Princípios e Aplicações da Computação no Brasil

Ernane Rosa Martins
(Organizador)

Atena
Editora
Ano 2019

Ernane Rosa Martins
(Organizador)

Princípios e Aplicações da Computação no Brasil

Atena Editora
2019

2019 *by Atena Editora*
Copyright © da Atena Editora
Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação e Edição de Arte: Geraldo Alves e Natália Sandrini
Revisão: Os autores

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

P957 Princípios e aplicações da computação no brasil [recurso eletrônico] / Organizador Ernane Rosa Martins. – Ponta Grossa (PR): Atena Editora, 2019. – (Princípios e aplicações da computação no Brasil; v. 1)

Formato: PDF
Requisito de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-85-7247-046-9
DOI 10.22533/at.ed.469191601

1. Computação. 2. Informática. 3. Redes sociais. I. Martins, Ernane Rosa. II. Título. III. Série.

CDD 004

Elaborado por Maurício Amormino Júnior – CRB6/2422

APRESENTAÇÃO

Esta obra se propõe a permitir conhecer melhor o panorama atual da computação no Brasil por meio dos textos dos 15 capítulos que a constituem. Assim, estes trazem a reflexão temas importantes da área, tais como: performance web de e-commerce, análise de redes sociais, teoria de redes complexas, automação de teste em sistemas legados, ambiente virtual, arquitetura e organização de computadores, sistema integrado de gestão, sistema de apoio à avaliação de atividades de programação, rastreamento de objetos em vídeo, segurança da informação, ensino de programação, ensino de teoria da computação, sistemas de informação, fábrica de software, interdisciplinaridade, estilos de aprendizagem em computação, plataformas multiprocessadoras baseadas em barramentos.

Deste modo, esta obra reúne debates e análises acerca de questões relevantes, tais como: Qual o tamanho médio das páginas das lojas virtuais brasileiras e como estão em comparação com a média mundial? Quais informações estratégicas, para a segurança pública, podem ser obtidas com o uso da análise das redes sociais e complexas provenientes de uma base de dados de Tatuagens em Criminosos? A proposta de um novo ambiente virtual de simulação pode apoiar a aprendizagem? A proposta de um sistema de reconhecimento automático de possíveis soluções com mapeamento destas em escores atribuídos por professores, pode auxiliar professores na avaliação de exercícios de programação? A proposta de uma metodologia para rastreamento de múltiplos objetos em vídeos usando subtração de plano de fundo via mistura de gaussianas, morfologia matemática e o filtro de Kalman é mais precisa do que quando feita usando somente a subtração de plano de fundo? Como mensurar e priorizar a segurança da informação corporativa com base nos atuais arcabouços existentes na área? Quais páginas mais se preocupam com o usuário? Algumas ferramentas que foram propostas em trabalhos anteriores e que são utilizadas no ensino de programação atendem a nova realidade do ensino inicial de programação para crianças e jovens? Um projeto de extensão de uma Fábrica de Software, pode propiciar aos alunos capacitação nas principais tecnologias de mercado e vivência no mundo do trabalho?

Nesse sentido, este material ganha importância por constituir-se numa coletânea de trabalhos, experimentos e vivências de seus autores, tendo por objetivo reunir e socializar os estudos desenvolvidos em grandes universidades brasileiras. Certamente os trabalhos apresentados nesta obra são de grande relevância para o meio acadêmico, proporcionando ao leitor textos científicos que permitem análises e discussões sobre assuntos pertinentes à computação, por meio de linguagem clara e concisa, propiciando a aproximação e o entendimento sobre temas desta área do conhecimento. A cada autor, nossos agradecimentos a submissão de seus estudos na Editora Atena. Aos leitores, desejo proveitosa reflexão sobre as temáticas abordadas.

Ernane Rosa Martins

SUMÁRIO

CAPÍTULO 9

PROPOSTA DE ESTRATÉGIA DE MATURIDADE E PRIORIZAÇÃO PARA SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E 27002 ADERENTE AOS PRINCÍPIOS DA GOVERNANÇA ÁGIL

Gliner Dias Alencar
Instituto Brasileiro de Geografia e Estatística (IBGE)
Centro de Informática (CIn), Universidade Federal de Pernambuco (UFPE)
Recife – PE

Hermano Perrelli de Moura
Centro de Informática (CIn), Universidade Federal de Pernambuco (UFPE)
Recife – PE

