avançado	29	A.7.2.3, A.8.1.4, A.8.2.2, A.9.1.1, A.9.3.1, A.9.4.1, A.9.4.5, A.11.1.1, A.11.1.2, A.11.2.1, A.11.2.9, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.6.1, A.12.7.1, A.13.1.2, A.13.2.4, A.14.1.2, A.14.1.3, A.14.2.5, A.14.2.9, A.15.1.2, A.16.1.3, A.16.1.4, A.17.2.1, A.18.2.1 e A.18.2.3
Completo	28	A.6.1.3, A.6.1.4, A.7.1.2, A.7.3.1, A.8.3.2, A.8.3.3, A.9.2.2, A.10.1.1, A.10.1.2, A.11.1.4, A.11.1.6, A.11.2.8, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.2, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.7, A.14.2.8, A.14.3.1, A.15.2.1, 15.2.2, A.16.1.6, A.17.1.2 e A.17.1.3

A etapa iii consiste na análise de possíveis controles empatados no final de cada estágio. Analisando a Tabela 6, verificou-se:

- O último controle do estágio essencial (posição 29) foi o A.18.1.2, com média das notas 3,52. Estando empatado com os controles A.8.1.3 e A.12.5.1 (posições 30 e 31);
- O último controle do estágio intermediário (posição 57) foi o A.16.1.2, com média das notas 3,25. Estando empatado com o controle A.16.1.4 (posição 58).
- O último controle do estágio avançado (posição 86) foi o A.14.1.3, com média das notas 3,09. Estando empatado com o controle A.15.2.1 (posição 87).

Executando a atividade da etapa iii, os controles empatados foram incluídos nos estágios, resultando na organização exposta no Quadro 14.

A última etapa para separação dos controles e criação dos estágios (etapa iv), consiste em verificar possíveis pré-requisitos dos controles e enquadrá-los devidamente. Conforme inserido no Quadro 8, foram elencados 14 controles que necessitam de pré-requisitos. Apenas um controle ainda não tinha sido contemplado, como detalhado no Quadro 15.

Quadro 14 – Controles Separado por Estágio - Etapa iii

Estágio	**Quantidade de Controles**	**Controles**
Essencial	31	A.5.1.1, A.6.1.1, A.6.1.5, A.6.2.2, A.7.1.1, A.7.2.1, A.8.1.2, A.8.1.3 A.8.2.1, A.8.2.3, A.9.1.2, A.9.2.1, A.9.2.3, A.9.2.4, A.9.2.5, A.9.4.2, A.9.4.4, A.11.1.5, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.12.5.1, A.12.6.2, A.13.1.3, A.15.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 e A.18.1.5
Intermediário	27	A.5.1.2, A.6.1.2, A.6.2.1, A.7.2.2, A.8.1.1, A.8.3.1, A.9.2.6, A.9.4.3, A.11.1.3, A.11.2.2, A.11.2.3, A.12.1.3, A.12.1.4, A.12.2.1, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.1, A.14.2.6, A.15.1.1, A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.7, A.17.1.1 e A.18.2.2
Avançado	29	A.7.2.3, A.8.1.4, A.8.2.2, A.9.1.1, A.9.3.1, A.9.4.1, A.9.4.5, A.11.1.1, A.11.1.2, A.11.2.1, A.11.2.9, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.6.1, A.12.7.1, A.13.1.2, A.13.2.4, A.14.1.2, A.14.1.3, A.14.2.5, A.14.2.9, A.15.1.2, A.15.2.1 A.16.1.3, A.17.2.1, A.18.2.1 e A.18.2.3
Completo	27	A.6.1.3, A.6.1.4, A.7.1.2, A.7.3.1, A.8.3.2, A.8.3.3, A.9.2.2, A.10.1.1, A.10.1.2, A.11.1.4, A.11.1.6, A.11.2.8, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.2, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.7, A.14.2.8, A.14.3.1, 15.2.2, A.16.1.6, A.17.1.2 e A.17.1.3

Por fim, o resultado final da separação dos controles em quartis e criação dos estágio pode ser vista no Quadro 16. Esta consolidação mostrada no Quadro 16 representa a base de dados de importância dos controles exibida na Figura 37.

Periodicamente, a princípio anualmente ou antes caso as empresas percebam tal necessidade, os controles de cada estágio deverão ser recalculados, devido a possibilidade de novas respostas ao modelo, aumentando a base de dados e representando a real importância de cada controle. Fato que confere um dinamismo ao modelo, sendo mais um diferencial aos já existentes. Bem como incorporando à estratégia os princípios do método iterativo de gestão PDCA (Plan, Do, Check e Act).

5.3.2 Modelo de Maturidade Comparável

Para ser possível a medição da maturidade e comparação entre as empresas mensuradas torna-se necessário um modelo padrão, de forma a se comparar questões iguais. Os modelos de maturidade em segurança da informação, como já mencionados durante o trabalho, utilizam, por exemplo, os controles da ISO/IEC 27.001 ou 27.002 medindo-os e classificado a maturidade, normalmente, com a média dos valores medidos. Tendo todos os controles o mesmo peso.

Como um diferencial da presente estratégia, o modelo de maturidade proposto trabalha com estágios e níveis de maturidades. Nos estágios estão classificados os controles por

Quadro 15 – Análise dos Controles Pré-requisitos por Estágio - Etapa iv

Controle	**Estágio**	**Pré-requisito**	**Estágio**	**Ação**
A.5.1.2	Intermediário	A.5.1.1	Essencial	nenhuma
A.8.2.2	Avançado	A.8.2.1	Essencial	nenhuma
A.8.2.3	Essencial	A.8.2.1	Essencial	nenhuma
A.8.3.1	Intermediário	A.8.2.1	Essencial	nenhuma
A.9.4.1	Avançado	A.9.1.1	Avançado	nenhuma
A.9.4.2	Essencial	A.9.1.1	Avançado	Inserir o controle A.9.1.1 no estágio Essencial
A.11.1.2	Avançado	A.11.1.1	Avançado	nenhuma
A.12.4.2	Completo	A.12.4.1	Avançado	nenhuma
A.17.1.2	Completo	A.17.1.1	Intermediário	nenhuma
A.17.1.3	Completo	A.17.1.2	Completo	nenhuma
A.18.1.2	Essencial	A.18.1.1	Essencial	nenhuma
A.18.1.3	Essencial	A.18.1.1	Essencial	nenhuma
A.18.1.4	Essencial	A.18.1.1	Essencial	nenhuma
A.18.1.5	Essencial	A.18.1.1	Essencial	nenhuma

quartis, de acordo com a importância dada a eles pelas empresas. E a empresa só será avaliada no segundo quartil ao atender o nível mínimo dos controles do estágio anterior. Nesta nova configuração, os controles mais importantes serão inseridos de forma prioritária. O modelo de maturidade proposto tem seus estágios e níveis apresentados na Figura 34. E o resultado final da organização dos controles na amostra pesquisada foi demonstrado no Quadro 16, priorizando os controles por estágios de acordo com a importância dada pelas empresas e analisando seus pré-requisitos.

No modelo proposto, para se passar de um estágio (Essencial, Intermediário, Avançado ou Completo) para o seguinte só é possível após atingir o nível de maturidade mínimo de 3 (nível definido) para todos os controles, sendo este o parâmetro da base de dados dos níveis mínimo para cada controle (Figura 37). Ou seja, se a empresa é categorizada como Avançada Nível 2, significa que a média dos controles do grupo Avançado obteve o nível de maturidade 2 (Repetível) e que todos os controles aplicáveis do estágio Essencial e do Intermediário foram mensurados, no mínimo, como nível 3 (Definido). Sendo um diferencial do modelo proposto.

5.3.3 Aplicação Independente

A aplicação independente da estratégia visa o atendimento das empresas que estão em busca da implantação da segurança da informação e necessitam de uma estratégia que se adeque à sua empresa, não necessitando, neste momento, utilizar o padrão de melhores práticas apontados no modelo de maturidade comparável (Seção 5.3.2).

Esta ação consiste em aplicar a estratégia já mencionada (Figuras 34, 36 e 37). Porém a Base de dados de importância dos controles (Figura 37), não será a apresentada no

Quadro 16 – Controles Separado por Estágio - Etapa iv

Estágio	**Quantidade de Controles**	**Controles**
Essencial	32	A.5.1.1, A.6.1.1, A.6.1.5, A.6.2.2, A.7.1.1, A.7.2.1, A.8.1.2, A.8.1.3 A.8.2.1, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.3, A.9.2.4, A.9.2.5, A.9.4.2, A.9.4.4, A.11.1.5, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.12.5.1, A.12.6.2, A.13.1.3, A.15.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 e A.18.1.5
Intermediário	27	A.5.1.2, A.6.1.2, A.6.2.1, A.7.2.2, A.8.1.1, A.8.3.1, A.9.2.6, A.9.4.3, A.11.1.3, A.11.2.2, A.11.2.3, A.12.1.3, A.12.1.4, A.12.2.1, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.1, A.14.2.6, A.15.1.1, A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.7, A.17.1.1 e A.18.2.2
Avançado	28	A.7.2.3, A.8.1.4, A.8.2.2, A.9.3.1, A.9.4.1, A.9.4.5, A.11.1.1, A.11.1.2, A.11.2.1, A.11.2.9, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.6.1, A.12.7.1, A.13.1.2, A.13.2.4, A.14.1.2, A.14.1.3, A.14.2.5, A.14.2.9, A.15.1.2, A.15.2.1 A.16.1.3, A.17.2.1, A.18.2.1 e A.18.2.3
Completo	27	A.6.1.3, A.6.1.4, A.7.1.2, A.7.3.1, A.8.3.2, A.8.3.3, A.9.2.2, A.10.1.1, A.10.1.2, A.11.1.4, A.11.1.6, A.11.2.8, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.2, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.7, A.14.2.8, A.14.3.1, 15.2.2, A.16.1.6, A.17.1.2 e A.17.1.3

Quadro 16, mas sim uma análise da aplicação do mesmo survey (questões acerca da importância de cada controle) dentro da própria empresa com os stakeholders.

A Base de Dados dos níveis mínimo para cada Controle (Figura 37) será montada conforme a avaliação de risco referente à aplicação de cada controle, de acordo com a matriz apresentada na Figura 35.

Desta forma temos a aplicação da mesma estratégia, porém adaptada ao ambiente e necessidades da empresa. Tal fato segue a linha de pensamento da governança ágil, em especial seus meta-valores que apontam (LUNA et al., 2016):

- Comportamento e prática do que processos e procedimentos;
- Alcançar a sustentabilidade e a competitividade do que ser auditada para estar em conformidade;
- Transparência e envolvimento das pessoas com a empresa do que monitoramento e controle;
- Sentir, adaptar e responder do que seguir um plano.

Nesta aplicação a empresa está moldando o processo ao seu negócio e não o contrário para ser comparada com outras, buscando atingir seus objetivos, priorizar suas ações em segurança da informação, bem como promover definições básicas para o tratamento

dos controles, tendo parâmetros para definição dos investimento e funcionando com um alinhamento da segurança da informação ao negócio, podendo ser visto como governança da segurança da informação, que apoia a governança de TIC que, por fim, incorpora à governança corporativa.

Importante ressaltar que este modo de aplicação não é totalmente comparável entre empresas para classificá-las. Visto que os controles selecionados em cada estágio, a quantidade de controles em cada estágio, como também o nível mínimo por controle podem ser diferentes. Porém, a nota e análise de cada controle de cada empresa pode ser inserido em um modelo padrão (modelo de maturidade comparável - Seção 5.3.2), fazendo com que exista a possibilidade de comparação entre os entes desejados sem grandes esforços.

5.3.4 Avaliação da Versão 3

Como método de avaliação desta versão, foram executadas três ações:

- Aplicação em caso real;
- Submissão de artigo;
- Realização de grupo focal com especialistas.

Cada uma das ações, por ordem cronológica de execução, serão detalhas a seguir.

5.3.4.1 Aplicação em Caso Real

Para verificar a funcionalidade da estratégia elaborada, foi feita uma aplicação real da estratégia para uma empresa brasileira, neste trabalho apresentada como Empresa A.

A Empresa A tem mais de 40 anos no mercado, atuando no segmento industrial e comercial. Tem sua sede em Recife, Pernambuco, e filial no estado do Rio Grande do Norte. Seus produtos são comercializados em todo território nacional. Com aproximadamente 120 colaboradores, tem uma equipe de TIC de 5 pessoas e um dos atuais sócios tem formação na área de TIC.

Em contato com a Empresa A, a mesma optou pela aplicação independente da estratégia (conforme descrita na Seção 5.3.3). Nesta aplicação a empresa está moldando o processo ao seu negócio e não o contrário para ser comparada com outras, buscando atingir seus objetivos, priorizar suas ações em segurança da informação, bem como promover definições básicas para o tratamento dos controles, tendo parâmetros para definições dos investimento e funcionando com um alinhamento da segurança da informação ao negócio, podendo ser visto como Governança da Segurança da Informação, que apoia a governança de TIC que, por fim, incorpora a governança corporativa.

O survey para definição da importância de cada controle foi respondido por sete funcionários, sendo 3 da área de TIC e 4 gerentes e diretores de outras áreas. Com as respostas

foi calculada a média de importância de cada controle, seguindo a mesma metodologia já exposta.

A divisão dos controles por níveis apontou alteração em onze controles ao comparar com base exposta no Quadro 16. Três controles por exclusão (não aplicável à empresa), sendo eles: "A.14.2.1 - Política de desenvolvimento seguro", "A.14.2.6 - Ambiente seguro para desenvolvimento" e "A.14.2.7 - Desenvolvimento terceirizado" e 8 por categorização diferente, conforme detalhado no Quadro 17.

Quadro 17 – Empresa A x Base de Controles

Controle	**Estágio na Base de Dados (Exibido no Quadro 16)**	**Estágio na Base de Dados Empresa A**
A.5.1.2	Intermediário	Essencial
A.6.1.2	Intermediário	Essencial
A.6.1.5	Essencial	Intermediário
A.6.2.2	Essencial	Completo
A.7.1.1	Essencial	Avançado
A.7.2.3	Avançado	Completo
A.11.1.2	Avançado	Intermediário
A.18.1.4	Essencial	Intermediário

Com as alterações expostas a Estratégia da Empresa A resultou em 29 controles no estágio Essencial, 27 no Intermediário, 28 no Avançado e 27 no Completo.

A Empresa A tinha realizado, 4 meses antes, uma análise de riscos interna, baseada na ISO/IEC 27.005. O relatório desta ação serviu como insumos para os respondentes definirem a pontuação de cada controle e, principalmente, para definir o nível mínimo de cada controle, conforme matriz proposta (Figura 35). Com as duas Bases de Dados formadas (controles e nível mínimo) a estratégia foi seguida, conforme Figuras 36 e 37.

A empresa atendeu a todos os critérios mínimos dos controles Essenciais, resultando em uma maturidade medida no estágio de 3,49, estando apta ao próximo estágio. Nos controles Intermediários resultou em uma maturidade média de 3,30, por ter atendido ao nível mínimo em todos os controles, habilitou-se ao próximo estágio.

No estágio Avançado a empresa atingiu uma maturidade média de 3,07. Porém, não atingiu o nível mínimo em dois controles: "A.9.3.1 - Uso da informação de autenticação secreta", que alcançou nível 3 (Definido) e a matriz de Riscos tinha apontado com critério mínimo o nível 4 (Gerenciado), e o controle "A.14.1.3 - Protegendo as transações nos aplicativos de serviços", que alcançou nível 2 (Repetível) e a matriz de Riscos tinha apontado com critério mínimo, também, o nível 4 (Gerenciado).

Por não ter completado o Estágio Avançado, a empresa não avançou ao Estágio Completo. A Empresa A teve seu nível de maturidade geral, definido como Estágio Avançado, Nível de Maturidade 3,07 (Definido) ou, de forma mais direta, Avançado - 3,07.

A empresa optou pela estratégia de aplicação independente (Seção 5.3.3), por não ter uma necessidade institucional de uma certificação de sua maturidade ou comparar-se com

as demais. Acrescentando que a estratégia independente permitiu à Empresa desenhar uma forma de direcionar seus recursos aos controles mais críticos ao seu negócio, fato que ficou evidenciado no relatório de avaliação para comunicação aos stakeholders, visto que alguns controles do estágio completo, ou seja, não categorizado com crítico ao negócio, apontou nível de Maturidade 5, enquanto alguns controles de estágios anteriores, mais críticos, estavam em Nível 2 (Repetível). Demonstrando que, possivelmente, esforços e recursos foram direcionados para ações não prioritárias no momento.

A reunião final de entrega do relatório e explanação sobre a estratégia adotada foi realizada entre o autor da pesquisa e onze integrantes da empresa, incluindo seis dos sete respondentes da pesquisa. Tal ação servia para a empresa como forma de retorno do trabalho realizado e, para o pesquisador, como meio de avaliação da ferramenta. Neste sentido, a equipe da empresa presente na reunião ficaram espantados com o investimento realizado em ações não prioritárias, mas concordaram com o resultado. O responsável pela área de TIC e de segurança da informação afirmou que a metodologia proposta é trabalhosa, mas não é difícil, tem baixo custo e aponta resultados interessantes.

Caso a empresa optasse pela estratégia do Modelo de Maturidade Comparável (Seção 5.3.2), sendo analisada conforme descrição dos controles do Quadro 16, estaria categorizada no Estágio Intermediário, com nível de maturidade 3,42 (Definido). Mesmo obtendo níveis de Maturidade 5 (Otimizado) em alguns controles, inclusive do último estágio (Completo), a empresa teve dois controles com nível de Maturidade 2 (Repetível) no estágio intermediário, não atingindo o nível mínimo 3 e, consequentemente, não completando este segundo estágio. Mas que pela análise da aplicação independente, correlacionada pela matriz de risco, foi suficiente na aplicação independente.

Fazendo uma média geral dos controles, como é realizado na maioria dos trabalhos, inclusive na maioria dos trabalhos correlatos, a Empresa A estaria inserida com nível de maturidade 3,22, nível Definido. Apesar de ser o mesmo nível apontado pelas duas estratégias propostas neste trabalho, acredita-se que a presente proposta seja mais rica, visto que aponta diferenças para um mesmo nível de maturidade. Deixando claro que uma empresa estágio Essencial, nível de maturidade 3,3 está em um patamar bem abaixo de uma empresa estágio Completo, nível de maturidade 3,3. Mesmo ambas podendo ter o mesmo nível de maturidade se calculado pelos moldes tradicionais (média simples dos níveis de cada controle), ao estar em um estágio mais avançado, aponta para o atendimento ordenado de controles mais importantes ao negócio.

5.3.4.2 Publicação de Artigo

Utilizou-se, também, a submissão de artigo como forma de avaliação. Como resultado, houve uma publicação: Alencar et al. (2018a). Tal publicação pode ser considerada a mais relevante para esta pesquisa por:

- Apontar a versão completa do artefato;
- Ser em uma revista internacional de maior visibilidade e impacto;
- Ter a classificação Qualis B1 na área de ciência da computação na avaliação vigente da Capes e atendendo aos pré-requisitos do Programa de Pós-graduação em Ciência da Computação do CIn/UFPE.

O trabalho foi avaliado em nove critérios com possibilidade de pontuação entre zero e dez. Mesmo não sendo possível abordar detalhadamente a pesquisa, como neste documento, devido aos limites de escopo e número de páginas, o trabalho recebeu nota igual ou superior a oito em todos os itens. Destaca-se as seguintes avaliações:

- Qualidade do conteúdo (0-10): 9;
- Contribuição e originalidade (0-10): 9;
- Nível de Inovação (0-10): 8;
- Recomendação global decisiva (0-10): 9.

A comissão avaliadora da revista enalteceu a relevância do tópico e a utilização de arcabouços já consolidados como o COBIT e os normativos ISO/IEC 27.001 e 27.002. Um outro ponto levantado pela comissão foi a possibilidade de adaptação do modelo às necessidades das empresas, devendo ser explorada e evidenciada essa questão. Inclusive o parecer final recomendou, para este ponto, a análise quanto à possibilidade de alteração do título do artigo, evidenciando a adaptabilidade do mesmo.

5.3.4.3 Realização de Grupo Focal com Especialistas

O planejamento da etapa de grupo focal proposta para avaliar o presente artefato, estratégia de priorização e maturidade da segurança da informação, está descrita no Apêndice I.

Ressalta-se a dificuldade, nos dias atuais, de se conseguir encontrar especialistas com disponibilidade em participar de tais ações, bem como de compatibilizar a agenda para encontrar um horário possível para todos do grupo, além das possíveis eventualidades. Na presente pesquisa, depois de um árduo esforço, foi possível encaixar o horário, interesse e disponibilidade com oito especialistas. Este número estava confirmado até a noite anterior do evento. Quando um especialista afirmou a sua impossibilidade de participação por questões de saúde e, no dia da sessão, outro especialista também não participou por problemas de saúde com familiar. Diante dos fatos, o grupo focal foi realizado com seis especialistas, conforme descrição exposta no Quadro 18.

Quadro 18 – Dados Especialistas - Grupo Focal

	Esp. 1	**Esp. 2**	**Esp. 3**	**Esp. 4**	**Esp. 5**	**Esp. 6**
Experiência com TIC (anos)	20	22	18	10	20	6
Experiência com segurança (anos)	10	18	8	9	12	4
Trabalha em empresa de segurança	Não	Sim	Sim	Sim	Não	Não
Maior cargo assumido	Diretor de TIC	Diretor Técnico	Diretor Executivo (CEO)	Gerente de Segurança da Informação	Chefe do Núcleo de Segurança da Informação	Analista de Segurança
Tempo no maior cargo (anos)	2	12	5	2	7	2
Maior titulação	Mestrado	Especialização	Mestrado	Mestrado	Mestrado	Mestrado
Titulação em andamento	Doutorado	-	-	-	-	Doutorado
Titulação na área de segurança	Especialização e Mestrado	Especialização	Especialização e Mestrado	Mestrado	Especialização e Mestrado	Especialização e Mestrado
Tem experiência com maturidade	Sim	Não	Sim	Não	Sim	Sim
Quantidade de publicações acadêmicas	Mais que 7	Entre 1 e 3	Mais que 7	Entre 1 e 3	Mais que 7	Entre 4 e 7
Quantas delas em segurança	Entre 4 e 7	Entre 1 e 3	Entre 4 e 7	Entre 1 e 3	Mais que 7	Entre 4 e 7
Certificações na área de TIC	Entre 4 e 7	Mais que 7	Entre 4 e 7	0	0	Entre 1 e 3
Quantas delas em segurança	Entre 1 e 3	Mais que 7	Entre 1 e 3	0	0	Entre 1 e 3
Experiência no ensino em TIC	Palestrante, Professor e Coordenador em Graduação e Especialização	Palestrante em Graduação e Especialização	Palestrante e Professor em Graduação e Especialização	Palestrante e Professor em Especialização	Palestrante e Professor em Graduação e Especialização	Palestrante e Professor em Graduação
Experiência no ensino em segurança	Palestra e Professor em Graduação e Especialização	Palestrante em Graduação e Especialização	Palestrante e Professor em Graduação e Especialização	Palestrante e Professor em Especialização	Palestrante e Professor em Graduação e Especialização	Palestrante e Professor em Graduação
Tempo de experiência no ensino de TIC	10	8	10	6	10	4
Quanto deste tempo em segurança	8	8	8	6	7	4

Tais fatos devem ser previstos como possíveis riscos no planejamento do grupo focal. Nesta pesquisa, por estar prevista a realização com o número máximo (oito), foi possível suportar as duas perdas sem alteração do método proposto.

A quantidade de seis especialistas, menor do que os oito inicialmente propostos, mas dentro da quantidade prevista no método, tem o lado negativo de se obter uma menor quantidade de vieses ou pensamentos. Por outro lado, por se ter um grupo menor, alguns debates foram mais rápidos, sendo possível tratar de mais temas ou fazer mais perguntas de cobertura (MUNARETTO; CORRÊA; CUNHA, 2013).

A utilização de arcabouços já consolidados na elaboração da estratégia, como COBIT e normas da ISO/IEC, gerou um consenso mais rápido dos especialistas em determinados questionamentos propostos pelo moderador. Tal fato serviu como confirmação para a utilização dos mesmos. E, consequentemente, também favoreceu o debate de uma quantidade maior de assuntos no período da sessão.

A sessão do grupo focal estava prevista para duas horas e teve tempo de realização de 1 hora e 45 minutos. A sessão foi gravada em áudio, com a devida permissão dos especialistas, conforme termo específico (Apêndice A). Posteriormente os áudios foram transcritos e analisados. Seus principais pontos são apresentados a seguir.

Após a etapa inicial de apresentações, conforme Apêndice I, iniciou-se a discussão com os especialistas. Ao apresentar a estratégia, o Especialista 3 apontou que a estratégia proposta em quartis, sua forma de aplicação e a utilização do COBIT e ISO estão alicerçados no PDCA. O que era de grande valia para o modelo.

O Especialista 1 falou de sua experiência na aplicação dos controles da norma ISO/IEC 27.002 em uma empresa na qual trabalhou. Mesmo com a experiência dele, da equipe e contando com uma consultoria, é árdua a atividade de implantação e das mudanças necessárias. Com esse aspecto, o Especialista 1 questionou se a estratégia proposta não seria mais uma atividade burocrática.

O Especialista 4 apontou que tentar aferir a maturidade nesse início pode ser uma atividade burocrática, mas necessária para saber onde a empresa está e depois conseguir saber o quanto se caminhou, mas que não era obrigatório. O mesmo especialista elencou que mesmo que a empresa não tenha interesse em aferir a maturidade a estratégia como artefato de priorização será bem útil. Ao final, todos concordaram com a importância da priorização, em especial, ao se começar a implantação.

Quanto à quantidade proposta de estágios, os Especialistas 1 e 3 acreditavam que poderia ser reduzida para três. Excluindo o último estágio, completo.

O Especialista 5 argumentou da granularidade proposta pela estratégia. Normalmente os modelos tem quatro, cinco ou seis níveis. A estratégia proposta, por utilizar a combinação de duas dimensões, estágios e níveis, alterou para quatro estágios, cada um com cinco níveis, formando uma escala de vinte degraus. Tal assunto foi abordado pelos especialistas como uma forma mais gradual de aferição. Sendo importante, principalmente,

para empresas de pequeno porte ou que estejam iniciando, favorecendo o planejamento e o caminho. O Especialista 4, corroborou afirmando que a maior quantidade de níveis faz com que seja mais fácil evoluir ao próximo ponto. Fato que, provavelmente, estimula a equipe e permite se olhar com maior acurácia.

Por fim, os Especialistas 2 e 4 falaram que, ao se ter 3 estágios, o primeiro estágio ficaria, possivelmente, com mais de 40 controles. Esta abordagem seria mais difícil, assustando ao começar. O Especialista 6 chegou a cogitar aumentar para cinco níveis e ser ainda mais gradual.

Após a discussão, chegou-se ao consenso de se manter quatro estágios e ter uma maior granularidade. Ao fim, todos os especialistas concordaram.

O Especialista 4 levantou a possibilidade dos controles elencados em cada estágio não ser o cenário mais interessante para a empresa em questão. Devendo propor um recorte por nicho de empresas para uma melhor adequação. Visto que os controles mais importantes estão associados ao nicho que a empresa atual, por exemplo, ele citou o setor financeiro que tem uma série de regulações e cobranças próprias. Servindo bastante para comparar sua empresa com outras empresas do mesmo nicho, por exemplo, um banco pequeno querendo saber como os bancos grandes estão. Esse ponto foi concordado por todos os especialistas, inclusive citado pelo Especialista 3 que o modelo já propõem essa possibilidade, mas que deveria ser utilizada como uma ferramenta de consultoria ou como uma ferramenta de maturidade para cada nicho e poderia perder a comparabilidade entre nichos diferentes. O Especialista 5 ressaltou que para trabalhar com nichos a base de dado tem que ter uma boa quantidade, que deve ser calculada, para se manter o nível de confiança proposto na pesquisa, fatos que não se sabe se é atendido em ferramentas comerciais que visam, principalmente, o lucro.

Durante o debate sobre os estágios da estratégia, o Especialista 5 perguntou como seria o tratamento dos controles que obtivessem notas iguais. O moderador voltou a apresentação e afirmou que a metodologia incorpora os controles com notas iguais ao estágio anterior, mais importante. O Especialista 5 perguntou qual seria o tratamento para uma lista grande de controles empatados, por exemplo, 10 controles com uma mesma nota poderia popular demasiadamente um mesmo estágio. Tal questionamento não tinha sido ainda tratado na estratégia. No debate com os especialistas, para evitar uma super população em um estágio, foi sugerida uma regra limitando o acréscimo de até 3 controles com notas iguais ao estágio, ordenando-o pela numeração do controle exposta no ISO/IEC.

O Especialista 3 questionou se o modelo não estava apenas quantificando os controles e não mensurando a maturidade. O Especialista 6 inseriu que a divisão dos controles pode ser vista como uma abordagem quantitativa, mas a sua análise através do COBIT torna a abordagem qualitativa também. Chegou-se ao consenso que existe a separação quantitativa dos controles por estágios e depois, com a análise da sua forma de aplicação de acordo com o nível do COBIT, tem-se uma abordagem qualitativa e que a existe a

possibilidade de utilização da estratégia para aferir a maturidade.

Ao debater sobre a nomenclatura utilizada, os Especialistas 3 e 6 questionaram sobre o nome do último estágio, Completo. Pensando no PDCA que é um ciclo de melhoria contínua, colocar o nome do estágio como completo pode parecer que a empresa chegou ao fim e não precisaria mais de nenhuma ação ou não teria como evoluir. Os Especialistas 4 e 5 concordaram de imediato. O Especialista 2 achou que era preciosismo, não visualizando problema algum em manter ou alterar os nomes. O Especialista 6 propôs trocar "Completo" por "Maduro". Os especialistas acreditaram que, mesmo melhorando, tinha o mesmo sentido. Ao fim, chegou-se ao consenso de alterar de Essencial, Intermediário, Avançado e Completo para Básico, Essencial, Intermediário e Avançado, proposta dos Especialistas 1 e 3.

Com relação aos níveis de maturidade, todos concordaram que o COBIT é aplicável à segurança e à estratégia proposta. A quantidade de níveis utilizadas e sua nomenclatura (Nível 0 - Inexistente, Nível 1 - Inicial, Nível 2 - Repetível, Nível 3 -Definido, Nível 4 - Gerenciado, Nível 5 – Otimizado) oriundas do COBIT, foi aprovada por consenso sem maiores debates. Após algumas perguntas de sondagem o Especialista 1 afirmou que pode se utilizar qualquer outra escala sem problemas, mas que um padrão consolidado deixa o modelo mais fácil de aplicar e com maior credibilidade. O Especialista 2 citou que não cabia ao grupo debater um modelo tão consolidado.

Ao entrar no assunto do nível mínimo para os controles, foi apresentada a proposta de utilizar o nível três, definido na estratégia. O Especialista 1 achou muito bom, pois era o nível mínimo com os procedimentos já documentos, sendo um marco fundamental para a maturidade. O Especialista 6 apoiou. O Especialista 3 ainda citou que é importante ser um nível intermediário da escala, para não ser muito fácil, nem muito difícil. Visto que, para aumentar o nível há custos e nem toda empresa tem a necessidade de estar no nível otimizado ou perto dele.

O Especialista 5 levantou o debate de utilizar, ao invés do Nível 3, uma escala gradual. Para passar do essencial, ser o Nível 2. Do intermediário para o avançado ter o nível mínimo de 3, etc. Os demais especialistas não concordaram por achar que poderia complicar mais e achar que não faria muita diferença para quem já implantou com Nível 2 passar para o 3. Também foi falado que o Estágio 1 (essencial) tem os controles mais importantes, então eles não deveriam ter o nível mais baixo. O Especialista 5 sugeriu, então, fazer decrescente, colocando o como nível mínimo 4 ou 5 para o estágio essencial e reduzindo nos outros estágios. Os demais especialistas debateram que tal abordagem poderia dificultar muito no início, desestimular ou deixar todas as empresas no estágio essencial. Ao final, o nível três (nível definido) como mínimo para os controles foi aceito aceito por todos os especialistas.

Neste ponto, um outro assunto emergiu. O Especialista 6 questionou se a estratégia proposta estaria avaliando a capacidade ou a maturidade das empresas. Após a discussão chegou-se ao consenso que realmente se tratava de um modelo de maturidade. O Espe-

cialista 1 afirmou que os dois podem caminhar juntos e que a nomenclatura maturidade ainda era a mais aceita e utilizada no mercado até mesmo para modelos de capacidades.

Com relação ao modo de calcular risco para a aplicação independente da estratégia, através da matriz baseada na ISO/IEC 27.005 (Figura 35), também foi aprovada por consenso. O Especialista 5 ressaltou a importância de se utilizar um normativo conceituado, como aconteceu com o COBIT. Também houve concordância de todos os especialistas quanto à nomenclatura dos níveis utilizada na matriz (baixo, médio e alto). O Especialista 3 ressalta que é um padrão, não vendo motivo para utilizar outra.

O Especialista 1 afirma que utilizar padrões já conhecidos (COBIT, ISO/IEC) e nomenclaturas comuns (alto, médio e baixo), auxilia na aceitação, entendimento e aplicação nas empresas.

O método de somar a pontuação na matriz de impacto e probabilidade (Figura 35) foi aprovada pelos especialista. O Especialista 4 inseriu que usar uma soma é interessante por ser simples, facilitando o entendimento por parte da equipe que executará e os responsáveis podem até fazer o cálculo manualmente. O Especialista 1 corroborou ao apontar que a utilização de métodos simples tendem a diminuir erros.

O Especialista 3 levantou que acredita ser interessante os pesos utilizados na matriz de impacto e probabilidade (1, 2 e 3). Mas a estratégia precisaria ser executada em uma base de empresas pra saber quais seriam os pesos ideais, podendo ser o atual ou 0,5, 1 e 3, por exemplo. Devendo a estratégia se adequar depois. O Especialista 2 concordou e inseriu que não tem, realmente, como saber se a pontuação 1, 2 e 3 é a ideal, que necessitaria de mais estudos, mas que está nivelada com o mercado e acredita que, mesmo que no futuro se perceba que não é a ideal, não geraria problemas em executar assim. Os demais especialistas concordaram.

O Especialista 4 inseriu que, em sua visão, o modelo atual pode ser utilizado sem problemas. Sendo fácil sua aplicação. Difícil é descobrir, para cada item, se a probabilidade e o impacto são baixos, médios ou altos, bem como há grande variação entre empresas. Tendo isso em mãos, a matriz (Figura 35) funciona bem.

Os Especialistas 1 e 6 levantaram a possibilidade de aplicar nas 157 empresas um questionário para gerar uma base de dados de risco, aferindo o impacto e probabilidade de cada item. Semelhante ao que foi feito com os controles da ISO/IEC. Os demais especialistas concordaram que seria um excelente complemento. O Especialista 4 colocou que, neste caso, era ainda mais importante a utilização de nichos, pois o risco varia muito mais de acordo com o negócio, ambiente e outros aspectos do que o grau de importância dos controles da ISO/IEC 27.002. Fato que foi concordado pelos demais especialistas. Ao finalizar o tema, o Especialista 2 questionou se essa análise, apesar de ser complementar e muito útil ao trabalho, não seria voltada para uma ferramenta de gestão de riscos, fugindo um pouco do escopo do trabalho atual. Os especialistas concordaram com esse posicionamento.

Após finalizar o debate sobre a área de riscos, o processo de aplicação da estratégia (Figura 37) foi apresentado e aceito pelos especialistas.

Mesmo já tendo debatido a maioria dos pontos, como forma de confirmação e de cobertura visando apurar mais impressões do grupo, um conjunto de questionamentos gerais foram inseridos pelo moderador.

Ao serem perguntados sobre a impressão dos especialistas quanto à capacidade da estratégia avaliar a maturidade da organização, todos afirmaram que sim.

Com relação à capacidade da estratégia proposta auxiliar as organizações na busca de suas metas e objetivos na área de segurança da informação, também houveram respostas afirmativas de todos os presentes. O Especialista 5 ainda apontou que a estratégia deve ajudar bastante, servindo com um facilitador. O Especialista 6 complementa que auxilia, principalmente, pra quem ainda não tem nada implantado, está no início, não tem familiaridade com o assunto ou carece de profissionais capacitados na área de segurança.

O Especialista 5 ressaltou, novamente, que com a granularidade proposta a empresa não fica perdida no meio de um estágio ou desestimulada por ainda não alcançar o nível melhor. O Especialista 2 ressalta que a estratégia pode ser usada por empresas e consultorias. Trabalhando em um formato de ganha-ganha, auxiliando as empresas a saber onde está e como aferir, por outro lado auxilia as consultorias em demonstrar o que foi feito e, com isso, o que a empresa caminhou no período, passando de um nível para outro.

Com relação à utilização da estratégia para priorização, também houve um consenso da sua capacidade neste área. O Especialista 5 complementou afirmando que, para ele, a prioridade era mais importante do que a maturidade. Segundo o especialista, priorizar todos precisam, avaliar a maturidade nem todos. Inclusive quem não tem nada pode olhar a priorização como "eu preciso disso" e a maturidade como "um dia eu vou ter isso". Os demais especialistas concordaram de imediato. O Especialista 1 inseriu que já tinha visto outros modelos para avaliar a maturidade, mas nunca tinha dado ênfase ou visto um modelo que evidenciasse a priorização, sendo um bom diferencial deste trabalho.

Todos os especialistas concordaram que a estratégia proposta deve auxiliar a organização na governança, planejamento e alinhamento estratégico na área de segurança da informação. Bem como facilitar a concepção e implantação de uma PSI e SGSI.

Ao questionar os especialistas sobre outras possíveis aplicações para a estratégia proposta, nenhum tema emergiu além da governança, gestão, priorização e maturidade em segurança da informação.

O Especialista 2 argumentou que isso era um aspecto positivo, por ela está bem direcionada para resolver o problema da priorização e da maturidade. Os Especialistas 2 e 6 concordaram e acrescentaram que no mercado há muitas ferramentas para fazer "tudo" e que não fazem nada bem feito. Então, a estratégia presente neste estudo, ela ser direcionada e resolver bem uma determinada área é um grande diferencial.

No último momento, foi levantado pelo moderador se os especialistas tinham mais

alguma sugestão ou crítica à estratégia ainda não debatida ou se tinham mais algum ponto a acrescentar ao debate.

O Especialistas 4 apontou que a estratégia deveria utilizar uma forma modular para adaptar-se a necessidade do mercado. Com isso poderia, por exemplo, trocar a ISO/IEC pela NIST, o COBIT por outros níveis de maturidade utilizados na empresa, etc. O Especialista 5 corrobora com o assunto achando interessante a abordagem como uma estratégia modular e ressalta a importância da base de conhecimento feita. A estratégia seguirá sempre as regras propostas, mas os arcabouços teóricos poderão ser adaptados para evoluir no tempo ou para atender alguma empresa. O especialista 2 viu a estratégia como uma evolução das ferramentas existentes de "compliance" e "risk assessment", visualizando um grande potencial comercial devido à carência nesta área, tendo a concordância dos especialista neste ponto.

O Especialista 3 acredita que a estratégia proposta seja uma ferramenta muito útil para um consultor ou consultoria mapear o status da empresa, dar um norte e demonstrar o resultado. O especialista ainda coloca que a estratégia pode servir para a empresa consultiva realizar um diagnóstico da situação e saber por onde ela vai começar e traçar suas ações no cliente.

Tais fatos corroboram com o resultado proposto pela DSR que é a criação de um artefato para resolução de um problema real.

O Especialista 5 ressaltou, como debatido anteriormente, a utilização da base de risco para todos os clientes para criar uma base de dados dos controles e utilizar esse valor no lugar do Nível 3 como padrão. Afirmando, também, que o modelo de risco utilizado, calculando a probabilidade e impacto, atende e resolve. Mas poderia ser desenvolvido um método para aferir com maior acurácia os riscos. Os especialistas concordam. O Especialista 3 ressalta que o ponto foi debatido anteriormente. Que é algo bem complexo detalhar a matriz de risco e saber o quanto impacta cada fator ou parâmetro (cenário, humano, financeiro, tecnológico, ambiente, concorrentes). Podendo ser o objetivo de um outro trabalho, focado em de gestão de risco.

O Especialista 3 finalizou apontando a importância de ter a estratégia baseada em uma análise mercadológica, não puramente acadêmica.

5.4 Estratégia Primasia

Com base na evolução e ajustes realizados nas três versões anteriores, chegou-se à versão atual chamada de Estratégia Primasia - Priorização e Maturidade em Segurança da Informação Adaptável. A Estratégia Primasia, então, pode ser entendida como a última evolução do artefato para apresentação nesta tese.

Em termos de nomenclatura da estratégia proposta, foi buscado um acrônimo que apontasse ao desejo da estratégia de busca pela excelência através da melhoria contínua

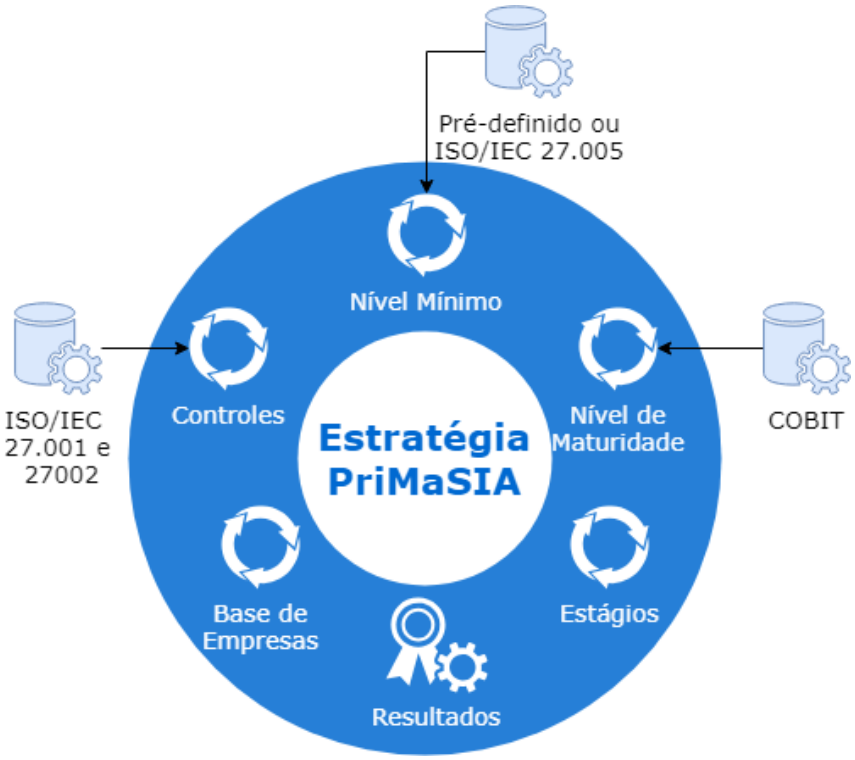
(primazia) e, ao mesmo tempo, levasse em consideração as recomendações recebidas nas avaliações.

Neste ponto, observou-se o apontamento recebido no grupo focal, no qual a ação de priorização da segurança da informação é mais importante do que a avaliação da maturidade. Inserido, portanto, a priorização no início do acrônimo.

Ao fim foi inserido o termo adaptável. Fazendo jus ao apontamento da comissão avaliadora da revista que publicou o trabalho de Alencar et al. (2018a). Os avaliadores destacaram o diferencial da estratégia em ter o modo de aplicação independente e para avaliação da maturidade comparável. Bem como os apontamentos no grupo focal sobre a estrutura modular da estratégia, permitindo possíveis adaptações e utilizações de outros arcabouços no lugar do COBIT ou ISO/IEC.

A Figura 38 representa a estratégia modular citada. Onde os arcabouços utilizados (COBIT, ISO/IEC 27.001, 27.002 e 27.005) são vistos como insumos para a estratégia proposta. Na versão atual, apresentada, da estratégia foram utilizados, de acordo com a revisão da literatura análise com a indústria e especialistas, a ISO/IEC 27.001 e 27.002 como base dos controles, a ISO/IEC 27.005 para definir o nível mínimo de maturidade a ser alcançado de acordo com os riscos inerentes e o COBIT como definição dos níveis de maturidade (nomes e pré-requisitos).

Figura 38 – Estratégia Primasia



Fonte: autor.

Como detalhamento dos principais módulos da estratégia tem-se:

- Estágio: dever ser entendido como um bloco de controles. A Estratégia Primasia foi desenhada com 4 estágios: básico (1º), essencial(2º), intermediário(3º) e avançado (4º). Os controles são divididos nos quatro estágios pela função estatística quartil, alocando os controles mais importantes no primeiro estágio (básico) e os classificados com menor nível de importância no último estágio (avançado). Toda organização inicia a análise no estágio básico;

- Controles: É a lista de controles que serão verificada a importância para as empresas, ordenados de acordo com a importância e separado nos estágios. Na aplicação será avaliada a aplicação de cada controle, sendo categorizada na escala de maturidade proposta. Para a estratégia Primasia, foram utilizados os 114 controles da norma ISO/IEC 27.0001 e 27.0002;

- Nível de Maturidade: É a escala de maturidade a ser utilizada ao se analisar os controles. Para a Estratégia Primasia foram utilizadas as definições e nível de maturidade do COBIT, são eles: nível 0 - Inexistente (apenas para os controles não aplicáveis), 1 - Inicial, 2 - Repetível, 3 - Definido, 4 - Gerenciado, 5 - Otimizado;

- Nível mínimo de maturidade: É o nível mínimo que cada controle analisado deverá alcançar para que a empresa esteja apta a passar de estágio e ser analisada no próximo bloco de controles. Na Estratégia Primasia o nível de maturidade pode ser pré-definido (nível 3 - Definido), quando se aplicar o modo de Modelo de Maturidade Comparável, ou calculado de acordo com o a matriz de risco (Figura 35).

- Base de empresas: É a base de dados coletadas através dos questionários. Esses questionários levantam características das empresas e a importância de cada controle. A medida que a base é atualizada, pode haver resposta diferentes gerando alteração na ordem de importância dos controles e, consequentemente, sua posição no estágio da Estratégia. A base de empresas atual da Estratégia Primasia conta com respostas de 157 empresas distintas;

- Resultado: O resultado não é um módulo propriamente dito, mas sim a resposta da da correta utilizada dos módulos acima. Como resultado final tem-se o nível de maturidade da empresa para segurança da informação.

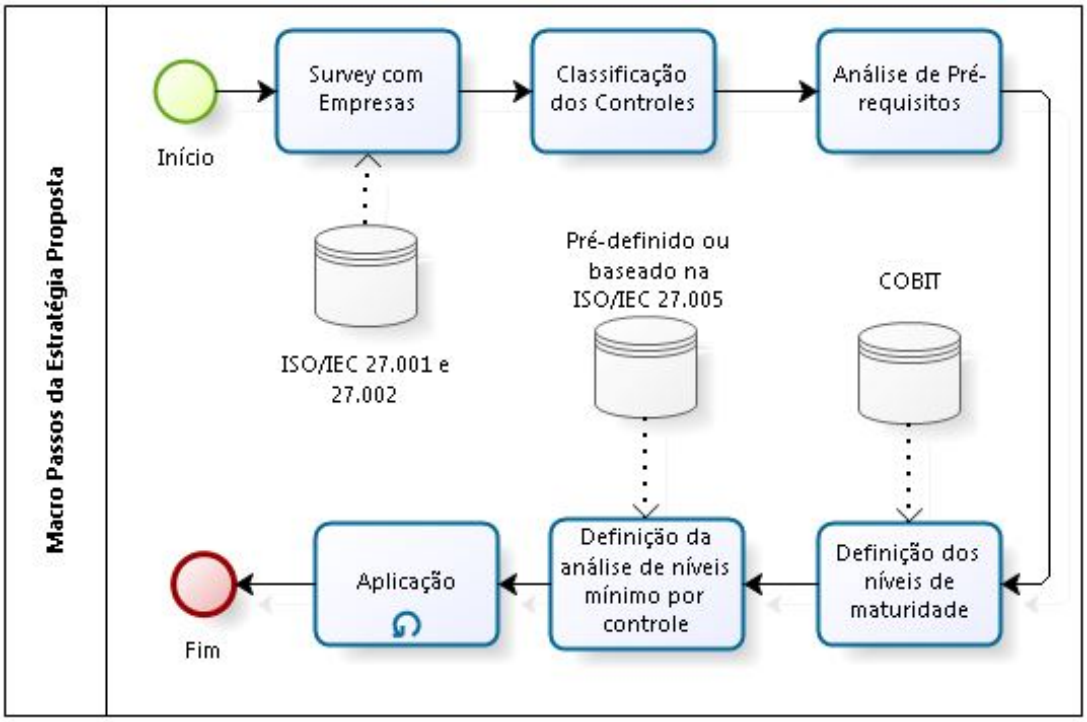
Porém, neste aspecto, os arcabouços podem ser trocados ou atualizados sem prejuízo à estratégia. Se a empresa já tiver uma tabela de níveis de maturidade implantada, pode ser utilizada no lugar dos níveis do COBIT. Ou a base de dados da ISO/IEC 27.001 e 27.002 pode ser trocada por um conjunto de controles do NIST, da LGPD[1], de qualquer outro arcabouço ou junção deles.

[1] LGPD - Lei Geral de Proteção de Dados. Lei nº 13.709, de 14 de agosto de 2018. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Em suma, a Estratégia Primasia tem suas regras descritas e deve funcionar de forma cíclica indiferente do arcabouço que a fundamente, sendo modular e adaptável ao ambiente.

Sendo importante deixar claro, neste aspecto, que o objetivo da estratégia não é implantar o COBIT ou alguma norma da ISO/IEC, mas sim melhorar o nível de segurança das empresas. Bem como a estratégia deve ser adaptável para, caso necessário, se moldar ao ambiente e facilitar sua implantação e alcance dos objetivos e não forçar as empresas a se ajustar à estratégia. Seus passos são expostos na Figura 39.

Figura 39 – Macro Passos da Estratégia - Artefato Primasia



Fonte: autor.

Outra evolução, também relativa à nomenclatura, foi referente aos estágios. A nova nomenclatura dos estágios visa dar um sentido de continuidade da estratégia e não de finalização ao se atingir o último estágio. Os novos nomes para os estágios podem ser visto no Quadro 19 que apresenta a evolução dos nomes, porém a mesma separação dos controles já exposta no Quadro 16. Visto que a ordenação e separação não foi questionada, nem sofreu evolução.

Ressalta-se que os controles apontados no primeiro estágio, Básico, são considerados os elementos para a concepção de um SGSI ou PSI simplificados, conforme proposta do artefato na Versão 1.

A última alteração refere-se a uma possível falha levantada pelos especialistas do grupo focal que ainda não tinha sido detectada. Mesmo não acontecendo nesta pesquisa, uma hipótese plausível é ter um conjunto grande de controles com a mesma média, por

Quadro 19 – Controles Separado por Estágio - Primasia

Estágio	**Quantidade de Controles**	**Controles**
Básico	32	A.5.1.1, A.6.1.1, A.6.1.5, A.6.2.2, A.7.1.1, A.7.2.1, A.8.1.2, A.8.1.3 A.8.2.1, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.3, A.9.2.4, A.9.2.5, A.9.4.2, A.9.4.4, A.11.1.5, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.12.5.1, A.12.6.2, A.13.1.3, A.15.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 e A.18.1.5
Essencial	27	A.5.1.2, A.6.1.2, A.6.2.1, A.7.2.2, A.8.1.1, A.8.3.1, A.9.2.6, A.9.4.3, A.11.1.3, A.11.2.2, A.11.2.3, A.12.1.3, A.12.1.4, A.12.2.1, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.1, A.14.2.6, A.15.1.1, A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.7, A.17.1.1 e A.18.2.2
Intermediário	28	A.7.2.3, A.8.1.4, A.8.2.2, A.9.3.1, A.9.4.1, A.9.4.5, A.11.1.1, A.11.1.2, A.11.2.1, A.11.2.9, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.6.1, A.12.7.1, A.13.1.2, A.13.2.4, A.14.1.2, A.14.1.3, A.14.2.5, A.14.2.9, A.15.1.2, A.15.2.1 A.16.1.3, A.17.2.1, A.18.2.1 e A.18.2.3
Avançado	27	A.6.1.3, A.6.1.4, A.7.1.2, A.7.3.1, A.8.3.2, A.8.3.3, A.9.2.2, A.10.1.1, A.10.1.2, A.11.1.4, A.11.1.6, A.11.2.8, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.2, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.7, A.14.2.8, A.14.3.1, 15.2.2, A.16.1.6, A.17.1.2 e A.17.1.3

exemplo, se os controles das posições 27 até 45 estivessem com a mesma média de nota, todos seriam incorporados no primeiro quartil, segundo a metodologia exposta na Versão 3. Nessa situação o primeiro estágio ficaria com 45 controles, tornando bastante denso e difícil de se começar a implantação.

Para evitar que tenha-se, um excesso de controles em um mesmo nível, é limitada em três a quantidade de controles empatados nas últimas posições a ser incorporado. Caso tenha mais do que três controles empatados, deve-se utilizar o máximo possível de casas decimais para o desempate. Caso ainda persista, deverá ser seguida a ordem numérica dos controles da ISO/IEC, inserindo, desta forma, os controles com a numeração mais baixa primeiro.

Agora, com a regra implantada, caso acontecesse a hipótese levantada, ou seja, os controles das posições 27 até 45 estivessem exatamente com a mesma média de nota, seria ordenado pela numeração do controle e selecionado os 3 empatados. Como o primeiro quartil tem 29 controles como referência (Quadro 12), seria inserido mais 3, totalizando 32 controles.

Por fim, dois pontos foram debatidos e sugeridos como melhorias no grupo focal para este trabalho:

- Realizar a divisão e ordenação dos controles por nicho de mercado;

- Criar uma base de dados de risco, incorporando as probabilidades e impactos para cada controle.

Para atendimento do primeiro ponto, torna-se necessário uma base de dados muito maior do que as 157 empresas alcançadas pelo autor. Visto que, para um correto funcionamento da estratégia, é necessário ter uma amostra significativa para formar a base de dados dos controles ordenados pela importância dada pelas empresas. Quanto maior for a base de dados mais granular será possível fazer a divisão, atendendo de forma mais precisa cada nicho de mercado ou subnichos, por exemplo empresas de TIC e do nordeste. Ou empresas da área financeira com mais de 100 funcionários. Para cada nicho deve ser feito o cálculo da amostra, conforme Figura 5, e alcançar a quantidade mínima de respostas.

Com relação ao segundo item, no próprio grupo focal foi inserido pelos especialistas a dificuldade de tal mensuração. Devendo ser tratado a parte, por um trabalho focado na gestão de riscos.

Ambos os pontos, apesar de importantes, não foram incorporados ao presente trabalho por questão de escopo e tempo.

Deste modo, a Estratégia Primasia pode ser utilizada como Modelo de Maturidade Comparável (Seção 5.3.2) ou como Aplicação Independente (Seção 5.3.3), bem como outras possíveis formas de aplicações podem surgir, como apontadas por Alencar et al. (2018b) e demonstrada a seguir.

Tais aplicações devem ser pensadas como complemento e apoio para a implantação da estratégia ou como características para uma ferramenta que execute a estratégia e consiga dar um maior auxílio às empresas.

5.4.1 Guia para Aplicação da Estratégia Primasia

Para aplicação da Estratégia Primasia, torna-se necessário o correto conhecimento dos módulos que a compõem, conforme detalhado na Figura 38 e suas explicações.

Com o conhecimento da estratégia e seus módulos, para aplicá-la, deverá ser escolhida a forma de aplicação, se será como Modelo de Maturidade Comparável, conforme Seção 5.3.2, ou como Aplicação Independente, conforme Seção 5.3.3.

Para a forma de Modelo de Maturidade Comparável, tem-se:

- Separação dos Controles por Estágio: Quadro 19.
- Nível mínimo para cada controle: 3 - Definido.

Com essas premissas o aplicador deverá seguir os seguintes passos:

1. Pega-se a base atual de estágios e controles da Estratégia Primasia, atualmente a base disposta no Quadro 19.

2. Analisa-se se existe algum dos 114 controles não aplicável à organização. Caso exista, deverá ser devidamente justificado o motivo de não ser aplicável e será excluído da análise.

3. Insere-se a organização no primeiro Estágio (básico).

4. Aplica-se todos os controles do estágio em que a empresa se encontra;

5. Avalia-se a forma de aplicação e utilização de cada controle, categorizando-o como Inicial, Repetível, Definido, Gerenciado ou Otimizado, de acordo com as diretrizes do COBIT.

6. No caso de todos os controles terem sido categorizados como definido ou de forma superior (gerenciado ou otimizado), a empresa passará pra o próximo estágio, devendo voltar ao passo 3 e seguir novamente a sequência de passos, agora com os controles do novo estágio. Exceto se a empresa já estiver no último estágio (avançado), onde finaliza-se a avaliação. Caso algum controle seja categorizado de forma inferior a definido (inicial ou repetível), a avaliação se encerra, pois a empresa não está apta a passar de estágio, podendo a mesma, após melhorar a aplicação do seu controle reiniciar este processo de aferição da maturidade organizacional.

7. Gera-se o nível de maturidade da empresa que será expresso pelo estágio que a empresa finalizou e a média dos controles que fazem parte do referido estágio (exemplos de cálculos são expostos na Seção 5.2).

A referida aplicação também pode ser vista na Figura 40. Os passos 1 e 2 supracitados, são englobadas na etapa de Definição dos Estágios do modelo da Figura 40.

Para a forma de Aplicação Independente, tem-se:

- Separação dos Controles por Estágio: a ser criado pelo aplicador de acordo com as resposta da empresa.

- Nível mínimo para cada controle: a ser criado pelo aplicador para cada controle de acordo com a matriz de risco (Figura 35).

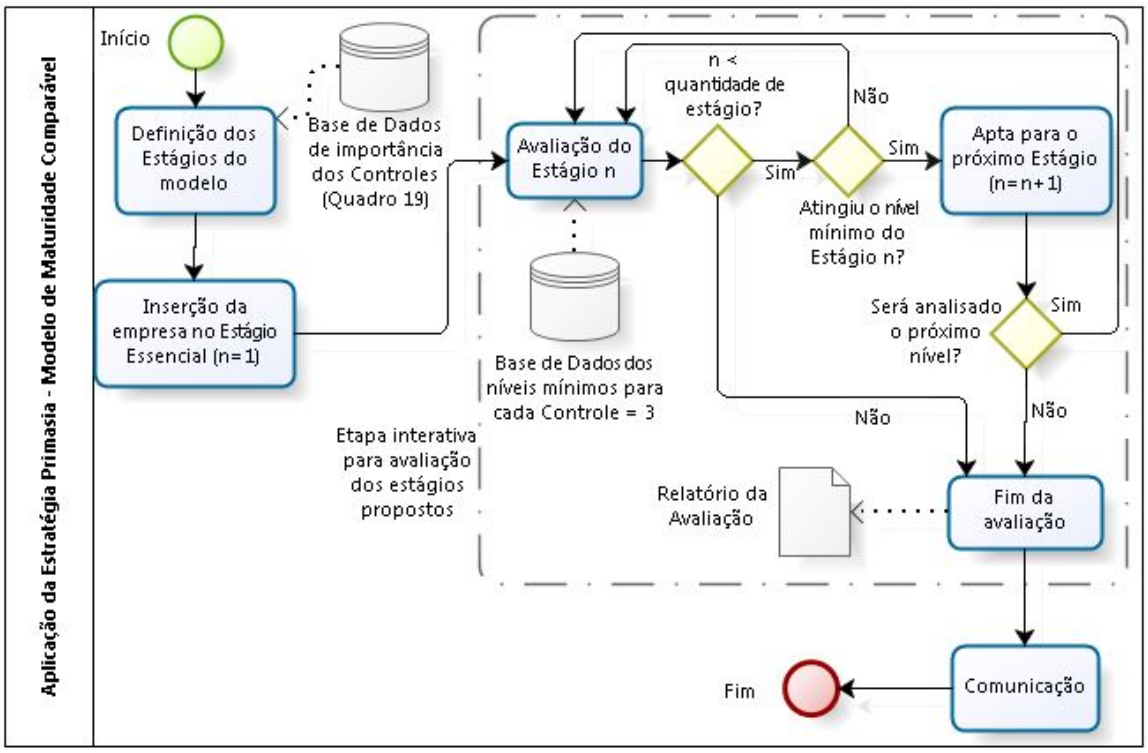
Com essas premissas o aplicador deverá seguir os seguintes passos:

1. Solicita-se aos stakeholders que respondam ao questionário da pesquisa (Apêndice C);

2. Ordena os controles pela média das notas de importância (conforme Seção 4.3).

3. Separa-se os controles por Quartis (conforme Seção 5.3.1)

Figura 40 – Aplicação da Estratégia Primasia - Modelo de Maturidade Comparável



Fonte: autor.

4. Analisa-se se existe algum dos 114 controles não aplicável à organização. Caso exista, deverá ser devidamente justificado o motivo de não ser aplicável e será excluído da análise.

5. Analisa-se o nível mínimo a ser aplicado em cada controle conforme matriz de risco (Figura 35) e detalhamentos expostos na Seção 5.3.

6. Insere-se a organização no primeiro Estágio (básico).

7. Aplica-se todos os controles do estágio em que a empresa se encontra;

8. Avalia-se a forma de aplicação e utilização de cada controle, categorizando-o como Inicial, Repetível, Definido, Gerenciado ou Otimizado, de acordo com as diretrizes do COBIT.

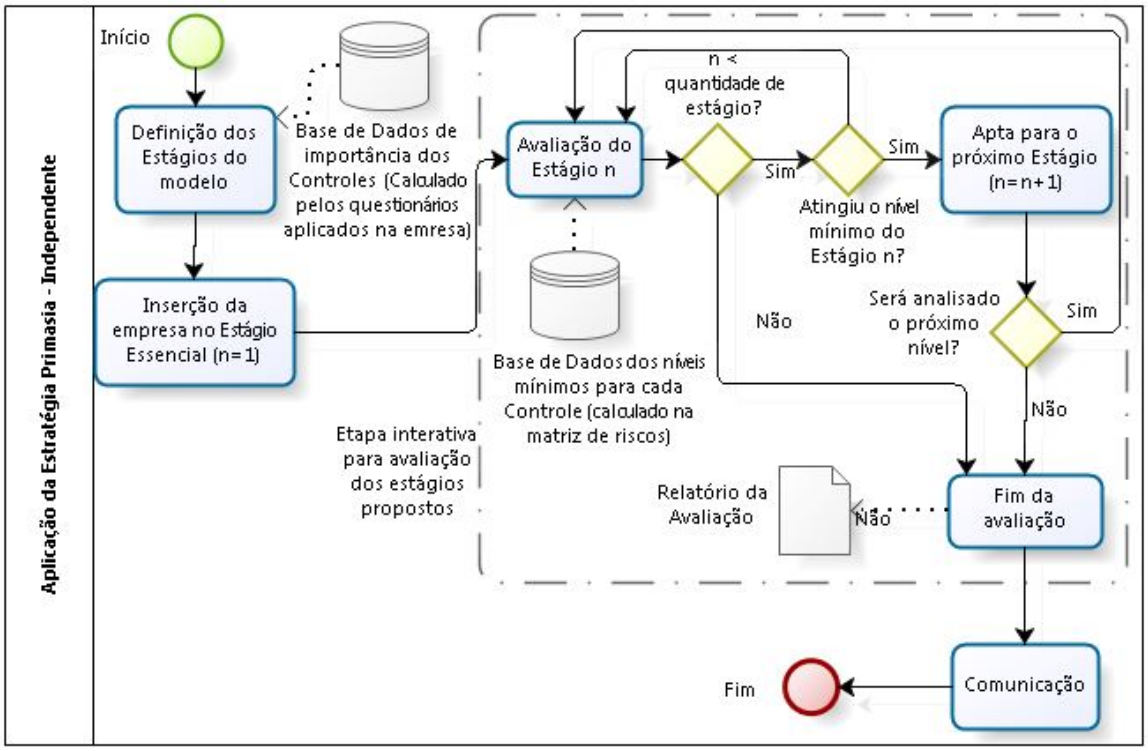
9. No caso de todos os controles terem atingido o seu nível mínimo, conforme matriz de risco, ou ultrapassado-o, a empresa passará pra o próximo estágio, devendo voltar ao passo 6 e seguir novamente a sequência de passos, agora com os controles do novo estágio. Exceto se a empresa já estiver no último estágio (avançado), onde finaliza-se a avaliação. Caso algum controle seja categorizado de forma inferior a definido (inicial ou repetível), a avaliação se encerra, pois a empresa não está apta a passar

de estágio, podendo a mesma, após melhorar a aplicação do seu controle reiniciar este processo de aferição da maturidade organizacional.

10. Gera-se o nível de maturidade da empresa que será expresso pelo estágio que a empresa finalizou e a média dos controles que fazem parte do referido estágio (exemplos de cálculos são expostos na Seção 5.2).

A referida aplicação também pode ser vista na Figura 41. Como diferença para a representação da aplicação anterior, tem-se que as etapas 1, 2, 3 e 4 supracitadas, são englobadas na etapa de Definição dos Estágios do modelo da Figura 41. Como também as duas base de dados utilizadas são diferentes.

Figura 41 – Aplicação da Estratégia Primasia - Independente



Fonte: autor.

5.4.2 Outras Possíveis Aplicações da Estratégia

Pensando na estratégia como uma ferramenta corporativa, novas características podem ser adicionadas auxiliando, ainda mais, as empresas e profissionais na aplicação da segurança da informação. Algumas opções foram apontadas por Alencar et al. (2018b) e são detalhadas a seguir.

5.4.2.1 Banco de Melhores Práticas em Segurança da Informação

Em um pensamento mais amplo, o modelo proposto de levantamento de dados pode servir como insumos para outras finalidades. Entre elas como uma base de melhores práticas para a segurança da informação, como diagramado na Figura 37.

Com uma base de dados com amostras significativas, é possível verificar a indicação de controles da ISO/IEC 27.001 e 27.002 selecionados como mais importante para o tipo de empresa específica, por exemplo, selecionando apenas os controles importantes para Pequenas e Médias Empresas (PMEs), por região específica, por tipo de negócio, etc. Bem como a inserção de requisitos legais, contratuais ou regulamentares para compor e ser aferido e analisado dentro da área de segurança da informação (Figura 37).

Tal solução pode ser útil para apontar os controles mais utilizados (melhores práticas) por nicho, região ou características para que empresas sigam como referência. Seja por não ter um profissional para apoiar e melhor definir as áreas e controles a serem tratados dentro da empresa ou, caso exista, para comparar o modelo da empresa com o que está sendo utilizado no mercado.

5.4.2.2 Sistema de Recomendações

Com a base de dados formulada, é possível utilizar um sistema de recomendações. Após a empresa se cadastrar respondendo o questionário inicial com os dados do negócio (Apêndice B), o sistema poderá verificar o banco de respostas para empresas semelhantes e recomendar a aplicação de um conjunto de controle específicos para formação do Banco de Dados Personalizado (Figura 37) para a empresa em questão.

Acredita-se que essas recomendações servirão como guia para aqueles que não tem uma análise mais aprofundada na área de segurança da informação e, consequentemente, não conseguem definir corretamente os controles a implantar, bem como, no caso de empresas que já têm um nível de conhecimento, confrontar com o que é mais utilizado de forma a avaliar os controles já selecionados ou levantar o debate para inserção ou exclusão de algum controle.

O sistema de recomendações também pode ser ativado por indicação de especialistas na área de segurança da informação que poderão atuar na implantação da estratégia ou em uma ferramenta que a execute. Por exemplo, ao se ter algum normativo ou lei específicos para um grupo que a empresa em questão se enquadra, poderá ser indicado algum controle para o tratamento ou atendimento da norma ou lei. Uma outra situação é em caso de algum ataque que esteja se espalhando. Dá mesma forma o sistema, guiado por especialista, poderá recomendar algum controle na tentativa de mitigar as possíveis ações ou reduzir vulnerabilidades. Fatores que, em uma segunda etapa, podem ser otimizados a partir de meios com inteligência computacional.

5.4.2.3 Correlação com Ferramentas de Mercado

Uma outra característica possível é a correlação com classes de ferramentas do mercado. Em um primeiro momento, é possível que o sistema aponte tipos de soluções para atender ao controle selecionado. Por exemplo, ao ser indicado o controle 12.2.1 - Controles contra códigos maliciosos, da ISO/IEC 27.002: "Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário" (ABNT, 2013b), o sistema poderá apontar a utilização de categorias de ferramentas para solucionar, por exemplo, antivírus nos dispositivos e um proxy web com filtro (web filter).

5.5 Síntese do Capítulo

O etapa da pesquisa descrita neste capítulo teve, como principal norte, o atendimento dos seguintes objetivos específicos:

- Propor um meio para diminuir a burocracia e formalismos dos modelos atuais aplicados na área de segurança da informação, norteado pelos princípios de governança ágil de TIC;
- Definir uma estratégia para avaliação da maturidade da segurança da informação na corporação;
- Definir uma estratégia para priorização das ações de segurança da informação;
- Propor um guia simplificado de controles para concepção de uma PSI e de um SGSI;
- Auxiliar a melhoria contínua do SGSI da empresa.

Para alcançar os objetivos, foi concebido um artefato que evoluiu ao longo de quatro versões. A primeira versão teve como foco o auxílio à concepção de uma política de segurança da informação simplificada, apontando os principais controles que deveriam ser tratados e inseridos na PSI. Esta versão foi avaliada por cinco especialistas e 104 empresas utilizando um questionário como instrumento (Apêndice G). Gerou-se, além dos controles para a PSI simplificada, uma avaliação dos controles pré-requisitos da norma (Quadro 15).

A Versão 2 foi concebida para manter o que já se tinha construído na versão anterior e aprimorá-la. Dessa forma, a Versão 2 visou a construção de um modelo de avaliação da maturidade e priorização da segurança da informação. Essa versão iniciou a divisão de controles por estágios, indicando o nível de maturidade da empresa como o estágio mais o nível alcançado. Também inseriu o conceito de nível mínimo para cada controle como critério para passar de estágio. A Versão 2 foi avaliada por seis especialistas.

A Versão 3 é a evolução acumulativa da versão anterior. Agora denominada como estratégia e contendo quatro estágios. Não mais dividindo os controles em estágios por

um valor fixo da nota do controle, mas sim utilizando um percentual (quartil). Dessa forma, indiferente da nota, se manteria a proporção de controles por estágio. Essa versão manteve o conceito de nível mínimo para cada controle, podendo ser um valor fixo, igual à Versão 2, e inseriu a possibilidade de ser calculado através de uma matriz de risco.

A Versão 3 apontou, também, duas formas de aplicação da estratégia: o modelo de maturidade comparável e a aplicação independente. A estratégia foi avaliada através de uma aplicação em caso real e pela realização de um grupo focal com seis especialistas.

Ressalta-se a dificuldade em realizar o grupo focal, em especial pelos obstáculos de se conciliar agendas, local, horário e trânsito do Recife. Porém, o árdua atividade de planejamento foi compensada em sua execução, pois os especialistas trouxeram apontamentos e melhorias significativas para o artefato.

Com as melhorias propostas pelas avaliações realizadas na Versão 3, chegou-se à versão atual, a Estratégia Primasia, que contempla os ganhos obtidos nas versões anteriores e as correções ou melhorias apontadas nas avaliações. Dessa forma, o processo da evolução acumulativa do artefato pode ser visto na Figura 42.

Figura 42 – Evolução Acumulativa do Artefato

Fonte: autor.

Para as três primeiras versões do artefato utilizou-se a submissão de artigos como forma de avaliação e divulgação. Como resultado, alcançou-se quatro publicações. São

elas: Silva Neto, Alencar e Queiroz (2015), Alencar, Tenorio Junior e Moura (2017a), Alencar e Moura (2018) e Alencar et al. (2018a).

Para que a estratégia continue melhor representando o mercado e, consequentemente, direcionando de forma correta as empresas, periodicamente os controles de cada estágio deverão ser recalculados. Para isso, novas respostas deverão ser inseridas ao modelo, aumentando a base de dados e representando a real importância de cada controle. Fato que confere um dinamismo ao modelo, sendo mais um diferencial aos já existentes.

Importante destacar que a proposta de ser uma estratégia contínua de melhoria foi enaltecida no grupo focal, aos especialistas apontarem sua aderência ao método interativo de gestão PDCA.

6 CONSIDERAÇÕES FINAIS

Para finalizar o presente trabalho, esse capítulo revisará os objetivos propostos, relatando como eles foram realizados (Seção 6.1). Na Seção 6.2 indicará as principais contribuições obtidas. Sendo complementada pelas limitações e dificuldades encontradas (Seção 6.3). Encerrando o capítulo, a Seção 6.4 apresentará propostas de trabalhos futuros em continuidade, melhoria ou complemento à pesquisa apresentada.

6.1 Resolução dos Pontos Propostos

Conforme apresentado na Seção 1.5, o presente trabalho guiou-se pelo seguinte objetivo geral:

- Propor uma estratégia para avaliação da maturidade e priorização da segurança da informação no ambiente corporativo através da utilização, em conjunto, dos principais arcabouços existentes na área.

Sendo desdobrado em sete ações (objetivos específicos) que, quando atendidas, cumpririam o objetivo supracitado. São elas:

i. Consolidar uma visão geral de iniciativas para evolução de maturidade na área de segurança da informação;

ii. Compreender como a segurança da informação é tratada, nos diversos aspectos que abrangem essa área, no meio corporativo;

iii. Propor um meio para diminuir a burocracia e formalismos dos modelos atuais aplicados na área de segurança da informação, norteado pelos princípios de governança ágil de TIC;

iv. Definir uma estratégia para avaliação da maturidade da segurança da informação na corporação;

v. Definir uma estratégia para priorização das ações de segurança da informação;

vi. Propor um guia simplificado de controles para concepção de uma PSI e de um SGSI;

vii. Auxiliar a melhoria contínua do SGSI da empresa.

Como insumo para atender às ações, realizou-se uma pesquisa bibliográfica envolvendo trabalhos de diversas áreas da academia, normativos e documentos do meio corporativo. Tal mescla visou seguir o conceito de Marconi e Lakatos (2010), que aponta que a pesquisa

bibliográfica não é apenas uma repetição do que já foi retratado, mas propicia a análise de determinado tema com um novo enfoque, podendo chegar a conclusões inovadoras ou parcialmente percebidas anteriormente. Assim, construindo uma visão pautada sob diversos ângulos de áreas distintas da segurança da informação, espera-se não apenas contribuir para a área de tecnologia, mas também para as demais áreas que estudam o vasto ramo da segurança da informação.

Outro ponto importante de entrada de informações para o trabalho foram os dados obtidos através dos surveys (Apêndices B e C) aplicados nas empresas. Com os conhecimentos da base teórica e o panorama do ambiente coletado e analisado, construiu-se os Capítulos 3 e 4. Acredita-se, portanto, que esses capítulos atendem ao que era esperado pelos dois primeiros objetivos específicos: "Consolidar uma visão geral de iniciativas para evolução de maturidade na área de segurança da informação" e "Compreender como a segurança da informação é tratada, nos diversos aspectos que abrangem essa área, no meio corporativo".

O terceiro objetivo específico, "Propor um meio para diminuir a burocracia e formalismos dos modelos atuais aplicados na área de segurança da informação, norteado pelos princípios de governança ágil de TIC", acredita-se que foi atendido por se elencar controles críticos da ISO/IEC, possibilitando a sua aplicação parcial e pela definição do modo de aplicação independente da Estratégia Primasia. Tal forma de aplicação parece estar alinhada aos meta-valores propostos por (LUNA et al., 2016). Nesta forma de aplicação, as empresas estão moldando o processo ao seu negócio e não o contrário. Buscando obter uma melhoria na área de segurança da informação e não a aplicação de um modelo ou normativo formal para estar em conformidade.

Acredita-se que a Estratégia Primasia tenha atendido aos quatro últimos objetivos específicos: "Definir uma estratégia para avaliação da maturidade da segurança da informação na corporação", "Definir uma estratégia para priorização das ações de segurança da informação" e "Propor um guia simplificado de controles para concepção de uma PSI e de um SGSI". A proposta foi avaliada e obteve êxito quanto à afirmação de sua aplicação para auxílio das empresas nas áreas de priorização, maturidade, gestão e governança da segurança da informação.

Por fim, acredita-se que a Estratégia Primasia também atende ao último objetivo específico: "Auxiliar a melhoria contínua do SGSI da empresa", ao proporcionar que os questionários e avaliação sejam realizados periodicamente. Essa concepção faz com que seja possível a visão atual dos controles mais críticos e ajustada a estratégia, bem como priorizando os controles a aplicar, auxiliando, desta forma, o SGSI.

Os controles do primeiro estágio (básico) da Estratégia Primasia podem ser vistos como um guia simplificado de controles para uma PSI ou SGSI. Caso a empresa tenha interesse e necessidade de um conjunto mais completo, pode incluir, além do primeiro estágio, o segundo (essencial). Tais estágios podem ser utilizados até se chegar a implantação de

todos os controles, tendo o benefício de aplicar os controles priorizando os mais críticos em cada estágio.

A Estratégia Primasia também pretende ser evoluída e continuar coletando informações de empresas. Com isso ficará atualizada e sempre indicando a importância real dos controles, mantendo a corretude da priorização dos controles. Trabalhando de forma cíclica, conforme o PDCA. Essa proposta deve auxiliar, continuamente, nas adaptações e melhorias do SGSI nas empresas.

Com o atendimento de todos os objetivos específicos, acredita-se que, por consequência, o objetivo geral da pesquisa também tenha sido realizado.

Em uma sequência lógica, com o atendimento aos objetivos específicos e geral, a pergunta de pesquisa foi respondida.

Diante dos fatos expostos, temos:

Como mensurar e priorizar a segurança da informação corporativa com base nos atuais arcabouços existentes na área?
Através da Estratégia Primasia.

6.2 Principais Contribuições

No ambiente atual é visível a necessidade de se buscar melhorias na área de segurança da informação, bem como meios para garantir o melhor destino do tempo e recursos. Em diversos casos tais ações podem ser um diferencial para a continuidade do negócio.

O trabalho apresentou uma estratégia para a segurança da informação que pode ser aplicada para auxiliar na priorização e na avaliação da maturidade em segurança da informação.

A estratégia permite uma análise do nível de maturidade de forma mais aprimorada e granular, fazendo com que esta tenha maior visibilidade, através dos estágios. Não apenas analisando um nível de maturidade final da empresa, mas também se os controles principais foram tratados.

A estratégia proposta consiste, basicamente, em um conjunto de módulos:

- Quatro estágios propostos (Básico, Essencial, Intermediário e Avançado);
- Níveis de maturidade (baseados no COBIT);
- Aspectos e controles a analisar (utilizado os controles da ISO/IEC 27.001 e 27.002);
- Definição do nível mínimo de cada controle (pré-definido ou baseado nos riscos inerentes à aplicação de cada um deles conforme ISO/IEC 27.005).

Acredita-se que essa estrutura modular adaptável seja um diferencial da estratégia proposta, visto que utiliza arcabouços consolidados, mas também possibilita a troca de algum módulo por outro, ao critério da empresa.

Por exemplo, um conjunto de níveis de maturidades diferentes já utilizados na empresa ou uma análise de risco baseado em outros parâmetros. Tal possibilidade, permite um maior ajuste da estratégia ao negócio, bem como pode reduzir tempo e recursos em sua aplicação ao utilizar algum módulo já conhecido e existente.

O fato da possibilidade de se avaliar como uma aplicação independente, utilizar módulos adaptáveis, permitindo ajustes ao negócio, apontam a convergência aos pensamentos da governança ágil.

Por fim, no que tange à Estratégia Primasia, acredita-se que a mesma possibilite melhorias significativas na área de segurança corporativa, como exposto no presente trabalho e mencionado pelos especialistas nas diversas avaliações dos artefatos.

Além da Estratégia Primasia, elemento central deste doutorado, um conjunto de outras pequenas contribuições para o meio acadêmico foram alcançadas, entre elas:

- O Mapeamento Sistemático da Literatura realizado e a base de artigos da área construída (Apêndice J), que poderão auxiliar novas pesquisas na área;
- Os onze trabalhos aceitos ou já publicados (Apêndice K), fortalecendo o tema, divulgando os resultados e dando materiais para aqueles que desejam estudar, pesquisar ou implantar a segurança da informação;
- A concepção da PSI e SGSI simplificada. Além de entregar um conjunto possível de controles reduzidos, ressalta-se a visão e possibilidade de fazer algo diferente com o existente, traçar novos caminhos (no sentido de simplificar) para a aplicação da PSI e SGSI e demais áreas da segurança da informação.

Outra contribuição é a fotografia do ambiente de segurança da informação corporativo, detalhado no Capítulo 4. Acredita-se que as informações passadas sirvam, na área acadêmica, como uma exposição do ambiente possibilitando comparações com outras amostras ou, com outros estudos apropriados, para construir tendências de mudanças na área. Como também acredita-se que contribui para as empresas, com possibilidade de comparação de como está o ambiente e a sua posição. E, por fim, auxilia os profissionais e empresas fornecedoras de consultorias, serviços e produtos de TIC, em especial de segurança. Propondo informações para análises e avanços, desta forma, da área de segurança como um todo.

As contribuições aqui destacadas podem ser vistas como diferenciais ou evoluções da literatura da área relacionada, em especial, no Capítulo 3. Alguns destaques são exibidos a seguir.

A presente pesquisa apontou que entre os principais normativos da área de segurança da informação estão as normas ISO/IEC 27.001 e 27.002. Ao mesmo tempo que também foi apontado pela amostra de empresas alcançadas a dificuldade de sua implantação. Neste aspecto a Estratégia Primasia é de grande valor, priorizando os controles e facilitando sua implantação.

O trabalho de Silva Neto, Alencar e Queiroz (2015) propõe uma lista de controles para uma PSI simplificada. Nesse caso, a Estratégia Primasia pode ser vista como uma evolução. Não apenas apontando uma lista de controles, como também a inserção de módulos para aferição da maturidade e a priorização dos demais controles. Sendo esse aspecto uma área não trabalhada nas demais pesquisas analisadas.

A divisão da Estratégia Primasia em quatro estágios e cinco níveis por estágio, cria uma maior granularidade na aferição (uma combinação de 20 possíveis estados), sendo um ponto positivo levantado pelos especialistas em comparação com os demais modelos existentes que atuam com quatro ou cinco níveis isolados, por exemplo: Lessing (2008), Saleh (2011b), Karokola, Kowalski e Yngström (2011), Rigon et al. (2014), Cholez e Girard (2014), Coelho, Fernandes Junior e Proença Junior (2014), Muthukrishnan e Palaniappan (2016), Menezes et al. (2017), Silva e Barros (2017) e Proença e Borbinha (2018).

As avaliações realizadas com empresas e especialistas, bem como uma aplicação em um caso real é um diferencial quanto aos trabalhos estritamente teóricos, por exemplo: Woodhouse (2008), Karokola, Kowalski e Yngström (2011) e Silva, Menezes e Costa (2012).

A grande maioria dos trabalhos verifica se o critério foi adotado ou não, entre os mais recentes pode-se citar Silva e Barros (2017) e Proença e Borbinha (2018). Porém acredita-se que uma empresa que aplicou, de maneira informal, um critério não está no mesmo nível de outra organização que aplicou de maneira formal, com treinamento, divulgação e ações para melhoria contínua daquele controle. Na Estratégia Primasia é verificado a forma de aplicação de cada critério, avaliando seu grau de maturidade para, com isso, aferir a maturidade do estágio e da empresa.

A apresentação de uma estratégia modular que visa possibilitar a utilização dos diversos arcabouços existentes, facilitando sua implantação e utilização pelas empresas, também é um diferencial, não se vendo ênfase nos trabalhos correlatos para essa área.

Por fim, outro ponto de evolução da estratégia proposta com relação aos estudos correlatos citados é o fato de trabalhar com uma base de controles segregados por estágios e priorizados de acordo com a resposta das empresas. Tal ação é detalhada como forma de possibilitar a atualização da divisão dos controles por estágio de forma a manter a priorização adequada atualmente e no futuro.

Nesse aspecto, alguns estudos trabalham com a análise de todos os controles, por exemplo Rigon et al. (2014). A ação de analisar todos os controles em um único momento foi debatida no trabalho como um ponto de dificuldade para a implantação. Outros trabalhos selecionam áreas ou controles específicos para analisar (PARK et al., 2008; CHOLEZ; GIRARD, 2014; COELHO; FERNANDES JUNIOR; PROENÇA JUNIOR, 2014; SILVA; BARROS, 2017; PROENÇA; BORBINHA, 2018), porém não detalham exatamente o motivo da escolha de tais áreas, controles ou peguntas. Também não explicam como atualizar essa escolha. Desta forma não se pode afirmar que as áreas, controles ou peguntas escolhidas serão as áreas recomendadas ou mais importantes em um futuro próximo, podendo, até mesmo,

invalidar esses modelos.

E, em todos os casos, os controles selecionados são tratados de forma estática, igualitária, sem priorização ou peso diferenciado para os controles mais importantes. Diferente da abordagem adotada na Estratégia Primasia, que, para suprir esta possível deficiência, prioriza os controles de acordo com a importância apontada pelas empresas, ou seja, sendo possível atualizar a base de resposta e, consequentemente, a ordenação e divisão dos controles de acordo com as necessidades atuais do mercado de forma contínua.

6.3 Principais Limitações e Dificuldades Encontradas

Entre as dificuldades encontradas, duas se destacaram, por coincidência no início e fim da pesquisa. A primeira foi o obstáculo de se conseguir respostas aos surveys iniciais (Apêndices B e C), tanto pelo tamanho do questionário, quanto por tratar de informações de tecnologia e segurança. Inclusive, algumas empresas iniciaram o questionário e, no meio, não finalizaram. Quando o pesquisador entrou em contato, foi informado que não era do interesse deles enviar tais informações. Por outro lado, todos afirmaram ter interesse em receber a síntese das respostas.

Ressalta-se que, uma empresa não respondeu a pesquisa e ainda indagou se não era uma forma de engenharia social para descobrir fraquezas ou possíveis vulnerabilidades da empresa. Em outras situações, o pesquisador teve que informar os métodos utilizados para não identificar a empresa e o informante, como também mitigar as chances de haver algum vazamento das informações coletadas.

A segunda dificuldade principal foi no planejamento e execução do grupo focal. Percebeu-se uma carência na área de profissionais de segurança da informação com conhecimento em governança, gestão e maturidade. Ou se tinha gestores de TIC, com pouco conhecimento em segurança. Ou profissionais de segurança da informação, da área técnica, com conhecimento em firewalls, antivírus, linux, teste de penetração, etc, mas sem conhecimento em assuntos de segurança da informação em nível estratégico.

Após se encontrar um grupo seleto de profissionais que poderiam auxiliar como especialistas para a presente pesquisa, houve resistência para o profissional abdicar de suas atividades para atuar no grupo focal, como também, diversos problemas para se compatibilizar dia, horário e local entre os possíveis especialistas.

Mesmo com todos os obstáculos, acredita-se que as contribuições obtidas na sessão foram fundamentais para o aperfeiçoamento da estratégia.

Entre os principais fatores limitantes do trabalho, têm-se a própria área de maturidade. Diferente de outras temáticas, é difícil avaliar o resultado de uma estratégia ou modelo de maturidade. Visto que a maturidade é intangível, influenciada por uma série de aspectos e não se vê o resultado de imediato. Por mais que se possa fazer uma aferição da maturidade através de um modelo ou estratégia, torna-se necessário esperar o tempo passar para saber

o quanto aquela estratégia ou modelo auxiliou a empresa a ficar mais madura, não apenas aferir a maturidade.

Também foram aspectos limitadores do processo a pequena equipe para auxiliar no desenvolvimento da estratégia e todos os seus componentes. Bem como, a restrição de tempo para implementação prática e análise do comportamento da estratégia.

O espalhamento da amostra obtida, com 52 empresas em Recife - PE, por mais que as mesmas tenham atuação nacional ou, em alguns casos, internacional, ainda pode ter direcionado as resposta para algum aspecto regional.

Por fim, destaca-se que algumas áreas complementares à pesquisa e de suma importância não foram pesquisadas devido às limitações de escopo deste projeto.

Como inserido, por diversas vezes, nos comparativos com outras pesquisas realizados no Capítulo 4, é importante ressaltar que a análise realizada é apenas de resultados, comparando dois ambientes. Devendo ser analisada com cuidado para apontamentos cabais devido, principalmente, ao período de realização de cada uma das pesquisas, à amostra, método utilizado, etc. Por conta desta situação qualquer explicação ou linha de tendência traçada deve ser vista apenas como hipótese e que carece de novos estudos para comprová-la. Não fazendo parte do objetivo deste trabalho, visto que, não se tinha no escopo estudar a dinâmica do mercado e traçar tendências.

Outro ponto, esse surgido no grupo focal, foi a necessidade de um maior aprimoramento na análise e definição do risco. A Estratégia Primasia permeou a área, mas não faz parte do seu escopo se aprofundar ou tratar a área de gestão de risco.

6.4 Trabalhos Futuros

Acredita-se que este trabalho poderá ganhar novas contribuições e desdobramentos se estudos futuros analisarem, entre outros, aspectos como:

- Atualizar o mapeamento sistemático e revisões da literatura com trabalhos do ano de 2018 em diante;
- Continuação da coleta de dados para que seja possível manter a base de dados atualizada e aplicar a Estratégia, com confiança estatística, em nichos específicos. Bem como, analisar se existem diferenças entre os resultados dos possíveis nichos e seus motivos;
- Realizar estudos de caso avaliativos para verificar, na prática, o comportamento e desempenho da estratégia;
- Analisar as hipóteses levantadas no Capítulo 4 quanto às variações dos resultados da pesquisa atual em comparação com as anteriores, pesquisar sobre a veracidade delas e formas de traçar ou prever tendências;

- Realizar uma análise estatística mais aprofundada dos dados coletados. Por exemplo, uma análise categórica e uso de regressão logística.

- Criar uma base de dados, assim como aconteceu com o nível de importância dos controles, para o risco de cada controle. Com essa base o nível mínimo de maturidade, estabelecido no trabalho como o nível 3 (definido), para passar de estágio, poderia ser a média do nível aferido de acordo com a matriz de risco proposta na Figura 35. Desta forma a Estratégia Primasia poderia tratar de modo diferente cada controle, de acordo com os riscos inerentes ao mesmo e, consequentemente, com uma maior aderência às necessidades das empresas e se ajustando dinamicamente de acordo com as respostas;

- Analisar outras possíveis formas e métodos de análise de risco para, se necessário, encaixar à Estratégia, de forma modular, um novo método testado e comprovadamente mais apropriado;

- Desenvolvimento de uma ferramenta para aplicação da Estratégia Primasia, de preferência web, visando facilitar a aplicação dos questionários, análise das respostas, geração dos quartis e criação de relatórios para as empresas;

- Definir um processo de certificação que permita capacitar e credenciar profissionais como avaliadores oficiais da estratégia proposta.

Por fim, ressalta-se que a presente pesquisa buscou evoluir a temática nos aspectos acadêmicos e profissionais, sendo os trabalhos futuros supracitados possíveis ações para galgar mais um degrau. Porém a segurança da informação ainda necessita de muitas ações e pesquisas para suprir demandas reprimidas da área, assim como para analisar novos problemas que surgem pelo melhoramento e criação de novas ameaças e técnicas de ataque, além dos novos problemas gerados pelas próprias soluções propostas.

Que este trabalho e suas propostas futuras sirvam de alicerces para a evolução da área.

REFERÊNCIAS

ABNT. *NBR ISO/IEC 17799 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2006. 120 p.

ABNT. *NBR ISO/IEC 27005 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2011. 87 p.

ABNT. *NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos*. Rio de Janeiro - RJ, Brasil: ABNT, 2013a. 32 p.

ABNT. *NBR ISO/IEC 27002 - Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2013b. 112 p.

ABNT. *NBR ISO/IEC 27014 - Tecnologia da informação - Técnicas de segurança - Governança de segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2013c. 12 p.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Produção Científica sobre Segurança da Informação em Anais de Eventos da ANPAD. In: *IV Encontro de Administração da Informação - EnADI / ANPAD*. [S.l.: s.n.], 2013. p. 1–16.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Adoção de Medidas de Segurança da Informação: Um Modelo de Análise para Institutos de Pesquisa Públicos. *Revista Brasileira de Administração Científica,*, v. 5, n. 2, p. 46–59, 2014.

ALENCAR, G. D. *O Impacto do Fator Humano na Segurança da Informação: Uma Visão Estratégica*. 70 p. Dissertação (Especialização em Gestão da Tecnologia da Informação) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2008.

ALENCAR, G. D. *Estratégias para Mitigação de Ameaças Internas*. 137 p. Dissertação (Mestrado em Ciência da Computação) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2011.

ALENCAR, G. D.; AMORIM, E. S. de; MENEZES, B. P.; MOURA, H. P. de. Produção Científica sobre Governança, Gestão e Maturidade da Segurança da Informação nos Principais Periódicos e Eventos Brasileiros Relacionados à Computação. In: *15th International Conference on Information Systems & Technology Management - CONTECSI*. São Paulo - SP: USP, 2018b. p. 2756–2782.

ALENCAR, G. D.; LIMA, M. F. de; FIRMO, A. C. A. A Perspectiva de Análise Comportamental como Forma de Combate à Engenharia Social e Phishing. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 3, p. 1–19, 2013a.

ALENCAR, G. D.; LIMA, M. F. de; FIRMO, A. C. A. O Efeito da Conscientização de Usuários no Meio Corporativo no Combate à Engenharia Social e Phishing. In: *IX Simpósio Brasileiro de Sistemas de Informação*. [S.l.: s.n.], 2013b. p. 254–259.

ALENCAR, G. D.; MENEZES, B. P.; AMORIM, E. S. D.; FARIAS JÚNIOR, H.; MOURA, H. P. Governança, Gestão e Maturidade da Segurança da Informação: Um Mapeamento Sistemático do Cenário Nacional. *Revista de Sistemas e Computação*, v. 8, n. 1, p. 153–173, 2018c. ISSN 2237-2903. Disponível em: <http://www.revistas.unifacs.br/index.php/rsc>.

ALENCAR, G. D.; MOURA, H. P. Maturity Model for Information Security: A Proposal Based on ISO/IEC 27001 and 27002 According to the Principles of Agile Governance. In: *14th International Conference on Information Systems & Technology Management - CONTECSI - Doctoral Consortium*. [s.n.], 2017b. p. 4817–4832. ISBN 9788599693131. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4959>.

ALENCAR, G. D.; MOURA, H. P. Método Simplificado para Aplicação e Priorização da Segurança Da Informação: Reflexões Teóricas e Soluções Futuras. In: *15th International Conference on Information Systems & Technology Management - CONTECSI*. São Paulo - SP: USP, 2018. p. 2801–2816.

ALENCAR, G. D.; MOURA, H. P.; FARIAS JÚNIOR, I. H.; TEIXEIRA FILHO, J. G. A. An Adaptable Maturity Strategy for Information Security. *Journal of Convergence Information Technology (JCIT)*, v. 13, n. 2, p. 1–12, 2018a. ISSN 1975-9320. Disponível em: <http://www.globalcis.org/dl/citation.html?id=JCIT-4403>.

ALENCAR, G. D.; MOURA, H. P. de. Proposta de Modelo de Maturidade para Segurança da Informação baseada na ISO/IEC 27001 e 27002 aderente aos Princípios da Governança Ágil. In: *XIII Simpósio Brasileiro de Sistemas de Informação / X Workshop de Teses e Dissertações em Sistemas de Informação*. Lavras/MG: [s.n.], 2017a. p. 80–84.

ALENCAR, G. D.; QUEIROZ, A. A. L.; QUEIROZ, R. J. G. B. Insiders: Análise e Possibilidades de Mitigação de Ameaças Internas. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 3, p. 1–38, 2013a.

ALENCAR, G. D.; QUEIROZ, A. A. L.; QUEIROZ, R. J. G. B. Insiders: Um Fator Ativo na Segurança da Informação. In: *IX Simpósio Brasileiro de Sistemas de Informação - SBSI*. [S.l.: s.n.], 2013b. p. 61–72.

ALENCAR, G. D.; TENORIO JUNIOR, A. J. d. A.; MOURA, H. P. Information Security Policy: A Simplified Model Based on ISO 27002. In: *14th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2017a. p. 4135–4156. ISBN 9788599693131. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4859>.

ALENCAR, G. D.; TENORIO JUNIOR, A. J. d. A.; MOURA, H. P. Theoretical Guidelines for an Agile Model of Governance, Management and Maturity for Information Security. In: *14th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2017b. p. 3661–3690. ISBN 9788599693131. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4799>.

ALEXANDRIA, J. C. S. *Gestão da Segurança da Informação: Uma Proposta para Potencializar a Efetividade da Segurança da Informação em Ambiente de Pesquisa Científica*. 193 p. Tese (Doutorado em Ciências da área de Tecnologia Nuclear – Aplicações) — Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo - SP Brasil, 2009.

ALMEIDA NETO, H. R. *Um Modelo de Maturidade para Governança Ágil em Tecnologia da Informação e Comunicação*. 322 p. Tese (Tese de Doutorado) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2015.

ALMEIDA NETO, H. R.; MOURA, H. P. Mangve maturity model (m3): Proposing a maturity model to support agile governance in information and communication technology. In: *X Simpósio Brasileiro de Sistemas de Informação (SBSI) - Workshop de Teses e Dissertações (WTDSI)*. Londrina - PR, Brasil: [s.n.], 2014. p. 42–54.

ALMEIDA NETO, H. R. D. de; MAGALHÃES, E. M. C. de; MOURA, H. P. de; TEIXEIRA FILHO, J. G. d. A.; CAPPELLI, C.; MARTINS, L. M. F. Avaliação de um Modelo de Maturidade para Governança Ágil em Tecnologia da Informação e Comunicação. *iSys – Revista Brasileira de Sistemas de Informação*, v. 8, n. 4, p. 44–79, 2015b.

ALMEIDA NETO, H. R. de; MAGALHÃES, E. M. C. de; MOURA, H. P. de; TEIXEIRA FILHO, J. G. d. A.; CAPPELLI, C.; MARTINS, L. M. F. Evaluation of a Maturity Model for Agile Governance in ICT using Focus Group. In: *XI Brazilian Symposium on Information System*. Goiânia - GO: [s.n.], 2015a. p. 15–22.

ALTURKI, A.; GABLE, G. G.; BANDARA, W. A Design Science Research Roadmap. In: *Service-Oriented Perspectives in Design Science Research*. Berlin, Heidelberg: Springer, 2011. v. 32, n. 4, p. 107–123. ISBN 978-3-642-20632-0, 978-3-642-20633-7. Disponível em: <http://link.springer.com/10.1007/978-3-642-20633-7_8>.

ANDERSON, R.; MOORE, T. The economics of information security. *Science*, American Association for the Advancement of Science, v. 314, n. 5799, p. 610–613, 2006.

ARAÚJO, W. J. *A Segurança do Conhecimento nas Práticas da Gestão da Segurança da Informação e da Gestão do Conhecimento*. 280 p. Tese (Doutorado em Ciência da Informação) — Universidade de Brasília, Brasília - DF, Brasil, 2009.

BECK, K.; BEEDLE, M.; BENNEKUM, A. van; COCKBURN, A.; CUNNINGHAM, W.; FOWLER, M.; GRENNING, J.; HIGHSMITH, J.; HUNT, A.; JEFFRIES, R.; KERN, J.; MARICK, B.; MARTIN, R. C.; MELLOR, S.; SCHWABER, K.; SUTHERLAND, J.; THOMAS, D. *Manifesto for Agile Software Development*. 2001. Acesso em: 20 mar. 2016. Disponível em: <http://agilemanifesto.org>.

BECKERS, K.; HEISEL, M.; CÔTÉ, I.; GOEKE, L.; GULER, S. Structured pattern-based security requirements elicitation for clouds. In: IEEE. *Eighth International Conference on Availability, Reliability and Security (ARES)*. [S.l.], 2013. p. 465–474.

BENZ, K. H. *Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI: estudos de caso em instituições financeiras*. 200 p. Dissertação (Mestrado em Administração) — Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre - RS, Brasil, 2008.

BERNERS-LEE, T. *The World Wide Web: Past, Present and Future*. 1996. Acesso em: 18 de agosto. de 2018. Disponível em: <http://www.w3.org/People/Berners-Lee/1996/ppf.html>.

BREIER, J.; HUDEC, L. New approach in information system security evaluation. In: IEEE. *First AESS European Conference on Satellite Telecommunications (ESTEL)*. [S.l.], 2012. p. 1–6.

CARCARY, M.; RENAUD, K.; MCLAUGHLIN, S.; O'BRIEN, C. A framework for information security governance and management. *IT Professional*, v. 18, n. 2, p. 22–30, Mar 2016. ISSN 1520-9202.

CARLINI-COTRIM, B. Potencialidades da técnica qualitativa grupo focal em investigações sobre abuso de substâncias. *Revista de Saude Publica*, v. 30, n. 3, p. 285–293, 1996. ISSN 00348910.

CASTELLS, M. *A Sociedade em Rede*. 10ª. ed. [S.l.]: Paz e Terra, 2009. 630 p. ISBN 9788577530366.

CEZAR, A.; CAVUSOGLU, H.; RAGHUNATHAN, S. Outsourcing information security: Contracting issues and security implications. *Management Science*, INFORMS, v. 60, n. 3, p. 638–657, 2013.

CHOI, Y. Human Resource Management and Security Policy Compliance. *International Journal of Human Capital and Information Technology Professionals (IJHCITP)*, v. 8, n. 3, p. 68–81, 2017. Disponível em: <https://www.igi-global.com/article/human-resource-management-and-security-policy-compliance/181830>.

CHOI, Y.; HWANG, H. What increases employees' security compliance intentions? *Journal of Convergence Information Technology (JCIT)*, v. 8, n. 12, p. 189–199, 2013. Disponível em: <http://www.globalcis.org/jcit/ppl/JCIT3910PPL.pdf>.

CHOLEZ, H.; GIRARD, F. Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software: Evolution and Process*, Wiley Online Library, v. 26, n. 5, p. 496–503, 2014.

CHOO, K.-K. R. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, Elsevier Advanced Technology, v. 30, n. 8, p. 719–731, nov 2011. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404811001040>.

COELHO, R. W.; FERNANDES JUNIOR, G.; PROENÇA JUNIOR, M. L. Gaia-mlis: A maturity model for information security. In: *The Eighth International Conference on Emerging Security Information, Systems and Technologies - SECURWARE*. Lisboa, Portugal: [s.n.], 2014. p. 50–55.

CORDEIRO, E. S. d. P. *Fatores críticos de sucesso para o aprimoramento da maturidade da gestão da segurança da informação das instituições federais de ensino superior*. 199 p. Dissertação (Mestrado em Ciência da Computação) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2017.

DA SILVA, C. A. *Gestão da segurança da informação: um olhar a partir da Ciência da Informação*. 99 p. Dissertação (Mestrado em Ciência da Informação) — Pontifícia Universidade Católica de Campinas, Campinas - SP, Brasil, 2009.

DA SILVA, D. R. P.; STEIN, L. M. Segurança da informação: uma reflexão sobre o componente humano. *Ciências & Cognição*, v. 10, p. 46–53, 2007. Disponível em: <http://www.cienciasecognicao.org/pdf/v10/m346130.pdf>.

DATACENTER DYNAMICS. *ISO/IEC 27001: Após processo de auditoria, Matrix passa a integrar seleto grupo de empresas certificadas*. 2017. Acesso em: 30 jan. 2018. Disponível em: <http://www.datacenterdynamics.com.br/focus/archive/2017/03/isoiec-27001-após-processo-de-auditoria-matrix-passa-integrar-seleto-grupo-de->.

DAYANAND, E.; KUMAR, R. K. S. Watershed Based Secret Image Segmentation for Efficient Visual Cryptography. *Journal of Convergence Information Technology (JCIT)*, v. 10, n. 1, p. 122–133, 2015.

DE HAES, S.; GREMBERGEN, W. V. *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*. 2ª. ed. [S.l.]: Springer Publishing Company, Incorporated, 2016. 167 p. ISBN 978-3319374475.

DE LIMA, M. V. M. *Uma metodologia para avaliar a maturidade das configurações de segurança em ambientes de data center: uma estrutura sistemática com multiperspectiva*. 134 p. Dissertação (Mestrado em Ciência da Computação) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2017.

DIMITRIADIS, C. K. Information security from a business perspective – a lottery sector case study. *ISACA Journal*, v. 1, p. 1–6, 2011. Disponível em: <https://www.isaca.org/Journal/archives/2011/Volume-1/Pages/Information-Security-From-a-Business-Perspective-A-Lottery-Sector-Case-Study.aspx>.

DINIZ, I. J. D.; MEDEIROS, M. F.; VERAS, M. Governança de TI: a visão dos concluintes de Administração e Ciências da Computação. *Revista Brasileira de Administração Científica*, v. 3, n. 2, p. 7–24, 2012. Disponível em: <http://arvore.org.br/seer/index.php/rbadm/article/viewArticle/435>.

DRESCH, A.; LACERDA, D. P.; ANTUNES JÚNIOR, J. A. V. *Design Science Research: Método de Pesquisa Para Avanço da Ciência e Tecnologia*. Porto Alegre - RS: Bookman, 2015. 204 p. ISBN 978-85-8260-299-7.

DUMOULIN, T. *COBIT Focus. Governance of Enterprise IT Missing In Action*. 2015. Reportagem: 23 mar. 2015. Acesso em: 17 de jun. de 2018. Disponível em: <http://www.isaca.org/COBIT/focus/Pages/governance-of-enterprise-it-missing-in-action.aspx>.

FARIAS JÚNIOR, I. H. *C2M - A Communication Maturity Model For Distributed Software Development*. 286 p. Tese (Doutorado em Ciência da Computação) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2014.

FAZENDA, R. V.; FAGUNDES, L. L. Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro. In: *XI Brazillian Symposium on Information Systems - SBSI*. [S.l.: s.n.], 2015. p. 307–314.

FERNANDES, A. A.; DE ABREU, V. F. *Implantando a Governança de TI-: Da estratégia à Gestão de Processos e Serviços*. 4ª. ed. Rio de Janeiro - RJ, Brasil: Editora Brasport, 2014. 656 p.

FERREIRA, F. N. F. *Segurança da Informação*. Rio de Janeiro - RJ, Brasil: Ciência Moderna, 2003. 176 p.

FERREIRA, F. N. F.; ARAUJO, M. T. *Política de Segurança da Informação: Guia Prático para Elaboração e Implementação*. 2ª. ed. Rio de Janeiro - RJ, Brasil: Ciência Moderna, 2009. 224 p.

FERREIRA, L. B. C. A revolução das tecnologias de informação e comunicação: conseqüências sociais, econômicas e culturais. *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação*, Campinas - SP, Brasil, v. 7, n. 1, p. 117–127, 2009.

FETAJI, B.; HALILI, F.; FETAJI, M.; EBIBI, M. Semantic Security Analyses of Web Enabled Databases using SQL Injection. *Journal of Convergence Information Technology (JCIT)*, v. 11, n. 4, p. 43–55, 2016.

FONTES, E. *Vivendo a Segurança da Informação: Orientações Práticas para Pessoas e Organizações*. São Paulo - SP: Editora Sicurezza, 2000. 208 p.

FONTES, E. L. G. *Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo. Dissertação*. 157 p. Dissertação (Mestrado em Tecnologia) — Centro Estadual de Educação Tecnológica Paula Souza, São Paulo - SP, Brasil, 2011.

FONTES, E. L. G. *Segurança da Informação: O Usuário Faz a Diferença*. São Paulo - SP, Brasil: Editora Saraiva (Edição Digital), 2012.

GABBAY, M. S. *Fatores Influenciadores da Implementação de Ações de Gestão de Segurança da Informação: um Estudo com Executivos e Gerentes de Tecnologia da Informação em Empresas do Rio Grande do Norte*. 147 p. Dissertação (Mestrado em Ciências em Engenharia de Produção) — Centro de Tecnologia, Programa de Engenharia de Produção, Universidade Federal do Rio Grande do Norte, Natal - RN, Brasil, 2003.

GHAZOUANI, M.; MEDROMI, H.; SAYOUTI, A.; BENHADOU, S. An integrated use of iso27005, mehari and multi-agents system in order to design a comprehensive information security risk management tool. *International Journal of Applied Information Systems – IJAIS*, Foundation of Computer Science FCS - Citeseer, New York, EUA, v. 7, n. 2, p. 10–15, 2014. ISSN 2249-0868.

GIL, A. C. *Métodos e Técnicas de Pesquisa Social*. 5ª. ed. São Paulo - SP: Editora Atlas, 1999. 206 p.

GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 5ª. ed. São Paulo - SP: Editora Atlas, 2010. 200 p.

GOMES, L. D.; GOULART JÚNIOR, C. R.; SIMEÃO, J. L. C.; SOUSA, T. d. J. R. de; SANTANA, A. C. Best Practices in Governance of Information and Tecnology Management. In: *13th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2016. p. 837–857. ISBN 978-8599693124. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/13CONTECSI/paper/view/3781>.

GONÇALVES, A. d. P.; GASPAR, M. A.; CARDOSO, M. V. Maturity Level of Information Technology Governance in Companies Operating in Brazil. In: *13th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2016. p. 3393–3410. ISBN 9788599693124. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/13CONTECSI/paper/view/4122>.

GONDIM, S. M. G. Grupos focais como técnica de investigação qualitativa: desafios metodológicos. *Paidéia*, v. 12, n. 24, p. 149–161, 2003. ISSN 0103-863X.

GREGORY, P.; BARROCA, L.; SHARP, H.; DESHPANDE, A.; TAYLOR, K. The challenges that challenge: Engaging with agile practitioners' concerns. *Information and Software Technology*, Elsevier, v. 77, p. 92–104, 2016.

HEVNER, A. R. A Three Cycle View of Design Science Research A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, v. 19, n. 2, p. 87–92, 2007. ISSN 09050167.

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAM, S. Design Science in the Information Systems. *MIS Quarterly*, v. 28, n. 1, p. 75–105, 2004.

IBGE. *Estatísticas do cadastro central de empresas: 2016*. Rio de Janeiro - RJ, Brasil: Instituto Brasileiro de Geografia e Estatística - IBGE, 2018. 101 p. Coordenação de Metodologia das Estatísticas de Empresas, Cadastros e Classificações. ISBN 978-85-240-4461-8.

ISACA. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows - IL, EUA: ISACA - Information Systems Audit and Control Association, 2012a. 98 p.

ISACA. *COBIT 5 for Information Security*. Rolling Meadows - IL, EUA: ISACA - Information Systems Audit and Control Association, 2012b.

ISACA. *COBIT 5 for Risk*. Rolling Meadows - IL, EUA: ISACA - Information Systems Audit and Control Association, 2013.

ISO. *International Organization for Standardization*. 2017. Acesso em: 20 set. 2017. Disponível em: <http://www.iso.org>.

ISO27K. *Information Security Management Standards*. 2016. Acesso em: 12 jul. 2016. Disponível em: <http://www.iso27001security.com>.

ISSEA. *Systems Security Engineering Capability Maturity Model (SSE-CMM)*. 2018. International Systems Security Engineering Association (ISSEA). Acesso em: 10 mar. 2018. Disponível em: <http://www.sse-cmm.org>.

ITGI. *COBIT 4.1: Framework, Control Objectives, Management Guidelines and Maturity Model*. Rolling Meadows - IL, EUA: ITGI - IT Governance Institute, 2007. 2012 p.

JANSSEN, L. A. *Instrumento de Avaliação de Maturidade em Processos de Segurança da Informação: Estudo de Caso em Instituições Hospitalares*. 166 p. Dissertação (Mestrado em Administração e Negócios) — Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre - RS, Brasil, 2008.

JAPPUR, R. F. *Modelo Conceitual para Criação, Aplicação e Avaliação de Jogos Educativos Digitais*. 296 p. Tese (Doutorado em Engenharia e Gestão do Conhecimento) — Universidade Federal de Santa Catarina, Florianópolis - SC, Brasil, 2014.

JIRASEK, V. Practical application of information security models. *Information security technical report*, Elsevier, v. 17, n. 1-2, p. 1–8, 2012.

JOIA, L.; NETO, A. Government-to-government enterprises in brazil: Key success factors drawn from two case studies. In: *17ª Bled eCommerce Conference eGlobal (BLED 2004)*. [S.l.: s.n.], 2004. p. 1–13.

JOIA, L. A. Developing government-to-government enterprises in brazil: a heuristic model drawn from multiple case studies. *International Journal of Information Management*, Elsevier, v. 24, n. 2, p. 147–166, 2004.

KAROKOLA, G.; KOWALSKI, S.; YNGSTRÖM, L. Towards an information security maturity model for secure e-government services: A stakeholders view. In: *5º International Symposium on Human Aspects of Information Security and Assurance (HAISA)*. Londres, Inglaterra: [s.n.], 2011. p. 58–73.

KERZNER, H. *Gestão de Projetos: As Melhores Práticas*. 3. ed. [S.l.]: Bookman Editora (edição digital), 2017. 796 p.

KIELY, L.; BENZEL, T. V. Systemic security management. *IEEE security & privacy*, IEEE, v. 4, n. 6, 2006.

KITZINGER, J. Qualitative Research: Introducing focus groups. *BMJ*, v. 311, n. 7000, p. 299–302, jul 1995. ISSN 0959-8138. Disponível em: <http://www.bmj.com/cgi/doi/10.1136/bmj.311.7000.299>.

KONTIO, J.; LEHTOLA, L.; BRAGGE, J. Using the focus group method in software engineering: obtaining practitioner and user experiences. *2004 International Symposium on Empirical Software Engineering, ISESE 2004*, p. 271–280, 2004.

KONZEN, M. P. *Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança*. 119 p. Dissertação (Mestrado em Engenharia de Produção) — Centro de Tecnologia, Universidade Federal de Santa Maria, Santa Maria – RS, Brasil, 2013.

KRUCHTEN, P. *The rational unified process: an introduction*. 3. ed. [S.l.]: Addison-Wesley, 2004. 336 p. ISBN 0321197704.

LACERDA, D. P.; DRESCH, A.; PROENÇA, A.; ANTUNES JÚNIOR, J. A. V. Design Science Research: Método de Pesquisa para a Engenharia de Produção. *Gestão & Produção*, São Carlos - SP, v. 20, n. 4, p. 741–761, 2013. ISSN 0104-530X. Disponível em: <http://www.scielo.br/scielo.php?script=sci{_}arttext{&}pid=S0104-530X2013000400001{&}lng=p>.

LANDWEHR, C. E. Computer security. *International Journal of Information Security*, Springer, v. 1, n. 1, p. 3–13, 2001.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. *Revista Economia & Tecnologia*, v. 8, n. 3, p. 38–44, 2005.

LEEM, C. S.; KIM, S.; LEE, H. J. Assessment methodology on maturity level of isms. In: SPRINGER. *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*. [S.l.], 2005. p. 609–615.

LESSING, M. M. Best practices show the way to information security maturity. In: *6th National Conference on Process Establishment, Assessment and Improvement in Information Technology - ImproveIT*. [S.l.: s.n.], 2008. p. 1–9.

LUNA, A. J. H. O.; COSTA, C. P.; MOURA, H. P.; NOVAES, M. A.; NASCIMENTO, C. A. D. C. Agile governance in information and communication technologies: shifting paradigms. *JISTEM - Journal of Information Systems and Technology Management*, SciELO Brasil, v. 7, n. 2, p. 311–334, 2010.

LUNA, A. J. H. O.; KRUCHTEN, P.; MOURA, H. P. Game: Governance for agile management of enterprises: A management model for agile governance. In: IEEE. *8th International Conference on Global Software Engineering Workshops (ICGSEW)*. Bari, Itália, 2013. p. 88–90.

LUNA, A. J. H. O.; KRUCHTEN, P.; MOURA, H. P. Agile Governance Theory: Conceptual Development. In: *12th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2015. p. 1–23. Disponível em: <http://contecsi.fea.usp.br/index.php/contecsi/12CONTECSI/paper/view/2423/2255>.

LUNA, A. J. H. O.; KRUCHTEN, P.; PEDROSA, M. L. G. E.; ALMEIDA NETO, H. R.; MOURA, H. P. State of the Art of Agile Governance: A Systematic Review. *International Journal of Computer Science and Information Technology*, v. 6, n. 5, p. 121–141, oct 2014. ISSN 09754660. Disponível em: <http://dx.doi.org/10.5121/ijcsit.2014.6510>.

LUNA, A. J. H. O.; KRUCHTEN, P.; RICCIO, E. L.; MOURA, H. P. Foundations for an Agile Governance Manifesto: a bridge for business agility. In: *13th International Conference on Information Systems & Technology Management - CONTECSI*. [S.l.: s.n.], 2016. p. 4391–4404. ISBN 9788599693124.

MACCARTHY, M. Information security policy in the US retail payments industry. *Stanford Technology Law Review*, v. 3, 2011. Disponível em: <http://heinonline.org/hol-cgi-bin/get{_}pdf.cgi?handle=hein.journals/stantlr2011{&}sec>.

MACONACHY, W. V.; SCHOU, C. D.; RAGSDALE, D.; WELCH, D. A model for information assurance: An integrated approach. In: UNITED STATES MILITARY ACADEMY, WEST POINT, NY. IEEE. *Proceedings of the 2001 IEEE workshop on information assurance and security*. [S.l.], 2001. v. 310, p. 306–310.

MAHOPO, B.; ABDULLAH, H.; MUJINGA, M. A formal qualitative risk management approach for it security. In: IEEE. *Information Security for South Africa (ISSA)*. Joanesburgo, África do Sul, 2015. p. 1–8.

MANOEL, S. S. *Governança de Segurança da Informação: Como criar oportunidades para o seu negócio*. Rio de Janeiro - RJ: Editora Brasport, 2014. 168 p.

MARCIANO, J. L.; LIMA-MARQUES, M. O enfoque social da segurança da informação. *Ciência da Informação*, v. 35, n. 3, p. 89–98, 2006. ISSN 0100-1965. Disponível em: <http://revista.ibict.br/ciinf/article/view/1116/1250>.

MARCONI, M. d. A.; LAKATOS, E. M. *Fundamentos da Metodologia Científica*. 7. ed. São Paulo - SP: Editora Atlas, 2010. 320 p.

MARQUES, É. V.; MOTA, A. F. Governança da tecnologia da informação: Um estudo bibliométrico em eventos e periódicos brasileiros. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 2, 2013.

MASCARENHAS, S. A. *Metodologia Científica*. São Paulo - SP: Pearson Education do Brasil, 2012. 136 p.

MAYER, J.; FAGUNDES, L. L. Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação. In: *VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSEG*. São Leopoldo - RS, Brasil: [s.n.], 2008. p. 347–356.

MENDONÇA, M. C. S. *A Percepção Gerencial sobre o Modelo de Gestão da Segurança da Informação de uma Empresa Pública de TIC: Perspectiva de Evolução para um Modelo de Governança*. 171 p. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) — Pró-Reitoria de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação, Universidade Católica de Brasília, Brasília - DF, Brasil, 2007.

MENEZES, B. P.; ROCHA, F. G.; MENEZES, P. M.; NASCIMENTO, R. P. C. Strategic Planning Methodology for Information Security – PESEG 1.0. In: *14th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2017. p. 303–330. ISBN 9788599693131. Disponível em: <http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4454>.

MERKER, J. *Data center da Sonda recebe ISO 27001*. 2017. Acesso em: 30 jan. 2018. Disponível em: <https://www.baguete.com.br/noticias/10/02/2017/data-center-da-sonda-recebe-iso-27001>.

MIANI, R. S.; ZARPELÃO, B. B.; MENDES, L. d. S. An Investigation About the Absence of Validation on Security Quantification Methods. In: *XI Brazilian Symposium on Information System*. [s.n.], 2015. p. 315–322. Disponível em: <http://dl.acm.org/citation.cfm?id=2814058.2814109{\%}5Cnhttp://www.lbd.dcc.ufmg.br/colecoes/sbsi/2015/043.>

MODULO. *Pesquisa Nacional de Segurança da Informação*. Rio de Janeiro - RJ, Brasil: [s.n.], 2006. 10ª Edição. Módulo Technology for Risk Management. Acesso em: 07 out. 2016. Disponível em: <http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf>.

MORGAN, D. L. *Focus Groups as Qualitative Research. Qualitative Research Methods Series, v. 16*. 2. ed. Califórnia - EUA: SAGE Publications, 1996. 108 p. ISBN 978-0761903437.

MOUTON, F.; MALAN, M. M.; VENTER, H. S. Social engineering from a normative ethics perspective. In: IEEE. *Information Security for South Africa (ISSA)*. [S.l.], 2013. p. 1–8.

MUNARETTO, L. F.; CORRÊA, H. L.; CUNHA, J. A. C. Um estudo sobre as características do método delphi e de grupo focal, como técnicas na obtenção de dados em pesquisas exploratórias. *Revista de Administração da Universidade Federal de Santa Maria*, Universidade Federal de Santa Maria, v. 6, n. 1, p. 9–24, 2013.

MUTHUKRISHNAN, S. M.; PALANIAPPAN, S. Security metrics maturity model for operational security. In: IEEE. *Computer Applications & Industrial Electronics (ISCAIE), 2016 IEEE Symposium on*. [S.l.], 2016. p. 101–106.

NERY JúNIOR, E. d. J.; MOURA, H. P.; TEIXEIRA FILHO, J. G. A. *Modelos de Maturidade em Gerenciamento de Projetos: Fatores Influenciadores para uma Melhor Escolha*. Curitiba - PR, Brasil: Editora Appris, 2018. 129 p. ISBN 978-85-473-0893-3.

NOBRE, A. C. d. S. *Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: Um Estudo com Gestores Públicos Estaduais no Brasil*. 171 p. Dissertação (Mestrado em Administração) — Universidade Federal do Rio Grande do Norte, Natal - RN, Brasil, 2009.

NORTHCUTT, S.; ZELTSER, L.; WINTERS, S.; KENT, K.; RITCHEY, R. W. *Inside Network Perimeter Security (Inside)*. 2. ed. Indianápolis - IN, EUA: Sams Publishing, 2005. ISBN 0672327376.

OLIVEIRA, M. A. F. *Implantação de uma Gestão da Segurança da Informação Através da Abordagem Seis Sigma*. 191 p. Dissertação (Mestrado em Engenharia de Produção) — Centro de Tecnologia, Universidade Federal de Santa Maria, Santa Maria - RS, Brasil, 2009.

PALMA, F. *As normas da família ISO 27000 - Gestão da Segurança da Informação*. 2016. Acesso em: 30 jan. 2016. Disponível em: <http://www.portalgsti.com.br/2013/12/ISO-27000.html>.

PARK, J.-O.; KIM, S.-G.; CHOI, B.-H.; JUN, M.-S. The study on the maturity measurement method of security management for itsm. In: IEEE. *International Conference on Convergence and Hybrid Information Technology (ICHIT)*. Daejeon, Coreia do Sul, 2008. p. 826–830.

PEFFERS, K.; TUUNANEN, T.; ROTHENBERGER, M. A.; CHATTERJEE, S. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, v. 24, n. 3, p. 45–77, 2007. ISSN 0742-1222. Disponível em: <http://www.tandfonline.com/doi/full/10.2753/MIS0742-1222240302>.

PFLEEGER, C. P.; PFLEEGER, S. L.; MARGULIES, J. *Security in Computing*. 5ª. ed. Upper Saddle River - NJ, Brasil: Editora Prentice Hall (Edição Digital), 2015.

PONTES, E. *Modelo Estendido de Gestão de Risco: uma Abordagem ao retorno de investimento em segurança da informação com previsão de incidentes*. 252 p. Dissertação (Mestrado em Tecnologia Ambiental) — Instituto de Pesquisas Tecnológicas do Estado de São Paulo, São Paulo – SP, 2009.

POSEY, C.; BENNETT, R. J.; ROBERTS, T. L. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, Elsevier Advanced Technology,

v. 30, n. 6-7, p. 486–497, sep 2011. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404811000630>.

PRADO, D. *A Importância da Evolução da Maturidade em Gerenciamento de Projetos*. 2018. Acesso em: 07 jun. 2018. Disponível em: <http://www.maturityresearch.com/novosite/biblio/importancia-da-evolucao.pdf>.

PRADO, D.; OLIVEIRA, W. *Maturidade em Gerenciamento de Projetos - Brasil. Relatório Pesquisa 2017: Relatório Geral - Parte A: Indicadores*. 2018. Acesso em: 07 jun. 2018. Disponível em: <http://www.maturityresearch.com/novosite/2017/download/RelatorioMaturidade2017-Global-Parte-A-Indicadores-V2.pdf>.

PRADO, E. P. V.; MANCINI, M.; BARATA, A. M.; SUN, V. IT Governance in Healthcare Industry Organizations : A Case Study of COBIT Implementation. In: *XII Brazilian Symposium on Information Systems*. Florianópolis - SC: [s.n.], 2016. p. 1–8.

PROENÇA, D.; BORBINHA, J. Information security management systems - a maturity model based on ISO/IEC 27001. In: ABRAMOWICZ, W.; PASCHKE, A. (Ed.). *International Conference on Business Information Systems*. [S.l.], 2018. p. 102–114. ISBN 978-3-319-93931-5.

PURICELLI, R. The underestimated social engineering threat in it security governance and management. *ISACA Journal: Governance & Management of Enterprise IT (GEIT*, ISACA, v. 3, p. 24–28, 2015.

PWC. *Pesquisa global de segurança da informação 2017*. 2017. Acesso em: 02 fev. 2018. Disponível em: <https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2017/pesquisa-global-seguranca-2017.html>.

RADANLIEV, P.; DE ROURE, D.; NURSE, J. R. C.; NICOLESCU, R.; HUTH, M.; CANNADY, S.; MONTALVO, R. M. Integration of cyber security frameworks, models and approaches for building design principles for the internet-of-things in industry 4.0. IET, Londre, Inglaterra, 2018.

RAMLAOUI, S.; SEMMA, A.; DACHRY, W. Achieving a balance between IT Governance and Agility. *IJCSI International Journal of Computer Science*, v. 12, n. 1, p. 89–96, 2015.

RAMOS, A.; BASTOS, A.; LYRA, A.; ANDRUCIOLI, A.; AFFONSO, C.; POGGI, E.; PINTO, E.; BLUM, R. O.; ALEVATE, W.; MARINHO, Z. *Security Officer – 1: Guia Oficial para Formação de Gestores em Segurança da Informação*. 2ª. ed. Porto Alegre - RS, Brasil: Editora Zouk, 2008. 352 p.

RAMOS, I. Q. *Contribuição da Ciência da Informação para Criação de um Plano de Segurança da Informação*. 117 p. Dissertação (Mestrado em Ciência da Informação) — Centro de Ciências Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas - SP, Brasil, 2007.

REA-GUAMAN, Á. M.; SÁNCHEZ-GARCÍA, I. D.; SAN FELIU, T.; CALVO-MANZANO, J. A. Modelos de madurez en ciberseguridad: una revisión sistemática. In: *12th Iberian Conference on Information Systems and Technologies*. Lisboa, Portugal: [s.n.], 2017. p. 284–289. Disponível em: <http://oa.upm.es/48746/>.

REGULWAR, G. B.; GULHANE, V. S.; JAWANDHIYA, P. M. A security engineering capability maturity model. In: IEEE. *International Conference on Educational and Information Technology (ICEIT)*. [S.l.], 2010. p. 306–311.

RIGON, E. A.; WESTPHALL, C. M. Modelo de avaliação da maturidade da segurança da informação. In: *VII Simpósio Brasileiro de Sistemas de Informação - SBSI*. Salvador - BA, Brasil: [s.n.], 2011. p. 93–104.

RIGON, E. A.; WESTPHALL, C. M. Modelo de avaliação da maturidade da segurança da informação. *Revista Eletrônica de Sistemas de Informação*, v. 12, n. 1, p. 1–21, 2013.

RIGON, E. A.; WESTPHALL, C. M.; SANTOS, D. R.; WESTPHALL, C. B. A cyclical evaluation model of information security maturity. *Information Management & Computer Security*, Emerald Group Publishing Limited, v. 22, n. 3, p. 265–278, 2014.

RIOS, O. K. L. *Melhores práticas para implantar política de segurança da informação e comunicação em instituições federais de ensino superior*. 161 p. Dissertação (Mestrado em Ciência da Computação) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2016.

SALAH, D.; PAIGE, R.; CAIRNS, P. An evaluation template for expert review of maturity models. In: SPRINGER. *International Conference on Product-Focused Software Process Improvement*. [S.l.], 2014. p. 318–321.

SALEH, M. F. The three dimensions of security. *International Journal of Security (IJS)*, v. 15, n. 10, p. 85–93, 2011.

SALEH, M. F. Information security maturity model. *International Journal of Computer Science and Security (IJCSS)*, Citeseer, v. 5, n. 3, p. 316–337, 2011b.

SCHNEIER, B. *Interview: Bruce Schneier. InfoSecurity Magazine. BT Counterpane's founder and chief technology officer talks to SA Mathieson at Infosecurity Europe*. 2007. Acesso em: 15 de mar. de 2018. Disponível em: <http://www.schneier.com/news-040.html>.

SÊMOLA, M. *Gestão da Segurança da Informação: Uma visão executiva*. 2ª. ed. Rio de Janeiro - RJ, Brasil: Editora Elsevier Academic (Edição Digital), 2013. 172 p. ISBN 9788535271782.

SHAY, R.; KOMANDURI, S.; KELLEY, P. G.; LEON, P. G.; MAZUREK, M. L.; BAUER, L.; CHRISTIN, N.; CRANOR, L. F. Encountering stronger password requirements: user attitudes and behaviors. In: ACM. *Sixth Symposium on Usable Privacy and Security*. [S.l.], 2010. p. 1–20.

SHIREY, R. *RFC 4949 – Internet Security Glossary, Version 2. The Internet Society*. 2007. Acesso em: 07 set. 2018. Disponível em: <http://www.ietf.org/rfc/rfc4949.txt>.

SILVA, L.; MENEZES, S.; COSTA, A. P. C. S. A model for evaluating information security with a focus on the user. In: *6ª Mediterranean Conference on Information Systems (MCIS)*. Guimarães, Portugal: [s.n.], 2012.

SILVA, L. F. C. P. *Gestão de Riscos em Tecnologia da Informação como fator crítico de sucesso na Gestão da Segurança da Informação dos órgãos da Administração Pública Federal: estudo de caso da Empresa Brasileira de Correios e Telégrafos – ECT*. 160 p. Dissertação (Mestrado em Ciência da Informação e Documentação) — Faculdade de Economia Administração e Ciência da Informação e Documentação, Universidade de Brasília, Brasília - DF, Brasil, 2010.

SILVA, L. S. P.; SAMPAIO, S. C. B.; MOREIRA, R. T.; VASCONCELOS, A. M. L. Proposta de uma abordagem para prestação de serviços de tecnologia da informação à administração pública federal por empresas brasileiras. *Revista de Sistemas e Computação*, v. 6, n. 2, p. 120–134, 2016. ISSN 2237-2903. Disponível em: <http://www.revistas.unifacs.br/index.php/rsc>.

SILVA, M. P.; BARROS, R. M. Maturity Model of Information Security for Software Developers. *IEEE Latin America Transactions*, v. 15, n. 10, p. 1994–1999, oct 2017. ISSN 1548-0992. Disponível em: <http://ieeexplore.ieee.org/document/8071246/>.

SILVA NETO, G. M.; ALENCAR, G. D.; QUEIROZ, A. A. L. Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In: *XI Brazillian Symposium on Information Systems - SBSI*. [S.l.: s.n.], 2015. p. 299–306.

SORDI, J. O. D.; MEIRELES, M.; SANCHES, C. Design Science: Uma Abordagem Inexplorada por Pesquisadores Brasileiros em Gestão de Sistemas de Informação. In: *XXXIV Encontro da ANPAD*. Rio de Janeiro - RJ, Brasil: [s.n.], 2010. p. 1–15.

SSE-CMM PROJECT. *Systems Security Engineering Capability Maturity Model SSE-CMM Model Description Document. Version 3.0*. 2003. Acesso em: 15 mar. 2018. Disponível em: <http://all.net/books/standards/ssecmmv3final.pdf>.

STAMBUL, M. A. M.; RAZALI, R. An assessment model of information security implementation levels. In: IEEE. *International Conference on Electrical Engineering and Informatics (ICEEI)*. Bandung, Indonesia, 2011. p. 1–6.

TARIQ, M. I.; HAQ, I. U.; IQBAL, J. Sla based information security metric for cloud computing from cobit 4.1 framework. *International Journal of Computer Networks and Communications Security*, v. 1, n. 3, p. 95–101, 2013.

THE OPEN GROUP. *Open Information Security Management Maturity Model (O-ISM3)*. Zaltbommel, Holanda: Editora Van Haren Publishing, 2011. 152 p.

THE OPEN GROUP. *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*. Berkshire, Inglaterra: Editora Van Haren Publishing, 2017. 130 p.

THOMAS, M. *COBIT Focus. The Core COBIT Publications: A Quick Glance*. 2015. Reportagem de: 13 abr. 2015. Acesso em: 14 de jun. de 2018. Disponível em: <http://www.isaca.org/COBIT/focus/Pages/the-core-cobit-publications-a-quick-glance.aspx>.

TIPTON, H. F.; NOZAKI, M. K. *Information Security Management Handbook*. Boca Raton - FL, EUA: Auerbach Publications, 2016. Volume 6. ISBN 978-1138199750.

TREMBLAY, M. C.; HEVNER, A. R.; BERNDT, D. J. Focus Groups for Artifact Refinement and Evaluation in Design Research. *Communications of the Association for Information Systems*, v. 26, n. Article 27, p. 599–618, 2010. ISSN 15293181. Disponível em: <http://search.ebscohost.com/login.aspx?direct=true{&}db=bth{&}AN=52686571{&}lang=zh-cn{&}sit>.

US CERT PROGRAM. *2010 CyberSecurity Watch Survey: Cybercrime increasing faster than some company defenses*. 2010. CSO Magazine, CERT Program, Deloitte, U.S. Secret Service. Acesso em: 21 mar. 2018. Disponível em: <http://www.cert.org/archive/pdf/ecrimesummary10.pdf>.

WANG, L.; LIU, F. A trusted measurement model based on dynamic policy and privacy protection in IaaS security domain. *EURASIP Journal on Information Security*, v. 2018, n. 1, p. 1–8, dec 2018. ISSN 2510-523X. Disponível em: <https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-018-0071-1>.

WARKENTIN, M.; WILLISON, R. Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, Palgrave Macmillan UK, v. 18, n. 2, p. 101–105, apr 2009. ISSN 0960-085X. Disponível em: <https://www.tandfonline.com/doi/full/10.1057/ejis.2009.12>.

WIERINGA, R. J. *Design Science Methodology for Information Systems and Software Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. 327 p. ISBN 978-3-662-43838-1. Disponível em: <http://link.springer.com/10.1007/978-3-662-43839-8>.

WOHLIN, C.; AURUM, A. Towards a decision-making structure for selecting a research design in empirical software engineering. *Empirical Software Engineering*, v. 20, n. 6, p. 1427–1455, dec 2015. ISSN 1382-3256. Disponível em: <http://link.springer.com/10.1007/s10664-014-9319-7>.

WOODHOUSE, S. An isms (im)-maturity capability model. In: IEEE. *8th International Conference on Computer and Information Technology Workshops, CIT Workshops*. [S.l.], 2008. p. 242–247.

APÊNDICE A – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

O Senhor(a) está sendo convidado(a) para participar, como voluntário(a), da atividade de Grupo Focal com especialistas na área de Segurança da Informação, como parte integrante da pesquisa doutoral em Ciência da Computação de Gliner Dias Alencar, no Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE), sob a orientação do Prof. Dr. Hermano Perrelli.

Declaro ter ciência e estar esclarecido sobre os seguintes pontos:

1. O trabalho tem por objetivo propor uma estratégia para avaliação da maturidade e priorização da segurança da informação no ambiente corporativo através da utilização, em conjunto, dos principais arcabouços existentes na área.

2. A minha participação nesta pesquisa consistirá em participar como especialistas nas atividades de Grupo Focal com temática principal a área de segurança da informação.

3. Ao participar desse trabalho estarei contribuindo com o levantamento de dados, avaliação e/ou debate para a criação, aprofundamento e/ou melhorias de estratégias e modelos para a área de segurança da informação corporativa.

4. A minha participação nesta etapa de grupo focal deverá ter a duração de, aproximadamente, 2 (duas) horas, podendo ter seu áudio gravado, a critério do pesquisador. No caso de ser gravado, os áudios, após a transcrição ou confecção de relatório, serão devidamente apagados/excluídos.

5. Estou ciente de que não há nenhum valor econômico, a receber ou a pagar, por minha participação.

6. Não terei nenhuma despesa ao participar da pesquisa e poderei deixar de participar ou retirar meu consentimento até 30 de setembro de 2018, sem precisar justificar, e não sofrerei qualquer prejuízo.

7. Meu nome e/ou da empresa será mantido em sigilo, assegurando assim a privacidade e anonimato, sendo tratado, genericamente, como Especialista e/ou Empresa. Bem como que se eu desejar terei livre acesso a todas as minhas informações e esclarecimentos adicionais sobre o estudo.

8. Estou ciente que os dados coletados serão utilizados, única e exclusivamente, para fins acadêmicos e que trechos das atividades poderão ser incluídos na minha tese, relatórios de pesquisa ou em quaisquer outras publicações posteriores, sem citar o nome do especialista ou da empresa.

Eu, _____,
RG nº _____ declaro ter sido informado(a), que estou ciente e concordo em participar, como voluntário(a), da etapa da pesquisa acima descrita.

Recife, 20 de setembro de 2018

_____

Assinatura do participante

APÊNDICE B – FORMULÁRIO DE PESQUISA: SITUAÇÃO DA SEGURANÇA DA INFORMAÇÃO

Formulário de Pesquisa:
Situação da Segurança da Informação

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o nome da empresa ou indícios que a caracterize diretamente.

DADOS DA EMPRESA

Razão Social: _____

Nome Fantasia: _____
(Os dados razão social e nome fantasia serão apenas para controle interno da pesquisa, de preenchimento opcional e não será em nenhum momento divulgado)

Localização da Empresa (Cidade, Estado, País):_____
_____

Da abrangência da empresa:
[ ] Local [ ] Estadual [ ] Regional
[ ] Nacional [ ] Multinacional

Da economia da empresa:
[ ] Privada [ ] Mista [ ] Pública

É uma empresa com atividade fim em Tecnologia da Informação?
[ ] Não [ ] Sim

Quantidade aproximada de funcionários: _____
Quantidade aproximada de estações de trabalho ou notebooks: _____

Ramo de atividade da corporação:
[ ] Setor primário (por exemplo, agricultura, extrativismo ou mineração)
[ ] Setor secundário (por exemplo, indústria)
[ ] Setor terciário (por exemplo, comércio, educação ou serviços)

DADOS DO RESPONDENTE

Você trabalha na área de TI ou no setor responsável pela informática em sua empresa?
[ ] Não [ ] Sim

Você é responsável ou ligado à área que trata a segurança da informação?
[ ] Não [ ] Sim

IMPORTÂNCIA ESTRATÉGICA DA INFORMAÇÃO

O assunto segurança da informação vem sendo debatido de forma sistemática e estratégica na sua empresa nos últimos meses?

[ ] Não, e a empresa não está preparada para discutir este assunto
[ ] Não, porém deverá ser em breve
[ ] Sim, mas ainda não é tratado com a relevância devida
[ ] Sim, é tratada com a relevância devida

Qual a importância para sua corporação das informações guardadas ou manipuladas?
[ ] muito importante [ ] importante [ ] neutro
[ ] pouco importante [ ] nenhuma importância

Quão prejudicial acredita-se ser a perda ou vazamento das informações para sua corporação?
[ ] muito prejudicial [ ] prejudicial [ ] neutro
[ ] pouco prejudicial [ ] não causa prejuízo

Existe uma campanha institucional e frequente sobre segurança da informação na sua empresa?
[ ] Não [ ] Sim

São realizados treinamentos periódicos ou processos de conscientização sobre segurança da informação para os funcionários?
[ ] Não [ ] Sim

Existe um alinhamento do investimento em segurança da informação com os objetivos de negócio da empresa?
[ ] Não estão alinhados [ ] Parcialmente alinhado [ ] Plenamente alinhado

FERRAMENTAS DE SI NA EMPRESA

Que tipos de ferramentas são utilizadas em seu ambiente? (Marque todas as utilizadas)
[ ] Antivírus
[ ] Ferramentas de IPS e/ou IDS
[ ] Ferramentas para controle ou monitoramento de *e-mails*
[ ] Ferramentas para controle ou monitoramento de acesso *Web*
[ ] *Firewall*
[ ] Outras: _____

Qual a(s) principal(is) dificuldades para se implementar as ferramentas ou processos de segurança da informação na sua empresa? Cite até 3.
[ ] Escassez de recursos humanos especializados
[ ] Falta de conscientização dos funcionários
[ ] Falta de ferramentas adequadas
[ ] Falta de Priorização
[ ] Restrições orçamentárias
[ ] Não existem obstáculos
[ ] Outras:_____

RECURSOS HUMANOS E ESTRUTURA ORGANIZACIONAL

Existe uma área, departamento, unidade ou equipe formal dedicada à segurança da informação (seja local ou terceirizada)?
[ ] Não [ ] Sim

Os responsáveis pela segurança da informação trabalham exclusivamente nesta área?
[ ] Não, tratam também de outros assuntos [ ] Sim, trabalham somente na área

Com relação ao conhecimento dos responsáveis e envolvidos com implantação ou administração da segurança da informação, pontue com uma média para a equipe de 0 a 10:

Conhecimentos gerais de SI (conceitos, políticas, normas, auditoria, criptografia, *malwares*):_____

Conhecimento das ferramentas de SI:_____

Os responsáveis pela segurança tiveram capacitação ou formação na área de segurança da informação no último ano?

Para os conhecimentos gerais de Segurança: [ ] Não [ ] Sim
Para as ferramentas de Segurança utilizadas: [ ] Não [ ] Sim

Existe terceirização, contrato ou parceria de pessoas externas envolvidas diretamente na área de segurança da informação?

[ ] Não
[ ] Sim, sendo menos da metade dos recursos humanos
[ ] Sim, sendo mais da metade dos recursos humanos
[ ] Sim, sendo todos os recursos externos

Que tipos de análises ou procedimentos são utilizados e eliminatórios para seleção de colaboradores (funcionários, servidores, terceirizados, estagiários)? (Marque todas as utilizadas)

[ ] Análise de antecedentes criminais [ ] Análise de Currículo/documental
[ ] Avaliação de conduta ética/moral [ ] Entrevista
[ ] Exame médico [ ] Exame psicotécnico
[ ] Outros:_____

SEGURANÇA DA INFORMAÇÃO CORPORATIVA

Na sua expectativa, nos próximos meses os problemas e ameaças relativos à segurança da informação na sua empresa deverão:

[ ] Aumentar [ ] Permanecer os mesmos [ ] Diminuir

E no ambiente global (por exemplo, na Internet):

[ ] Aumentar [ ] Permanecer os mesmos [ ] Diminuir

Esta empresa possui uma política de segurança da informação implementada?

[ ] Não possui nenhuma política de segurança nem previsão de implementação
[ ] Não possui uma política implementada, mas está em processo de formulação e/ou implementação
[ ] Sim, possui uma política de segurança informal implementada
[ ] Sim, possui uma política de segurança formal implementada

Em caso positivo, essa política é divulgada para os funcionários?

[ ] Não é divulgada [ ] Sim, é disponibilizada para quem tiver interesse conhecer [ ] Sim, de maneira formal e é obrigação de todos o conhecimento

Quais os principais obstáculos para que uma política seja implementada de forma eficiente em sua empresa? Cite até 3.

[ ] Escassez de recursos humanos especializados
[ ] Falta de conscientização dos funcionários
[ ] Falta de ferramentas adequadas
[ ] Falta de Priorização
[ ] Restrições orçamentárias
[ ] Não existem obstáculos
[ ] Outros:_____

Quais as principais ameaças às informações na sua empresa? Cite até 3.

[ ] Acessos não autorizados
[ ] Divulgação indevida de senhas
[ ] Engenharia social
[ ] *Hackers*/*crackers*
[ ] Pessoas insatisfeitas ou sem capacitação
[ ] Uso de *notebooks*, *palms*, celulares ou demais equipamentos móveis
[ ] Uso de *pen drives* ou HD externos
[ ] Utilização de senhas fracas
[ ] Vazamento de informações
[ ] Vírus/*malwares*
[ ] Outras:_____

Na sua empresa, quais são os métodos utilizados para segurança do controle de acesso aos meios tecnológicos e informações não públicas?

[ ] Biometria
[ ] Certificado digital
[ ] Usuário e senha
[ ] Outros:_____

Existe uma política de classificação e proteção às informações?

[ ] Não
[ ] Sim

Existem níveis de controles ou políticas diferenciadas para acessar informações mais críticas?

[ ] Não
[ ] Sim

A empresa sofreu algum tipo de ataque visando os recursos tecnológicos ou informações nos últimos dois anos.

[ ] Concordo
[ ] Indeciso
[ ] Discordo

Em caso de ter sofrido algum tipo de ataque, foi possível descobrir as vulnerabilidades exploradas.

[ ] Concordo
[ ] Indeciso
[ ] Discordo

Em caso de ter sofrido algum tipo de ataque, foi possível descobrir a origem do ataque.

[ ] Concordo
[ ] Indeciso
[ ] Discordo

Quais os principais tipos de perdas geradas pelo(s) ataque(s) sofridos por sua empresa? Cite até 3.

[ ] Danos à reputação
[ ] Exposição de informações confidenciais
[ ] Furto de informações sigilosas
[ ] Perdas de propriedade intelectual
[ ] Perdas financeiras
[ ] Perdas operacionais
[ ] Outros:_____

Foi possível mensurar as perdas?
[ ] Não [ ] Sim

Na sua empresa, as pessoas que realizaram ou estavam envolvidas nos ataques, normalmente eram:
[ ] Ex ou atuais funcionários, estagiários ou contratados
[ ] Pessoas sem ligação com a empresa
[ ] Não foi possível detectar

Na sua empresa existem procedimentos para checagem de privilégios dos usuários de redes, assim como procedimento para bloquear a conta ou os privilégios imediatamente após não haver mais a necessidade.
[ ] Concordo [ ] Indeciso [ ] Discordo

Os funcionários são obrigados a trocar a senha periodicamente, colocar senhas fortes e não repeti-las.
[ ] Concordo [ ] Indeciso [ ] Discordo

Os funcionários, ao entrar na empresa, assinam algum termo de compromisso ou documento relativo à confidencialidade de suas senhas e das informações que, por ventura, venha a ter acesso?
[ ] Não [ ] Sim

Caso exista, marque as principais medidas de segurança planejadas para os próximos 12 meses em sua corporação. Cite até 5.
[ ] Adequação a normas, regulamentações ou legislação
[ ] Análise de risco no ambiente de TI
[ ] Análise de vulnerabilidades
[ ] Antivírus corporativo
[ ] Atualizações de sistemas
[ ] Campanha de sensibilização ou conscientização
[ ] Capacitação em SI
[ ] Certificado Digital
[ ] Equipe de resposta a incidentes
[ ] Ferramentas de IPS e/ou IDS
[ ] Ferramentas para controle ou monitoramento de *e-mails*
[ ] Ferramentas para controle ou monitoramento de acesso *Web*
[ ] *Firewall*
[ ] Monitoramento de *logs*
[ ] Plano de Continuidade de negócios
[ ] Política de segurança
[ ] Sistema de *backup*
[ ] Sistema de controle de acesso
[ ] Testes de invasão
[ ] Outras:_____

As normas, modelos e padrões atuais (por exemplo COBIT, ISO 27001, 27002, 27005, 27014, ITIL, etc) atendem às necessidades da empresa?
[ ] Concordo Totalmente [ ] Concordo [ ] Neutro [ ] Discordo [ ] Discordo Totalmente

Quais os principais motivos para as Empresas não adotarem as normas, modelos ou padrões atuais (por exemplo COBIT, ISO 27001, 27002, 27005, ITIL, etc)?

_____

_____

_____

De 1 a 5, onde 1 é o mais baixo nível de segurança e 5 é o mais alto:
Qual o nível de segurança desejado por você para a empresa (1 – 5)?___
Qual o nível de segurança você acredita que a empresa esteja atualmente (1-5)?___

Quais os maiores problemas ou desafios de segurança da informação encontrados na empresa?

_____
_____
_____

APÊNDICE C – FORMULÁRIO DE PESQUISA: CONTROLES ISO/IEC 27001 E 27002

Formulário de Pesquisa:

Controles ISO/IEC 27001 e 27002

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o nome da empresa ou indícios que a caracterize diretamente.

DADOS DA EMPRESA

Razão Social: _____

Nome Fantasia: _____

(Os dados razão social e nome fantasia serão apenas para controle interno da pesquisa, de preenchimento opcional e não será em nenhum momento divulgado)

CONTROLES ISO/IEC 27001 E 27002

No que tange os controles da ISO/IEC 27001 e 27002, exposto abaixo, marque, de 1 a 5, o quão importante ele é para o ambiente de sua empresa:

Onde: 1significa nenhuma importância, 3 como neutro e 5 para muito importante.

Obs.: As informações contidas entre parênteses e em itálico no final de alguns controles, por exemplo, no número 4, são apenas exemplos inserido pelo autor para um melhor entendimento do controle, não fazendo parte, originalmente, do mesmo.

1.(5.1.1) Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

2.(5.1.2) Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

3. (6.1.1) Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

4.(6.1.2) Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

(o solicitante e o aprovador são pessoas distintas)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

5.(6.1.3) Convém que contatos apropriados com autoridades relevantes sejam mantidos.

(fiscais, polícia, bombeiros...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

6.(6.1.4) Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.

(associações profissionais, fóruns de segurança da informação...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

7.(6.1.5) Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

8.(6.2.1) Convém que uma política e medidas que apoiam a segurança da informação seja adotada para gerenciar os riscos decorrentes do uso de dispositivos móveis.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

9.(6.2.2) Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

10.(7.1.1) Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

11.(7.1.2) Convém que as obrigações contratuais com funcionários e partes externas, declarem as suas responsabilidades e a da organização para a segurança da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

12.(7.2.1) 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.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

13.(7.2.2) Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

14.(7.2.3) Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

15.(7.3.1) Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação, sejam definidas, comunicadas aos funcionários ou partes externas e sejam cumpridas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

16.(8.1.1) Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

17.(8.1.2) Convém que os ativos mantidos no inventário tenham um proprietário.

(Notebooks, PC's, Roteadores...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

18.(8.1.3) Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas. (Notebooks, PC's, Roteadores...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

19.(8.1.4) Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.

(Notebooks, PC's, Roteadores...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

20.(8.2.1) Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.

(Notebooks, PC's, Roteadores...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

21.(8.2.2) Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

22.(8.2.3) Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização.

(informação confidencial, restrita ou pública...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

23.(8.3.1) Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.

(Modens, Roteadores, PABX...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

24.(8.3.2) Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

25.(8.3.3) Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

26.(9.1.1) Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

27.(9.1.2) Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

28.(9.2.1) Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição de direitos de acesso.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

29.(9.2.2) Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

30.(9.2.3) Convém que a concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

31.(9.2.4) Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

32.(9.2.5) Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

33.(9.2.6) Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

34.(9.3.1) Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

35.(9.4.1) Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

36.(9.4.2) Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (log-on).

(incluindo autoridades e lideranças...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

37.(9.4.3) Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

38.(9.4.4) Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restrito e estritamente controlado.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

39.(9.4.5) Convém que o acesso ao código-fonte de programa seja restrito.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

40.(10.1.1) Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

41.(10.1.2) Convém que uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

42.(11.1.1) Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

43.(11.1.2) Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

44.(11.1.3) Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

45.(11.1.4) Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

46.(11.1.5) Convém que seja projetado e aplicado procedimentos para o trabalho em áreas seguras.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

47.(11.1.6) Convém que pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

48.(11.2.1) Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

49.(11.2.2) Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

50.(11.2.3) Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.

(ambientes protegidos de raios, inundações...)

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

51.(11.2.4) Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

52.(11.2.5) Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

53.(11.2.6) Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

54.(11.2.7) Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre-gravados com segurança, antes do descarte ou do seu uso.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

55.(11.2.8) Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

56.(11.2.9) Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

57.(12.1.1) Convém que os procedimentos de operação sejam documentados e disponibilizados a todos os usuários que necessitem deles.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

58.(12.1.2) Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

59.(12.1.3) Convém que a utilização dos recursos seja monitorada e ajustada e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

60.(12.1.4) Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

61.(12.2.1) Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

62.(12.3.1) Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

63.(12.4.1) Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

64.(12.4.2) Convém que as informações dos registros de eventos (log) e seus recursos sejam protegidas contra acesso não autorizado e adulteração.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

65.(12.4.3) Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

66.(12.4.4) Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

67.(12.5.1) Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

68.(12.6.1) Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

69.(12.6.2) Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

70.(12.7.1) Convém que os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

71.(13.1.1) Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

72.(13.1.2) Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

73.(13.1.3) Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

74.(13.2.1) Convém que políticas, procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

75.(13.2.2) Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

76.(13.2.3) Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

77.(13.2.4) Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

78.(14.1.1) Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

79.(14.1.2) Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

80.(14.1.3) Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

81.(14.2.1) Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

82.(14.2.2) Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

83.(14.2.3) Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

84.(14.2.4) Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

85.(14.2.5) Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

86.(14.2.6) Convém que as organizações estabeleçam e protejam adequadamente ambientes de desenvolvimento seguros para os esforços de desenvolvimento e integração de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

87.(14.2.7) Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

88.(14.2.8) Convém que os testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

89.(14.2.9) Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

90.(14.3.1) Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

91.(15.1.1) Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

92.(15.1.2) 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.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

93.(15.1.3) Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

94.(15.2.1) Convém que a organização monitore, analise criticamente e audite a intervalos regulares, a entrega dos serviços executados pelos fornecedores.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

95.(15.2.2) Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação de riscos.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

96.(16.1.1) Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

97.(16.1.2) Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

98.(16.1.3) Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização, sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

99.(16.1.4) Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

100.(16.1.5) Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

101.(16.1.6) Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

102.(16.1.7) Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

103.(17.1.1) Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

104.(17.1.2) Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

105.(17.1.3) Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

106.(17.2.1) Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

107.(18.1.1) Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

108.(18.1.2) Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

109.(18.1.3) Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

110.(18.1.4) Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

111.(18.1.5) Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

112.(18.2.1) Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

113.(18.2.2) Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas

áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

114.(18.2.3) Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.

1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

APÊNDICE D – FORMULÁRIO DE PESQUISA: DADOS DOS ESPECIALISTAS

Formulário de Pesquisa:

Dados do Especialista

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente.

Para uma padronização das respostas, solicitamos que todos os tempos sejam inseridos em anos. Bem como informamos que tudo que o questionário trata como Segurança, deve ser entendido como Segurança da Informação.

DADOS DO ESPECIALISTA

Nome: _____
Empresa: _____
Cargo: _____
Tempo no Cargo (anos): _____
Maior cargo assumido na área de segurança ou correlata: _____
Tempo no Cargo: _____
Tempo de experiência profissional com TIC: _____
Deste tempo, quanto foi com Segurança: _____
Maior titulação: ( ) Especialização ( ) Mestrado ( )Doutorado.
Titulação em Andamento: ( ) Mestrando ( ) Doutorando
Alguma titulação foi em segurança (curso ou trabalho de conclusão)? ( ) Sim ( ) Não.
Em caso positivo, qual(is): ( ) Especialização ( ) Mestrado ( ) Doutorado.
Área da titulação em segurança: _____
Tem experiência com Maturidade? ( ) Sim ( ) Não.
Quantidade de Publicações Acadêmicas: ( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7
Quantidade destas publicações acadêmicas que são em Segurança:
( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7
Certificações na área de TIC: ( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7
Quantidade destas certificações são na área de Segurança:
( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7
Tem experiência de ensino na área de TIC? ( ) Sim ( ) Não.
Em caso positivo,
Tipo: ( )Palestrante ( )Professor ( )Coordenador ( )Outros:_____
Nível: ( )Graduação ( )Especialização ( )Mestrado/Doutorado ( )Cursos/Palestras na área Profissional ( ) Outros: _____
Tempo de Experiência com ensino: _____
Alguma destas experiências de ensino é na área de Segurança? ( ) Sim ( ) Não.
Em caso positivo:
Tipo: ( )Palestrante ( )Professor ( )Coordenador ( )Outros: _____
Nível: ( )Graduação ( )Especialização ( )Mestrado/Doutorado ( )Cursos/Palestras na área Profissional ( ) Outros: _____
Tempo de Experiência com ensino em Segurança: _____
O senhor(a) tem interesse em receber informações sobre o resultado final desta pesquisa?
( ) Sim ( ) Não. Em caso positivo, e-mail: _____

APÊNDICE E – FORMULÁRIO DE PESQUISA: AVALIAÇÃO DOS CONTROLES PRÉ-REQUISITOS - RODADA INICIAL

Formulário de Pesquisa:

Pré-requisitos entre os Controles – Versão 1

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente.

DADOS DO ESPECIALISTA

Nome: _____

INTRODUÇÃO

Regras e Recomendações Gerais:

- Com base na análise deste pesquisador foram apontados os pré-requisitos para alguns controles existentes nas normas ISO/IEC 27.001 e 27.002.

Controles (19) das normas ISO/IEC 27.001 e 27.002 elencados com pré-requisitos:

Controle		Título	Pré-requisito	Título
Seção	**5**	**Políticas de segurança da informação**		
Subseção	**5.1**	**Orientação da direção para segurança da informação**		
	5.1.2	Análise crítica das políticas para segurança da informação	5.1.1	Políticas para segurança da informação
Seção	**6**	**Organização da segurança da informação**		
Subseção	**6.2**	**Dispositivos móveis e trabalho remoto**		
	6.2.1	Política para o uso de dispositivo móvel	5.1.1	Políticas para segurança da informação
	6.2.2	Trabalho remoto	5.1.1	Políticas para segurança da informação
Seção	**7**	**Segurança em recursos humanos**		
Subseção	**7.2**	**Durante a contratação**		
	7.2.1	Responsabilidades da direção	7.1.2	Termos e condições de contratação
	7.2.3	Processo disciplinar	5.1.1	Políticas para segurança da informação
Seção	**8**	**Gestão de ativos**		

Subseção	**8.1**	**Responsabilidade pelos ativos**		
	8.1.2	Proprietário dos ativos	8.1.1	Inventário dos ativos
Subseção	**8.2**	**Classificação da informação**		
	8.2.2	Rótulos e tratamento da informação	8.2.1	Classificação da Informação
	8.2.3	Tratamento dos ativos	8.2.1	Classificação da Informação
Subseção	**8.3**	**Tratamento de mídias**		
	8.3.1	Gerenciamento de mídias removíveis	8.2.1	Classificação da Informação
Seção	**9**	**Controle de acesso**		
Subseção	**9.1**	**Requisitos do negócio para controle de acesso**		
	9.1.2	Acesso às redes e aos serviços de rede	9.1.1	Política de controle de acesso
Subseção	**9.4**	**Controle de acesso ao sistema e à aplicação**		
	9.4.1	Restrição de acesso à informação	9.1.1	Política de controle de acesso
Seção	**11**	**Segurança física e do ambiente**		
Subseção	**11.1**	**Áreas seguras**		
	11.1.2	Controles de entrada física	11.1.1	Perímetro de segurança física
Seção	**12**	**Segurança nas operações**		
Subseção	**12.4**	**Registros e monitoramento**		
	12.4.2	Proteção das informações dos registros de eventos (logs)	12.4.1	Registros de eventos
Seção	**17**	**Aspectos da segurança da informação na gestão da continuidade do negócio**		
Subseção	**17.1**	**Continuidade da segurança da informação**		
	17.1.2	Implementando a continuidade da segurança da informação	17.1.1	Planejando a continuidade da segurança da informação
	17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação	17.1.2	Implementando a continuidade da segurança da informação
Seção	**18**	**Conformidade**		
Subseção	**18.1**	**Conformidade com requisitos legais e contratuais**		

	18.1.2	Direitos de propriedade intelectual	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.3	Proteção de registros	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.4	Proteção e privacidade de informações de identificação pessoal	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.5	Regulamentação de controles de criptografia	18.1.1	Identificação da legislação aplicável e de requisitos contratuais

QUESTIONAMENTOS - ESPECIALISTAS

O senhor(a) acredita que os controles selecionados têm a necessidade dos pré-requisitos listados? Em caso negativo, favor apontar o controle e justificar.

O senhor(a) acredita que existe mais algum controle que necessite de pré-requisito? Em caso positivo, favor apontar o controle, o pré-requisito e justificar.

APÊNDICE F – FORMULÁRIO DE PESQUISA: AVALIAÇÃO DOS CONTROLES PRÉ-REQUISITOS - RODADA FINAL

Formulário de Pesquisa:

Pré-requisitos entre os Controles – Versão 2

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente.

DADOS DO ESPECIALISTA

Nome: _____

INTRODUÇÃO

Regras e Recomendações Gerais:

- Com base na análise deste pesquisador foram apontados os pré-requisitos para alguns controles existentes nas normas ISO/IEC 27.001 e 27.002.
- Os 19 controles enviados sofreram alterações conforme detalhado abaixo, resultando em 14 controles expostos na sequência.

Controle	Pré-requisito	Ação	Justificativas dos Especialistas
A.6.2.1	**A.5.1.1**	Excluir	Mesmo sendo uma boa prática a inclusão de tais itens na PSI concebida conforme o controle A.5.1.1, pode ser uma política ou normativo a parte.
A.6.2.2	**A.5.1.1**	Excluir	Mesmo sendo uma boa prática a inclusão de tais itens na PSI concebida conforme o controle A.5.1.1, pode ser uma política ou normativo a parte.
A.7.2.1	**A.7.1.2**	Excluir	Mesmo sendo uma boa prática a unificação em um documento concebida conforme o controle A.5.1.1, pode ser uma política ou normativo a parte.
A.7.2.3	**A.5.1.1**	Excluir	Mesmo sendo uma boa prática a unificação em um documento concebida conforme o controle A.5.1.1, pode ser uma política ou normativo a parte.
A.8.1.2	**A.8.1.1**	Excluir	Mesmo sendo uma boa prática a realização de um inventário inicial concebido conforme o controle A.8.1.1, não é obrigatório a realização do mesmo para a identificação do proprietário.
A.9.1.2	**A.9.1.1**	Excluir	Mesmo sendo uma boa prática a definição dos acessos baseados em uma política concebida conforme o controle A.9.1.1. Procedimentos de autorização, até mesmo formal, podem ser feitos antes da política.
A.9.4.2	**A.9.1.1**	Incluir	Está na definição do controle "onde aplicável pela política de controle de acesso", portanto caso seja realizado a ação do controle A.9.4.2 sem a política proposta no controle A.9.1.1 o mesmo poderá prover melhorias na segurança, mas a ação não estará atendendo ao controle.

Controles (14) das normas ISO/IEC 27.001 e 27.002 elencados com pré-requisitos:

Controle		Título	Pré-requisito	Título
Seção	**5**	**Políticas de segurança da informação**		
Subseção	**5.1**	**Orientação da direção para segurança da informação**		
	5.1.2	Análise crítica das políticas para segurança da informação	5.1.1	Políticas para segurança da informação
Seção	**8**	**Gestão de ativos**		
Subseção	**8.2**	**Classificação da informação**		
	8.2.2	Rótulos e tratamento da informação	8.2.1	Classificação da Informação
	8.2.3	Tratamento dos ativos	8.2.1	Classificação da Informação
Subseção	**8.3**	**Tratamento de mídias**		
	8.3.1	Gerenciamento de mídias removíveis	8.2.1	Classificação da Informação
Seção	**9**	**Controle de acesso**		
Subseção	**9.4**	**Controle de acesso ao sistema e à aplicação**		
	9.4.1	Restrição de acesso à informação	9.1.1	Política de controle de acesso
	9.4.2	Procedimentos seguros de entrada no sistema (log-on)	9.1.1	Política de controle de acesso
Seção	**11**	**Segurança física e do ambiente**		
Subseção	**11.1**	**Áreas seguras**		
	11.1.2	Controles de entrada física	11.1.1	Perímetro de segurança física
Seção	**12**	**Segurança nas operações**		
Subseção	**12.4**	**Registros e monitoramento**		
	12.4.2	Proteção das informações dos registros de eventos (logs)	12.4.1	Registros de eventos
Seção	**17**	**Aspectos da segurança da informação na gestão da continuidade do negócio**		
Subseção	**17.1**	**Continuidade da segurança da informação**		
	17.1.2	Implementando a continuidade da segurança da informação	17.1.1	Planejando a continuidade da segurança da informação

	17.1.3	Verificação, análise crítica e avaliação da continuidade da segurança da informação	17.1.2	Implementando a continuidade da segurança da informação
Seção	**18**	**Conformidade**		
Subseção	**18.1**	**Conformidade com requisitos legais e contratuais**		
	18.1.2	Direitos de propriedade intelectual	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.3	Proteção de registros	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.4	Proteção e privacidade de informações de identificação pessoal	18.1.1	Identificação da legislação aplicável e de requisitos contratuais
	18.1.5	Regulamentação de controles de criptografia	18.1.1	Identificação da legislação aplicável e de requisitos contratuais

QUESTIONAMENTOS – ESPECIALISTAS

O senhor(a) acredita que os controles selecionados têm a necessidade dos pré-requisitos listados? Em caso negativo, favor apontar o controle e justificar.

O senhor(a) acredita que existe mais algum controle que necessite de pré-requisito? Em caso positivo, favor apontar o controle, o pré-requisito e justificar.

APÊNDICE G – FORMULÁRIO DE PESQUISA: PRÉ-AVALIAÇÃO DOS CONTROLES SELECIONADOS - ARTEFATO V. 1

Formulário de Pesquisa:

Pré-Avaliação – Artefato Versão 1 – Especialistas

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente.

DADOS DO ESPECIALISTA

Nome: _____

INTRODUÇÃO

Regras e Recomendações Gerais:

- Os controles propostos serão colocados em uma possível sequência de implementação;
- A implementação dos Controles pode ser feita de forma sequencial ou simultânea, a critério da empresa;
- As diretrizes para a implementação de cada controle devem ser consultadas a partir das respectivas normas da ISO/IEC;
- Alguns controles ou parte deles poderão ser omitidos, dependendo da necessidade da empresa;
- Recomenda-se que a política de segurança da informação, tenha o apoio da direção executiva sendo, aprovada, publicada e comunicada para todos da organização, incluindo a divulgação, das seções necessárias, aos parceiros e entes externos relevantes.

Controles Selecionados para o Modelo simplificado da ISO/IEC 27001 e 27002:

1 - A.5.1.1 Definição de Políticas de Segurança da Informação.
2 - A.6.1.1 Definição de as Responsabilidades
3 - A.6.1.5 Segurança da Informação considerada no gerenciamento de projetos
4 - A.6.2.2 Política e medidas em locais de trabalho remoto.
5 - A.7.1.1 Verificação do Histórico para todos os candidatos a emprego
6 - A.7.2.1 Funcionários e Terceiros praticando a Segurança da Informação
7 - A.8.1.2 Ativos com respectivos proprietários
8 - A.8.1.3 Regras para uso aceitável das informações
9 - A.8.2.1 Classificação da informação
10 - A.8.2.3 Procedimentos para o tratamento de ativos
11 - A.9.1.2 Perfil de acesso dos usuários
12 - A.9.2.1 Registro e cancelamento de usuários
13 - A.9.2.3 Direitos de acesso privilegiado sejam restritos e controlados
14 - A.9.2.4 Controle de concessão de informação de autenticação secreta
15 - A.9.2.5 Análise regular dos proprietários de ativos
16 - A.9.4.2 Procedimento seguro de entrada no sistema (log-on)
17 - A.9.4.4 Controle e restrições de programas utilitários
18 - A.11.1.5 Procedimentos para o trabalho em áreas seguras
19 - A.11.2.4 Manutenção correta dos equipamentos

20 - A.11.2.5 Não retirar equipamentos, informações ou softwares sem autorização
21 - A.11.2.6 Medidas de segurança para ativos fora da organização
22 - A.11.2.7 Análise de todos os equipamentos de mídias antes do descarte
23 - A.12.5.1 Controle de instalação de Software
24 - A.12.6.2 Regras e critérios para a instalação de software pelos usuários
25 - A.13.1.3 Segregação em redes de informação, usuários e serviços
26 - A.15.1.3 Requisitos para acordos com fornecedores relacionados a riscos
27 - A.18.1.1 Documentar todos os requisitos legais e contratuais
28 - A.18.1.2 Procedimentos apropriados legais e contratuais
29 - A.18.1.3 Proteção total dos registros
30 - A.18.1.4 Privacidade e Proteção das informações quando aplicável
31 - A.18.1.5 Controles de criptografia usados em conformidade com todas as leis

QUESTIONAMENTOS - ESPECIALISTAS

O senhor(a) acredita que a estratégia colocada conseguirá abranger todos principais pontos para uma Política de Segurança da Informação que embasará um plano de Governança de Segurança da Informação Ágil? Sim ou Não? Justifique.

Formulário de Pesquisa:

Pré-Avaliação – Artefato Versão 1 – Empresas

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o nome da empresa ou indícios que a caracterize diretamente.

DADOS DA EMPRESA

Razão Social: _____

Nome Fantasia: _____

(Os dados razão social e nome fantasia serão apenas para controle interno da pesquisa, de preenchimento opcional e não será em nenhum momento divulgado)

INTRODUÇÃO

Regras e Recomendações Gerais:

- Os controles propostos serão colocados em uma possível sequência de implementação;
- A implementação dos Controles pode ser feita de forma sequencial ou simultânea, a critério da empresa;
- As diretrizes para a implementação de cada controle devem ser consultadas a partir das respectivas normas da ISO/IEC;
- Alguns controles ou parte deles poderão ser omitidos, dependendo da necessidade da empresa;
- Recomenda-se que a política de segurança da informação, tenha o apoio da direção executiva sendo, aprovada, publicada e comunicada para todos da organização, incluindo a divulgação, das seções necessárias, aos parceiros e entes externos relevantes.

Controles Selecionados para o Modelo simplificado da ISO/IEC 27001 e 27002:

1 - A.5.1.1 Definição de Políticas de Segurança da Informação.
2 - A.6.1.1 Definição de as Responsabilidades
3 - A.6.1.5 Segurança da Informação considerada no gerenciamento de projetos
4 - A.6.2.2 Política e medidas em locais de trabalho remoto.
5 - A.7.1.1 Verificação do Histórico para todos os candidatos a emprego
6 - A.7.2.1 Funcionários e Terceiros praticando a Segurança da Informação
7 - A.8.1.2 Ativos com respectivos proprietários
8 - A.8.1.3 Regras para uso aceitável das informações
9 - A.8.2.1 Classificação da informação
10 - A.8.2.3 Procedimentos para o tratamento de ativos
11 - A.9.1.2 Perfil de acesso dos usuários
12 - A.9.2.1 Registro e cancelamento de usuários
13 - A.9.2.3 Direitos de acesso privilegiado sejam restritos e controlados
14 - A.9.2.4 Controle de concessão de informação de autenticação secreta
15 - A.9.2.5 Análise regular dos proprietários de ativos
16 - A.9.4.2 Procedimento seguro de entrada no sistema (log-on)

17 - A.9.4.4 Controle e restrições de programas utilitários
18 - A.11.1.5 Procedimentos para o trabalho em áreas seguras
19 - A.11.2.4 Manutenção correta dos equipamentos
20 - A.11.2.5 Não retirar equipamentos, informações ou softwares sem autorização
21 - A.11.2.6 Medidas de segurança para ativos fora da organização
22 - A.11.2.7 Análise de todos os equipamentos de mídias antes do descarte
23 - A.12.5.1 Controle de instalação de Software
24 - A.12.6.2 Regras e critérios para a instalação de software pelos usuários
25 - A.13.1.3 Segregação em redes de informação, usuários e serviços
26 - A.15.1.3 Requisitos para acordos com fornecedores relacionados a riscos
27 - A.18.1.1 Documentar todos os requisitos legais e contratuais
28 - A.18.1.2 Procedimentos apropriados legais e contratuais
29 - A.18.1.3 Proteção total dos registros
30 - A.18.1.4 Privacidade e Proteção das informações quando aplicável
31 - A.18.1.5 Controles de criptografia usados em conformidade com todas as leis

QUESTIONAMENTOS - EMPRESAS

O senhor(a) acredita que a estratégia colocada atende às necessidades de sua empresa? Sim ou Não? Justifique.

O senhor(a) implementaria a estratégia colocada em sua empresa? Sim ou Não? Justifique.

APÊNDICE H – FORMULÁRIO DE PESQUISA: AVALIAÇÃO DO MODELO DE PRIORIZAÇÃO E MATURIDADE – ARTEFATO V. 2

Formulário de Pesquisa:

Avaliação do Modelo de Maturidade – Artefato Versão 2

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente.

DADOS DO ESPECIALISTA

Nome: _____

INTRODUÇÃO

O Modelo consiste em:

- Criar uma base de dados de importância dos controles da norma ISO/IEC 27.001 e 27.002. Para isso um questionário com os 114 controles foi enviado às empresas. As empresas marcam a relevância de cada controle em uma escala de 1 a 5, (sendo 1 nenhuma importância, 3 neutro e 5 muito importante). A média (M) das notas de cada controle são calculadas e os controles são ordenados por ela.

- Com base na média (M), os controles são divididos em três estágios: Essencial, Avançado e Completo. O primeiro, Essencial, revela os controles mais importantes (média maior do que 3) e seus pré-requisitos. O segundo, Avançado, aponta os controles com média maior igual a 2 e menor do que 3 e seus pré-requisitos (caso não tenha sido inserido no estágio anterior). Por fim, o estágio Completo que contempla os controles com média abaixo de 2, como mostrado no quadro a seguir. Desta forma, tem-se o estágio Essencial como o inicial. Após atender este estágio pode-se buscar o Avançado e, por fim, após atender os dois estágios anteriores, o Completo que contempla os controles com menor índice de importância de acordo com as empresas. Desta forma, ao atender o estágio completo, a empresa terá atendido a todos os controles, neste caso do Anexo da ISO/IEC 27.001 e ISO/IEC 27.002.

Média do Controle	M>3	2=<M=<3	M<2
Estágio	Essencial	Avançado	Completo
Controles	1, 5, 7	2, 3, 8	4, 6, 9

- Dentro de cada estágio os controles são classificados em níveis, conforme descrição do COBIT.

Nível de Maturidade	**Descrição**
Nível 0 – Processo Inexistente	O processo não foi implementado ou não atingiu seu objetivo. Neste nível, há pouca ou nenhuma evidência de qualquer atingimento sistemático do objetivo do processo.
Nível 1 – Processo Executado	O processo implementado atinge seu objetivo.

Nível 2 – Processo Gerenciado	O processo executado descrito acima agora é implementado de forma administrativa (planejado, monitorado e ajustado) e seus produtos do trabalho são adequadamente estabelecidos, controlados e mantidos.
Nível 3 – Processo Estabelecido	O processo controlado descrito acima agora é implementado utilizando um processo definido capaz de atingir seus resultados.
Nível 4 – Processo Previsível	O processo criado descrito acima opera agora dentro dos limites definidos para produzir seus resultados.
Nível 5 - Otimizado	O processo previsível descrito acima é continuamente melhorado visando o atingimento dos objetivos corporativos pertinentes, atuais ou previstos.

- Desta forma temos um conjunto de controles ordenados, de acordo com a importância dada pelas empresas. Os controles são estratificados em três estágios e cada estágio tem os seis níveis do COBIT. É verificado o nível de cada controle aplicável à empresa. A empresa estará apta a passar de estágio quando todos os controles aplicáveis do estágio atual atingirem, ao menos, o nível 3 (processo estabelecido). O nível de maturidade da empresa é o estágio + a média dos níveis dos controles que a compõem, por exemplo: Essencial 3,5; Avançado 2,8; etc.
- Considera-se como principal vantagem do modelo não tratar todos os controles da igualmente e a maturidade ser alcançada através da nota média dos mesmos. No modelo em questão as empresas devem começar pelos controles considerados mais importantes.

QUESTIONAMENTOS – ESPECIALISTAS

Critério	Concordo Totalmente	Concordo	Neutro	Discordo	Discordo Totalmente
Os níveis de maturidade são suficientes para representar todos os estágios de maturidade do domínio em questão					
Não há sobreposição detectada entre as descrições dos níveis de maturidade					
Os controles são relevantes para o domínio					
Os controles cobrem todos os aspectos impactantes / envolvidos no domínio					
Os controles são corretamente atribuídos ao seu respectivo nível de maturidade					
Os níveis de maturidade são compreensíveis					
As diretrizes de avaliação são compreensíveis					
O esquema de pontuação é fácil de usar					
As diretrizes de avaliação são fáceis de usar					
O modelo de maturidade é útil na realização de avaliações					
O modelo de maturidade é prático para uso na indústria					

Questão 1. O senhor(a) adicionaria algum nível ou estágio de maturidade? Se sim, por favor descreva e justifique.

Questão 2. O senhor(a) atualizaria a descrição do nível de maturidade? Se sim, por favor descreva e justifique.

Questão 3. O senhor(a) adicionaria algum controle? Se sim, por favor descreva e justifique.

Questão 4. O senhor(a) removeria algum dos controles? Se sim, por favor descreva e justifique.

Questão 5. O senhor(a) redefiniria / atualizaria algum dos controles? Se sim, por favor descreva e justifique.

Questão 6. O senhor(a) sugeriria alguma atualização ou melhoria relacionada ao esquema de pontuação? Se sim, por favor descreva e justifique.

Questão 7. O senhor(a) sugeriria alguma atualização ou melhoria relacionada às diretrizes de avaliação? Se sim, por favor descreva e justifique.

Questão 8. O modelo poderia ser mais útil? Se sim, como?

Questão 9. O modelo poderia ser mais prático? Se sim, como?

Questão 10. Você tem mais alguma sugestão, crítica ou algo a comentar?

APÊNDICE I – PLANEJAMENTO DO GRUPO FOCAL: AVALIAÇÃO DA ESTRATÉGIA DE PRIORIZAÇÃO E MATURIDADE - ARTEFATO V. 3

Planejamento do Grupo Focal

Para se planejar um grupo focal torna-se necessário o conhecimento da área a ser pesquisada, os objetivos da pesquisa e da técnica a ser aplicada, neste caso a técnica de grupo focal para a área de segurança da informação visando a atendimento dos objetivos propostos para esta pesquisa de doutorado. Diante disto, o presente planejamento foi baseado nos princípios já descritos nos Capítulos 1, 2 (em especial a Seção 2.6.2) e 3.

Importante destacar que, por não existir consenso na quantidade ideal de participantes para o grupo focal (MUNARETTO; CORRÊA; CUNHA, 2013). Nesta pesquisa buscou-se a quantidade de seis a oito especialistas. A quantidade delimitada visa atender a maioria das recomendações encontradas na literatura e citadas na Seção 2.6.2 desta tese.

Outro ponto que deve estar claro é que não é necessário haver uma votação ou um consenso quanto a um determinado tema ou problemática. É necessário apenas que os especialistas exponham suas opiniões e que elas sejam debatidas, pois o intuito é que exista identificação dos padrões e das tendências preponderantes dos grupos analisados e não detalhar opiniões individuais (MUNARETTO; CORRÊA; CUNHA, 2013).

Para a realização do grupo focal o autor deste trabalho foi o moderador.

Os documentos necessários para avaliar os especialistas e sua autorização para a pesquisa (Apêndices A e D) e, consequentemente, sua habilitação para participar do grupo focal foram recolhidos pelo moderador antes do início da sessão e devidamente avaliados.

O grupo focal foi planejado para durar duas horas e foi executado seguindo a estrutura do roteiro descrito a seguir:

- Confirmação das características dos especialistas (Apêndice D);
- Autorização dos especialistas (Apêndices A);
- Confirmação da quantidade de especialistas, atendendo ao método proposto. No caso da presente pesquisa, 6 especialistas formaram o grupo focal;
- Apresentação do Autor/Moderador;
- Apresentação da pesquisa (explicações gerais da pesquisa de doutorado, pergunta de pesquisa, objetivo, método utilizado, etapas e grupo focal);
- Apresentação da agenda e etapas da atividade do grupo focal;
- Apresentação de cada um dos especialistas;
- Apresentação geral da estratégia proposta;
- Apresentação dos estágios da estratégia;
- Apresentação dos níveis de maturidade da estratégia;

- Apresentação das possíveis formas de se escolher o nível mínimo para cada controle (fixo ou através da matriz de risco);
- Apresentação das formas de implantação da estratégia (modelo de maturidade comparável ou aplicação independente);
- Discussão dos temas;
- Encerramento, agradecimentos e coffee break.

As ações supracitadas foram realizadas pelo moderador, exceto a apresentação dos especialistas. Neste ponto cada especialistas se apresentou.

Foi explicado pelo moderador aos especialistas que o moderador poderia, em alguns momentos, intervir no debate como forma de direcionar aos assuntos de interesse, cumprir o tempo estimado e manter o foco.

Os questionamentos e temas levados pelo moderador para o grupo focal foram baseados na estrutura proposta no trabalho de Salah, Paige e Cairns (2014).

A estrutura do grupo focal que o autor pretendia debater era composta por cinco temáticas da estratégia concebida, a saber: os estágios, os níveis de maturidade, nível mínimo para os controles, formas de aplicação e questionamentos gerais.

Para cada temática das questões (estágio, nível, fomas de aplicação, etc) o moderador inseria um slide de apresentação para relembrar aos especialista aquele item da estratégia proposta e facilitar o debate. As questões que abordaram as temáticas que o autor pretendia debater são expostos a seguir:

- ESTÁGIO: O que o senhor(a) acha da quantidade de estágios utilizadas?
- ESTÁGIO: O que o senhor(a) acha da nomenclatura de estágios utilizada adequada (Essencial, Intermediário, Avançado e Completo)?
- NÍVEL DE MATURIDADE: O que o senhor(a) acha da utilização dos níveis do COBIT nesta estratégia? É aplicável no contexto de segurança?
- NÍVEL DE MATURIDADE: O que senhor(a) acha da quantidade de níveis utilizada?
- NÍVEL DE MATURIDADE: O senhor(a) acredita que a nomenclatura dos níveis é adequada (Nível 0 - Inexistente, Nível 1 - Inicial, Nível 2 - Repetível, Nível 3 - Definido, Nível 4 - Gerenciado, Nível 5 – Otimizado)?
- NÍVEL MÍNIMO PARA OS CONTROLES: O que o senhor(a) acha do nível 3 (definido) escolhido como referência?
- NÍVEL MÍNIMO PARA OS CONTROLES: O que o senhor(a) acha da utilização do padrão ISO/IEC 27005 como base para calcular o risco nesta estratégia?

- NÍVEL MÍNIMO PARA OS CONTROLES: O que o senhor(a) acha sobre a quantidade de linhas (Probabilidade) e colunas (Impacto) da matriz?
- NÍVEL MÍNIMO PARA OS CONTROLES: O que o senhor(a) acha sobre a nomenclatura utilizada para os níveis de probabilidade e impacto (Baixa, Média, Alta)?
- NÍVEL MÍNIMO PARA OS CONTROLES: O que você acha sobre os pesos utilizados para cada nível de probabilidade e impacto (Baixa = 1, Média = 2, Alta =3)?
- NÍVEL MÍNIMO PARA OS CONTROLES: O que o senhor(a) acha sobre a forma de definição do nível mínimo de maturidade a ser alcançado, calculando a soma da probabilidade e impacto e correlacionando com o nível do COBIT?
- FORMAS DE APLICAÇÃO: O que o senhor(a) acha da estratégia de implementação (modelo de maturidade comparável e aplicação independente)?
- QUESTIONAMENTOS GERAIS: O senhor(a) acredita que a estratégia proposta é capaz de avaliar a maturidade da organização?
- QUESTIONAMENTOS GERAIS: O senhor(a) acredita que a estratégia proposta é capaz de auxiliar as organizações a alcançar suas metas e objetivos?
- QUESTIONAMENTOS GERAIS: O senhor(a) acredita que a estratégia proposta é capaz de auxiliar as organizações a priorizar suas ações na área de segurança da informação?
- QUESTIONAMENTOS GERAIS: O senhor(a) acredita que a estratégia proposta auxilia a organização na Governança e ações para alinhamento estratégico da Segurança da Informação?
- QUESTIONAMENTOS GERAIS: O senhor(a) acredita que a estratégia proposta auxilia a organização na construção de uma PSI ou SGSI, sendo mais fácil do que a aplicação pura das ISO/IEC 27001 e 27002?
- QUESTIONAMENTOS GERAIS: O senhor(a) consegue visualizar alguma outra aplicação para a presente estratégia?
- QUESTIONAMENTOS GERAIS: O modelo poderia ser mais útil?
- QUESTIONAMENTOS GERAIS: O modelo poderia ser mais prático?
- QUESTIONAMENTOS GERAIS: O senhor(a) tem mais alguma sugestão, crítica ou algo a comentar?

Como forma de atingir os objetivos, no final de cada rodada de respostas o moderador lançava questões de sondagem e cobertura, tais como “Alguma coisa mais vem à sua mente?”, "Por quê?", "Os outros especialistas concordam com esse pensamento?", "Alguém consegue pensar uma forma diferente?", etc. Tal técnica visa o esgotamento do assunto em meio ao grupo, como aborda Munaretto, Corrêa e Cunha (2013).

O moderador também exercia o papel de incentivar a participação de todos os especialistas, evitando a preponderância de um ou parte do grupo.

Ressalta-se a dificuldade, nos dias atuais, de se conseguir encontrar especialistas com disponibilidade em participar de tais ações, bem como de compatibilizar a agenda para encontrar um horário possível para todos do grupo, além das possíveis eventualidades. Na presente pesquisa, depois de um árduo esforço, foi possível encaixar o horário, interesse e disponibilidade com oito especialistas. Este número estava confirmado até a noite anterior do evento. Quando um especialista afirmou a sua impossibilidade de participação por questões de saúde e, no dia da sessão, outro especialista também não participou por problemas de saúde com familiar.

Tais fatos devem ser previstos como possíveis riscos no planejamento do grupo focal. Nesta pesquisa, por estar prevista a realização com o número máximo (oito), foi possível suportar as duas perdas sem alteração do método proposto.

APÊNDICE J – TRABALHOS RESULTANTES DAS REVISÕES DA LITERATURA

Trabalhos resultantes das Revisões da Literatura

Os trabalhos estão ordenados de forma crescente pelo ano de publicação e não se configura como nível de importância. Os trabalhos listados foram inseridos pelas etapas de revisão realizadas pelo autor: etapa Ad hoc e o MSL publicado em Alencar *et al.* (2018b, 2018c), e as revisões sistemáticas da literatura: Rios (2016), De Lima (2017), Cordeiro (2017) Rea-Guaman et al. (2017).

Nº	Referência	Ano	Inserido por
1	SIPONEN, M.T. Maturity Criteria for Developing Secure IS and SW: Limits, and Prospects. In: Ghonaimy M.A., El-Hadidi M.T., Aslan H.K. (eds) **Security in the Information Society. IFIP Advances in Information and Communication Technology**, v. 86. Springer, Boston, MA, 2002.	2002	Rea-Guaman et al. (2017)
2	LEEM, C. S.; KIM, S.; LEE, H. J. Assessment Methodology on Maturity Level of ISMS. In: **9th International Conference on Knowledge Based Intelligent Information and Engineering Systems**, v. 3683, p. 609–615, 2005.	2005	De Lima (2017)
3	MENDES, R.; MOREIRA, M. A. R. Itil on Security Information Management. In: **5th International Conference on Information Systems & Technology Management - CONTECSI 2008**, **Anais**...	2008	Alencar *et al.* (2018b, 2018c)
4	VIANEZ, M. S.; SEGOBIA, R. H.; CAMARGO, V. Segurança de Informação: Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005. **Revista de Informática Aplicada**, [s. l.], v. 4, n. 1, p. 33–44, 2008.	2008	Alencar *et al.* (2018c)
5	WOODHOUSE, S. An ISMS (im)-maturity capability model. In: **8th IEEE International Conference on Computer and Information Technology Workshops (CIT Workshops 2008), 2008, Anais...**	2008	Etapa Ad hoc do autor e De Lima (2017)
6	LESSING, M. M. Best practices show the way to Information Security Maturity. In: **6th National Conference on Process Establishment, Assessment and Improvement in Information Technology (ImproveIT 2008)**, p. 1–9, 2008.	2008	Etapa Ad hoc do autor e De Lima (2017)
7	BRETERNITZ, V. J.; NAVARRO NETO, F.; NAVARRO, A. F. Gerenciamento de Segurança Segundo ITIL: Um Estudo de Caso em uma Organização Industrial de Grande Porte. **Revista Eletrônica de Sistemas de Informação**, [s. l.], v. 8, n. 2, p. 4, 2009.	2009	Alencar *et al.* (2018b, 2018c)
8	MACHADO, C. A. N. et al. Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico. In: **V Simpósio Brasileiro de Sistemas de Informação - SBSI 2009**, **Anais**...	2009	Alencar *et al.* (2018b, 2018c)

9	OLIVEIRA, M. A. F.; NUNES, R. C.; ELLWANGER, C. Uma Metodologia Seis Sigma para Implantação de uma Gestão de Segurança da Informação Centrada na Percepção dos Usuários. In: **IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSEG 2009, Anais**...	2009	Etapa Ad hoc do autor e Alencar *et al.* (2018b, 2018c)
10	ALEXANDRIA, J. C. S.; QUONIAM, L. M. Proposal to Structure the Information Security Management in a Scientific Research Environment. In: **7th International Conference on Information Systems & Technology Management - CONTECSI 2010, Anais**...	2010	Cordeiro (2017) e Alencar *et al.* (2018b, 2018c)
11	KROLL, J. et al. Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008. In: **VI Simpósio Brasileiro de Sistemas de Informação - SBSI 2010**, **Anais**... [s.l: s.n.]	2010	Alencar *et al.* (2018b, 2018c)
12	LUNA, A. J. H. O.; COSTA, C. P.; MOURA, H. P.; NOVAES, M. A.; NASCIMENTO, C. A. D. C. Agile governance in information and communication technologies: shifting paradigms**. JISTEM-Journal of Information Systems and Technology Management**, SciELO Brasil, v. 7, n. 2, p. 311–334, 2010.	2010	Etapa Ad hoc do autor
13	MAYER, J.; FAGUNDES, L. L. Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação. In: **VI Simpósio Brasileiro de Sistemas de Informação - SBSI 2010, Anai**s...	2010	Alencar *et al.* (2018b, 2018c)
14	NOBRE, A. C. S.; RAMOS, A. S. M.; NASCIMENTO, T. C. Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: um estudo com gestores públicos estaduais no Brasil. In: **XXXIV Encontro da ANPAD 2010**, **Anais**...	2010	Alencar *et al.* (2018c)
15	ROQUE, A. S.; NUNES, R. C.; SILVA, A. D. Proposition of a Dynamic Model for Managing Security Information on Industrial Environments. **Revista Eletrônica de Sistemas de Informação**, [s. l.], v. 9, n. 2, p. 7, 2010.	2010	Alencar *et al.* (2018b, 2018c)
16	ZANICHELLI, A. S.; MARTIMIANO, L. A. F. Definição de uma Política de Segurança para um Ambiente de Desenvolvimento Distribuído de Software. In: **Workshop de Trabalhos de Iniciação Científica e De Graduaçãi - WTICG / X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSEG 2010**, **Anais**...	2010	Alencar *et al.* (2018b, 2018c)
17	REGULWAR, G. B.; GULHANE, V. S.; JAWANDHIYA, P. M. A Security Engineering Capability Maturity Model. In: **2010 International Conference on Educational and Information Technology, 2010, Anais...**	2010	De Lima (2017)
18	JOHNSON, L.; PINTO, J. S. P. Proposta de um Programa de Segurança da Informação para as Autarquias Federais. In: **Congresso InfoBrasil TI e Telecom**, **2010, Anais**... [s.l: s.n.]	2010	Cordeiro (2017)

19	PARANHOS, M. M. **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.	2010	Etapa Ad hoc do autor e Cordeiro (2017)
20	TORRES, M. T.; ANHESINE, M. W.; AZZOLINI JUNIOR, W. A Gestão da Segurança da Informação e seu Alinhamento Estratégico na Organização. **Interface Tecnológica,** v.7, n.1., 2010.	2010	Cordeiro (2017)
21	OUEDRAOGO, M.; MOURATIDIS, H.; DUBOIS, E.; KHADRAOUI, D. Information systems security criticality and assurance evaluation. **Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6059 LNCS**, p. 38–54, 2010.	2010	Rea-Guaman et al. (2017)
22	KNORST, A. M.; VANTI, A. A. Alinhamento Estratégico entre Objetivos de Negócio e Segurança da Informação no Contexto da Governança de Tecnologia da Informação (TI): Um Estudo no Setor de Automação Industrial. In: **8th International Conference on Information Systems & Technology Management - CONTECSI 2011, Anais**...	2011	Alencar *et al.* (2018b, 2018c)
23	GILLIES, A. Improving the quality of information security management systems with ISO27000. **The TQM Journal**. v. 23, No. 4, p. 367-376. 2011.	2011	Cordeiro (2017)
24	SALEH, M. F. Information Security Maturity Model. **International Journal of Computer Science and Security (IJCSS)**, v. 5, n. 3, 2011.	2011	Etapa Ad hoc do autor e Cordeiro (2017)
25	STAMBUL, M. A. M.; RAZALI, R. An Assessment Model of Information Security Implementation Levels. **In: 2011 International Conference on Electrical Engineering an Informatics, 2011**, **Anais...**	2011	Cordeiro (2017)
26	YILDIRIM, E. Y.; AKALP, G.; AYTAC, S.; BAYRAM, N. Factors incluencing information security management in small-and-medium-sized enterprises: A case study from Turkey. **International Journal of Information Management**, v. 31, n. 4, p.360-365, 2011.	2011	Etapa Ad hoc do autor e Cordeiro (2017)
27	ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Controles e práticas de segurança da informação em um instituto de pesquisa federal. In: **2011 Simpósio de Excelência em Gestão e Tecnologia, 2011, Anais...**	2011	Rios (2016)
28	CARDOSO, M. O. **Propostas de Diretrizes para o Desenvolvimento de uma Política de Segurança da Informação e Comunicações para o Centro de Processamento de Dados Distrito Federal da Dataprev Baseadas na Norma ABNT NBR ISO/IEC 27002:2005**. Brasília: Universidade de Brasília. Trabalho de Especialização, Departamento de Ciência da computação, 2011.	2011	Rios (2016)

29	FAILY, S.; FLECHAIS, I. User-centered information security policy development in a post-stuxnet world. In: **6th International Conference on Availability, Reliability and Security (ARES), 2011, IEEE. Anais...**	2011	Rios (2016)
30	FONTES, E. L. G.. **Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo**. Centro Estadual de Educação Tecnológica Paula Souza. Dissertação de mestrado. São Paulo-SP. 2011.	2011	Etapa Ad hoc do autor e Rios (2016)
31	SENGUPTA, A.; MAZUMDAR, C.; BAGCHI, A. A Methodology for Conversion of Enterprise-Level Information Security Policies to Implementation-Level Policies/Rule. In: **2nd International Conference on Emerging Applications of Information Technology (EAIT), 2011, Anais...**	2011	Rios (2016)
32	TUYIKEZE, T.; POTTAS, D. An Information Security Policy Development Life Cycle. In: **South African Information Security Multi-Conference, 2010, Anais...**	2011	Rios (2016)
33	SALEH, M. F. The Three Dimensions of Security. **International Journal of Security (IJS)**, v. 15, n. 10, p. 85-93, 2011.	2011	Etapa Ad hoc do autor
34	DIMITRIADIS, C. K. Information Security From a Business Perspective – A Lottery Sector Case Study. **ISACA Journal: Virtualization Security, Challenges and Solutions**, v. 1, p 1-6, 2011.	2011	Etapa Ad hoc do autor
35	KAROKOLA, G.; KOWALSKI, S.; YNGSTRÖM, L. Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. In: **5th International Symposium on Human Aspects of Information Security and Assurance - HAISA, 2011, Anais...**	2011	Etapa Ad hoc do autor
36	RIGON, E. A.; WESTPHALL, C. M. Modelo de avaliação da maturidade da segurança da informação. In: **VII Simpósio Brasileiro de Sistemas de Informação - SBSI**, **2011, Anais...**	2011	Etapa Ad hoc do autor
37	ALEXANDRIA, J. C. S. A Picture of Information Security in Public Institutions of Scientific Research in Brazil. In**: 9th International Conference on Information Systems & Technology Management - CONTECSI 2012**, **Anais**...	2012	Alencar *et al.* (2018b, 2018c)
38	LEE, S.; CHUNG, T.; CHOI, M. An empirical study of quality and cost based security engineering. **Information Security Practice and Experience**, p. 379–389. 2012.	2012	Rea-Guaman et al. (2017)
39	DZAZALI, S.; ZOLAIT, A. H. Assessment of information security maturity: An exploration study of Malaysian public service organizations. **Journal of Systems and Information Technology**. v. 14, n. 1, p. 23-57, 2012.	2012	Cordeiro (2017)

40	NORMAN, A. A.; YASIN, N. M. Information Systems Security Management (ISSM) Success Factor: Restrospection From the Scholars. In: **11th European Conference on Information warfare and security, 2012. Anais...**	2012	Cordeiro (2017)
41	ANAND, V.; SANIIE, J.; ORUKLU, E. Security policy management process within Six Sigma framework. **Journal of Information Security**, v. 3, 49-58, 2012.	2012	Rios (2016)
42	ARAUJO, Wagner Junqueira De. Leis, decretos e normas sobre Gestão da Segurança da Informação nos órgãos da Administração Pública Federal. **Informação & Sociedade: Estudos**, v. 22, p. 13-24, 2012.	2012	Rios (2016)
43	NASCIMENTO, E. C. L. Fatores culturais e estruturais que impactam na implantação da política de segurança da informação: um estudo de caso sobre o Ministério do Desenvolvimento Agrário. **Universitas: Gestão e TI**, v. 2, n. 1, 2012.	2012	Rios (2016)
44	JIRASEK, V. Practical Application of Information Security Models. **Information security technical report**, v. 17, n. 1, p. 1-8, 2012.	2012	Etapa Ad hoc do autor
45	SILVA, L.; MENEZES, S.; COSTA, A. P. C. S. A model for evaluating information security with a focus on the user. In: **6th Mediterranean Conference on Information Systems - MCIS, 2012, Anais...**	2012	Etapa Ad hoc do autor
46	ALENCAR, G. D.; QUEIROZ, A. A. L.; QUEIROZ, R. J. G. B. Insiders: Um Fator Ativo na Segurança da Informação. In: **IX Simpósio Brasileiro de Sistemas de Informação - SBSI 2013, Anais...**	2013	Alencar *et al.* (2018b, 2018c)
	ADLER, R. M. A dynamic capability maturity model for improving cyber security. In: **2013 IEEE International Conference on Technologies for Homeland Security (HST), 2013, Anais...**	2013	Rea-Guaman et al. (2017)
	CASTILHO, S. D. Política de segurança da informação aplicada em uma instituição de ensino mediante análise de risco. **RETEC - Revista de Tecnologias**, v. 5, n. 2, 2013.	2013	Rios (2016)
	DISTERER, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. **Journal of Information Security**, v. 4, n. 2, p. 92-100, 2013.	2013	Cordeiro (2017)
47	GUALBERTO, E. S. et al. Proposição de uma Ontologia de Apoio à Gestão de Riscos de Segurança da Informação. **ISys - Revsta Brasileira de Sistemas de Informação**, v. 6, n. 1, p. 30–43, 2013.	2013	Alencar *et al.* (2018b, 2018c)
48	LUNA, A. J. H. O.; KRUCHTEN, P.; MOURA, H. P. Game: Governance for agile management of enterprises: A management model for agile governance. **In: IEEE. 8th International Conference on Global Software Engineering Workshops (ICGSEW), 2013, Anais...**	2013	Etapa Ad hoc do autor

49	MATTES, I. V.; PETRI, S. M. Accounting Information Security: Procedures for the Preparation of a Security Policy Based on ISO 27001 and ISO 27002. In: **10th International Conference on Information Systems & Technology Management - CONTECSI 2013, Anais**...	2013	Rios (2016) e Alencar *et al.* (2018b, 2018c)
50	RIGON, E. A.; WESTPHALL, C. M. Modelo de Avaliação da Maturidade da Segurança da Informação. **Revista Eletrônica de Sistemas de Informaçao**, v. 12, n. 1, p. 1-19, 2013.	2013	Etapa Ad hoc do autor e Alencar *et al.* (2018b, 2018c)
53	QUINTELLA, H. L. M.; BRANCO, M. P. O. Fatores Críticos de Sucesso em Segurança da Informação em um Órgão da Administração Pública Federal. In: **II Simpósio Internacional de Gestão de Projetos (Singep), 2013, Anais....**	2013	Rios (2016) e Cordeiro (2017)
55	TARIQ, M. I; HAQ, I. U; IQBAL, J. SLA Based Information Security Metric for Cloud Computing from COBIT 4.1 Framework. **International Journal of Computer Networks and Communications Security**, v. 1, n. 3, p. 95 – 101, 2013.	2013	Etapa Ad hoc do autor
56	ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M.; ALBUQUERQUE, E. S. Segurança da Informação em um Instituto de Pesquisa: Uma Análise Utilizando a Norma ISO/IEC 27002:2005. **Revista Formadores: Vivências e Estudos**, , v. 7, n. 2, p. 71–89, 2014.	2014	Alencar *et al.* (2018c)
57	ALMEIDA NETO, H. R.; DE MOURA, H. P. MAnGve Maturity Model (M3): Proposing a Maturity Model to Support Agile Governance in Information and Communication Technology. In: **Workshop de Teses e Dissertações em Sistemas de Informação - WTDSI / X Simpósio Brasileiro de Sistemas de Informação - SBSI, 2014, Anais...**	2014	Etapa Ad hoc do autor
58	ALSHAIKH, M.; AHMAD, A.; MAYNARD, S. B.; SHANTON, C. Towards a Taxonomy of Information Security Management Practices in Organisations. In: **25th Australian Conference on Information Systems, 2014, Anais...**	2014	Cordeiro (2017)
59	BARCLAY, C. Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). In: **2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?, 2014, Anais...**	2014	Rea-Guaman et al. (2017)
60	BERGMANN, F. B.; SILVEIRA, M. S. Human Aspects of Information Security Privacy and Trust. **Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)**, v. 8533, p. 387-399, 2014.	2014	Etapa Ad hoc do autor e Rea-Guaman et al. (2017)
61	CHOLEZ, H.; GIRARD, F. Maturity assessment and process improvement for information security management in small and medium enterprises. **Journal of Software: Evolution and Process**, v. 26, n. 5, p. 496-503, 2014.	2014	Cordeiro (2017)

62	COELHO, R. W.; FERNANDES, G.; PROENÇA, M. L. GAIA-MLIS: A Maturiy Model for Information Security. In: **SECURWARE 2014: 8th International Conference on Emerging Security Information, System and Technologies, 2014, Anais...**	2014	Cordeiro (2017)
63	FERNANDES, A. A.; DE ABREU, V. F. **Implantando a Governança de TI: Da estratégia à Gestão de Processos e Serviços.** 4ª. ed. Rio de Janeiro - RJ, Brasil: Editora Brasport, 2014. 656 p.	2014	Etapa Ad hoc do autor
64	FERNANDES, F. C.; CARPES, A. M. S.; DIEL, E. H. Information Security Management: A Case Study in a Brazilian Financial Institution. In: **11th International Conference on Information Systems & Technology Management - CONTECSI 2014, Anais**...	2014	Alencar *et al.* (2018b, 2018c)
65	FONTES, E. L. G.. Alignment of Information Security with Business Areas - Contribution of NBR ISO/IEC 27002:2013. In: **11th International Conference on Information Systems & Technology Management - CONTECSI 2014**, **Anais**...	2014	Alencar *et al.* (2018b, 2018c)
66	LUNA, A. J. H. O.; KRUCHTEN, P.; PEDROSA, M. L. G. E.; ALMEIDA NETO, H. R.; MOURA, H. P. State of the Art of Agile Governance: A Systematic Review. **International Journal of Computer Science and Information Technology**, v. 6, n. 5, p. 121–141, 2014.	2014	Etapa Ad hoc do autor
67	MOETI, M.; KALEMA, B. M. Analytical Hierarchy Process Approach for the Metrics of Information Security Management Framework. In: **6th International Conference on Computational Intelligence, Communication Systems and Networks, 2014, Anais...**	2014	Cordeiro (2017)
68	TUYIKEZE, T.; FLOWERDAY, S.. Information Security Policy Development and Implementation: A Content Analysis Approach. In: **International Symposium on Human Aspects of Information Security and Assurance HAISA, 2014, Anais...**.	2014	Rios (2016)
69	RIGON, E. A. et al. A Cyclical Evaluation Model of Information Security Maturity. **Information Management & Computer Security**, v. 22, n. 3, p. 265–278, 2014.	2014	Etapa Ad hoc do autor e Cordeiro (2017)
70	WEBER, E. L. et al. Analysis of Maturity Levels in IT Process Related to Information Systems Security. In: **11th International Conference on Information Systems & Technology Management - CONTECSI 2014, Anais...**	2014	Alencar *et al.* (2018b, 2018c)
71	ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. Adoption of Information Security Measures in Public Research Institutes. In: **12th International Conference on Information Systems & Technology Management - CONTECSI, 2015**, **Anais**...	2015	Alencar *et al.* (2018b, 2018c)

72	ALNATHEER, M. A. Information Security Culture Critical Success Factors. In: **12th International Conference on Information Technology – New Generations, 2015, Anais...**	2015	Cordeiro (2017)
73	ALMEIDA NETO, H. R.; MAGALHÃES, E. M. C.; MOURA, H. P.; TEIXEIRA FILHO, J. G. A.; CAPELLI, C.; MARTINS, L. M. F. Avaliação de um Modelo de Maturidade para Governança Ágil em TIC usando Focus Group. In: **XI Simpósio Brasileiro de Sistemas de Informação - SBSI, 2015, Anais...**	2015	Etapa Ad hoc do autor
74	ALMEIDA NETO, H. R.; MAGALHÃES, E. M. C.; MOURA, H. P.; TEIXEIRA FILHO, J. G. A.; CAPELLI, C.; MARTINS, L. M. F. Avaliação de um Modelo de Maturidade para Governança Ágil em Tecnologia da Informação e Comunicação. **iSys – Revista Brasileira de Sistemas de Informação**, v. 8, n. 4, p. 44-79, 2015.	2015	Etapa Ad hoc do autor
75	BISHOP, M.; MILOSLAVSKAYA, N.; THEOCHARIDOU, M. **Information Security Education Across the Curriculum**. Springer International PU, 2016.	2015	Rea-Guaman et al. (2017)
76	BUENO, P. M. S. et al. Uma Iniciativa para Aprimorar a Gestão de Riscos de Segurança da Informação na Administração Pública Federal. In: I **Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança - WRAC / XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSEG 2015, Anais...**	2015	Alencar *et al.* (2018b, 2018c)
77	FAZENDA, R. V.; FAGUNDES, L. L. Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro. In: **XI Simpósio Brasileiro de Sisitemas de Informação - SBSI, 2015, Anais...**	2015	Cordeiro 2017 e Alencar et al. (2018b, 2018c)
78	FREITAS, R. B. et al. Information Security Framework for Brazilian Small Business. In: **12th International Conference on Information Systems & Technology Management - CONTECSI 2015**, **Anais**...	2015	Alencar *et al.* (2018b, 2018c)
79	GOKSEN, Y.; CEVIK, E.; AVUNDUK, H.. A Case Analysis on the Focus on the Maturity Models and Information Technologies. **Procedia Economics and Finance**, v. 19, p. 208–216, 2015.	2015	Rea-Guaman et al. (2017)
80	HOHAN, A.I.; OLARU, M.; PIRNEA, I. C. Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. **Procedia Economics and Finance**, v. 32, p. 352 - 359, 2015.	2015	Rea-Guaman et al. (2017)
81	LANGE, J.; VON SOLMS, R.; GERBER, M.. Better Information Security Management in Municipalities. In: **IEEE IST-Africa 2015 Conference, 2015, Anais...**	2015	Cordeiro (2017)
82	LUNA, A. J. H. O.; KRUCHTEN, P.; MOURA, H. P. Agile Governance Theory: Conceptual Development. In: **12th International Conference on Information Systems & Technology Management - CONTECSI, 2015, Anais...**	2015	Etapa Ad hoc do autor

83	MAHOPO, B.; ABDULLAH, H.; MUJINGA, M. A formal qualitative risk management approach for IT security. In: **IEEE Information Security for South Africa - ISSA, 2015, Anais...**	2015	Etapa Ad hoc do autor
84	PAYETTE, J.; ANEGBE, E.; CACERES, E.; MUEGGE, S. Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. **Technology Innovation Management Review**, v. 5, n. 6, p. 26-34, 2015.	2015	Rea-Guaman et al. (2017)
85	PURICELLI, R. The Underestimated Social Engineering Threat in IT Security Governance and Management. **ISACA Journal: Governance & Managemente of Enterprise IT (GEIT),** v. 3, p. 24-28, 2015.	2015	Etapa Ad hoc do autor
86	SILVA NETO, G. M.; ALENCAR, G. D.; QUEIROZ, A. A. L. Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In: **XI Simpósio Brasileiro de Sistemas de Informação - SBSI, 2015, Anais...**	2015	Etapa Ad hoc do autor e Alencar *et al.* (2018b, 2018c)
87	TU, Z. **Effective Information Security Management: A Critical Success Factors Analysis**. MCMaster University. Tese de Doutorado, Hamilton, Ontario, 2015.	2015	Cordeiro (2017)
88	VON SOLMS, S.H.B. A maturity model for part of the African Union Convention on Cyber Security. In: **2015 Science and Information Conference - SAI, 2015, Anais...**	2015	Etapa Ad hoc do autor e Rea-Guaman et al. (2017)
89	ARIMA, C. H. et al. Information Security Risk Management and its Application in a Federal Public Institution. In: **13th International Conference on Information Systems & Technology Management - CONTECSI 2016, Anais**...	2016	Alencar *et al.* (2018b, 2018c)
90	DE BRUIN, R.; VON SOLMS, S. H. Modelling Cyber Security Governance Maturity. In: **International Symposium on Technology and Society, 2016, Anais...**	2016	Etapa Ad hoc do autor e De Lima (2017)
91	LE, N. T.; HOANG, D. B. Can maturity models support cyber security?. In: **IEEE 35th International Performance Computing and Communications Conference (IPCCC), 2016, Anais...**	2016	Rea-Guaman et al. (2017)
92	LUNA, A. J. H. O.; KRUCHTEN, P.; RICCIO, E. L.; MOURA, H. P. Foundations for an Agile Governance Manifesto: a bridge for business agility. In: **13th International Conference on Information Systems & Technology Management - CONTECSI, 2016, Anais...**	2016	Etapa Ad hoc do autor
93	MONTENEGRO, C. et al. DSR Approach to Assessment and Reduction of Information Security Risk in TELCO. **IEEE Latin America Transactions**, v. 14, n. 5, p. 2402–2410, 2016.	2016	Alencar *et al.* (2018b, 2018c)
94	MUTHUKRISHNAN, S. M.; PALANIAPPAN, S. Security metrics maturity model for operational security. In: **2016 IEEE Symposium on Computer Applications and Industrial Electronics ISCAIE, 2016, Anais...**	2016	De Lima (2017)

95	PRADO, E. P. V.; MANCINI, M.; BARATA, A. M.; SUN, V. Governança de TI em Organizações do Setor de Saúde: um Estudo de Caso de Aplicação do COBIT. In: **XII Simpósio Brasileiro de Sistemas de Informação - SBSI, 2016, Anais...**	2016	Etapa Ad hoc do autor
96	SANTOS-OLMO, A. et al. Methodology for Dynamic Analysis and Risk Management on ISO27001. **IEEE Latin America Transactions**, v. 14, n. 6, p. 2897–2911, 2016.	2016	Alencar *et al.* (2018b, 2018c)
97	ALENCAR, G. D.; TENORIO JUNIOR, A. J. A.; MOURA, H. P. Information Security Policy: A Simplified Model Based on ISO 27002. In: **14th International Conference on Information Systems & Technology Management - CONTECSI, 2017**, **Anais**...	2017	Alencar *et al.* (2018b, 2018c)
98	ALENCAR, G. D.; TENORIO JUNIOR, A. J. A.; MOURA, H. P. Theoretical Guidelines for an Agile Model of Governance, Management and Maturity for Information Security. In: **14th International Conference on Information Systems & Technology Management - CONTECSI, 2017, Anais...**	2017	Alencar *et al.* (2018b, 2018c)
99	AMORIM, E. S.; BERNARDES, M. C. A Model for Information Security Governance in Retail Enterprises. In: **14th International Conference on Information Systems & Technology Management - CONTECSI, 2017**, **Anais**...	2017	Alencar *et al.* (2018b, 2018c)
100	MENEZES, B. P. et al. Strategic Planning Methodology for Information Security – PESEG 1.0. In: **14th International Conference on Information Systems & Technology Management - CONTECSI, 2017**, **Anais**...	2017	Alencar *et al.* (2018b, 2018c)
101	MOREIRA, M. A. R.; ALMEIDA, M. F. Information Security in Corporations: A Study of the Impacts of Medium and High Management Behavior. In: **14th International Conference on Information Systems & Technology Management - CONTECSI 2017, Anais...**	2017	Alencar *et al.* (2018b, 2018c)
102	SILVA, M. P.; BARROS, R. M. Maturity Model of Information Security for Software Developers. **IEEE Latin America Transactions**, v. 15, n. 10, p. 1994–1999, 2017.	2017	Alencar *et al.* (2018b, 2018c)

APÊNDICE K – PUBLICAÇÕES REALIZADAS

Publicações Realizadas

Conforme exposto no Capítulo 2, sobre método da pesquisa, o presente trabalho baseou-se na Design Science Research. Para tanto foi utilizada a submissão de trabalhos em eventos e periódicos acadêmicos como uma das formas de avaliar o caminho e artefatos construídos, bem como comunicar à sociedade os resultados, mesmo que parciais, da presente pesquisa. Os trabalhos referentes ao presente projeto e produzidos durante o período do doutorado são expostos abaixo:

1. ALENCAR, G. D.; MOURA, H. P.; FARIAS JUNIOR, I. H.; TEIXEIRA FILHO, J. G. A. An Adaptable Maturity Strategy for Information Security. **Journal of Convergence Information Technology (GYEONGJU)**, v. 13, n. 2, p. 1-12, 2018. - (ALENCAR et al., 2018a).

2. ALENCAR, G. D.; MENEZES, B. P.; AMORIM, E. S.; FARIAS JUNIOR, I. H.; MOURA, H. P. Governança, Gestão e Maturidade da Segurança da Informação: um mapeamento sistemático do cenário nacional. **Revista de Sistemas e Computação - RSC**, v. 8, n. 1, p. 153-173, 2018. - (ALENCAR et al., 2018c).

3. ALENCAR, G. D.; MOURA, H. P. Método Simplificado para Aplicação e Priorização da Segurança da Informação: Reflexões Teóricas e Soluções Futuras. In: **15th International Conference on Information Systems & Technology Management**, 2018, São Paulo - SP. Anais... São Paulo - SP: USP, 2018. p. 2801-2816. - (ALENCAR; MOURA, 2018).

4. ALENCAR, G. D.; AMORIM, E. S.; MENEZES, B. P.; MOURA, H. P. Scientific Production about Governance, Management and Maturity of Information Security in the Main Computing-Related Brazilian Journals and Conferences. In: **15th International Conference on Information Systems & Technology Management**, 2018, São Paulo - SP. Anais... São Paulo - SP: USP, 2018. p. 2756-2782. - (ALENCAR et al., 2018b).

5. ALENCAR, G. D.; MOURA, H. P. Proposta de Modelo de Maturidade para Segurança da Informação baseada na ISO/IEC 27001 e 27002 aderente aos Princípios da Governança Ágil. In: **XIII Simpósio Brasileiro de Sistemas de Informação (SBSI'17) / X Workshop de Teses e Dissertações em Sistemas de Informação**, 2017, Lavras - MG. Anais... Porto Alegre, RS: Sociedade Brasileira de Computação - SBC, 2017. p. 80-84. - (ALENCAR; MOURA, 2017a).

6. ALENCAR, G. D.; MOURA, H. P. Maturity Model for Information Security: A Proposal Based on ISO/IEC 27001 and 27002 According to the Principles of Agile Governance. In: **14th International Conference on Information Systems & Technology Management - Doctoral Consortium**, 2017, São Paulo - SP. Anais... São Paulo - SP: USP, 2017. p. 4817-4832. - (ALENCAR; MOURA, 2017b).

7. ALENCAR, G. D.; TENORIO JUNIOR, A. J. A.; MOURA, H. P. Information Security Policy: A Simplified Model Based on ISO 27002. In: **14th International Conference on Information Systems & Technology Management**, 2017, São Paulo - SP. Anais... São Paulo - SP: USP, 2017. p. 4135-4156. - (ALENCAR; TENORIO JUNIOR; MOURA, 2017a).

8. ALENCAR, G. D.; TENORIO JUNIOR, A. J. A.; MOURA, H. P. Theoretical Guidelines for an Agile Model of Governance, Management and Maturity for Information Security. In: **14th International Conference on Information Systems & Technology Management**, 2017, São Paulo - SP. Anais... São Paulo - SP: USP, 2017. p. 3661-3690. - (ALENCAR; TENORIO JUNIOR; MOURA, 2017b).

9. SILVA NETO, G. M.; ALENCAR, G. D.; QUEIROZ, A. A. L. Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In: **XI Simpósio Brasileiro de Sistemas de Informação (SBSI'15)**, 2015, Goiânia - GO. Anais... Porto Alegre - RS: Sociedade Brasileira de Computação - SBC, 2015. v. 1. p. 299-306. - (SILVA NETO; ALENCAR; QUEIROZ, 2015).

Aceitos para publicação:

10. ALENCAR, G. D.; MOURA, H. P. Proposta de Estratégia de Maturidade e Priorização para Segurança da Informação Baseada nas ISO/IEC 27001 E 27002 Aderente aos Princípios da Governança Ágil. In: **Princípios e Aplicações da Computação no Brasil**. Ponta Grossa - PR: Atena Editora, 2018. (Capítulo de livro aceito. Previsão de publicação do livro em Dezembro de 2018)

11. ALENCAR, G. D.; TENORIO JUNIOR, A. J. A.; MOURA, H. P. Diretrizes para um Modelo Ágil de Governança, Gestão e Maturidade da Segurança da Informação. In: **Information Systems and Technology Management**. Ponta Grossa - PR: Atena Editora, 2019. (Capítulo de livro aceito. Previsão de publicação do livro em Fevereiro de 2019)