RESUMO: A adoção de um modelo para gestão da segurança da informação, implementação de políticas e adequação a alguma norma de segurança da informação não é algo simples, consequentemente, tem-se dificuldades em sua implantação devido, muitas vezes, a complexidade das normas. Esses desafios demonstram a necessidade de mais investigações que abordem o problema. Para isso, este trabalho propõem uma estratégia de maturidade e priorização para a segurança da informação como base nos princípios expostos nas normas ISO/IEC 27001 e 27002 e na Governança Ágil. A pesquisa proposta realizou uma revisão sistemática da literatura e questionários para levantamento da situação atual da área de Segurança da Informação nas empresas e dos principais controles necessários, alcançando 157 empresas distintas. Como resultado, foi possível classificar os controles ISO / IEC 27001 e 27002 em quatro estágios, de acordo com a importância dada pelas empresas. Também foram utilizados os níveis de maturidade do COBIT e uma matriz de análise de risco. Finalmente, a proposta foi testada com sucesso em uma empresa.

PALAVRAS-CHAVE: Segurança da Informação, Modelo de Maturidade, Governança de TIC, Governança Ágil.

ABSTRACT: The adoption of a model for information security management, along with the implementation of its policies and the required adjustments to some of its norms are not simple tasks. Therefore, the implementation of a model for information security management often implies in difficulties due to the complexity of the norms. Those challenges demonstrate a need for further investigations which address the problem. To achieve this goal, this work proposes a strategy to measure the maturity and prioritization of information security based on the principles exposed on the ISO/IEC 27001 and 27002 Standards and Agile Governance. The proposed research realized a systematic review of the literature and surveys regarding the current situation of information security in the industry and the main controls currently required, reaching 157 distinct companies. 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. Finally, the adaptable strategy was successfully tested in a company.
KEYWORDS: Information Security, Maturity Model, IT Governance, Agile Governance.

1 I INTRODUÇÃO

Na sociedade atual, globalizada, 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. Neste contexto, a informação tornou-se um dos mais valiosos ativos das empresas, visto que as informações manuseadas nas corporações podem gerar tanto lucro como grandes prejuízos, assim como o setor que a gerencia tornou-se, nas organizações, estratégico (CASTELLS, 2007).

Mesmo sabendo da importância das informações e da criticidade dos riscos atuais, diversas organizações não contam com planos adequados na área de segurança da informação e alinhamento dos mesmos ao negócio. Em alguns casos, as organizações adotam medidas de Segurança da Informação apenas para atender as forças externas, normalmente oriundas de obrigações legais e regulamentares (ALBUQUERQUE JUNIOR; SANTOS, 2014).

1.1 Motivação e Justificativa

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, 2016).

Por conta deste e de outros fatores, existem diversos padrões, frameworks, normas e regulamentos para a implementação de modelos de segurança. Eles fornecem diretrizes ou 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 os apliquem adequadamente e não gerenciem as características de segurança da informação de forma adequada.

A complexidade e formalismo dos modelos tradicionais mais utilizados atualmente abre 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, melhoria em seus processos e maior alinhamento entre a área de TIC e as estratégias organizacionais (PRADO *et al.*, 2016; SILVA NETO; ALENCAR; QUEIROZ, 2015).

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 essas questões no cenário dinâmico atual.

É importante destacar, também, a escassez de estudos que investiguem a presente temática, comparando com outras áreas da computação. Por exemplo, tem-se constantemente visto nos tópicos de interesses dos últimos anos dos principais eventos da área (pode-se citar: SBSI – Simpósio Brasileiro de Sistemas de Informação; CONTECSI – Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação; SBSEG – Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais; e o 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, ainda são poucos os trabalhos que abordem tais áreas nos anais, como abordam Alencar *et al.* (2018a).

Neste contexto, acredita-se ser relevante para a área de segurança da informação realizar estudos que busquem produzir modelos para aferir a maturidade da área de segurança da informação. Bem como, dar subsídios para um melhor alinhamento da área à Governança Ágil de TIC e ao negócio buscando meios menos complexos ou burocráticos que os atuais. Com este pensamento, espera-se que uma visão sistêmica da área de segurança da informação com processos menos burocráticos e complexos modifique, de forma positiva, o ambiente corporativo de maneira geral.

1.2 Organização do Capítulo

O presente capítulo está organizado, a partir deste ponto, da seguinte forma: a Seção 2 apresenta a problemática estudada, sendo complementada pela Seção 3 que insere a proposta de solução. Na Seção 4 é detalhado o método da pesquisa. A seção 5 traz os pontos teóricos que embasam o projeto e alguns trabalhos correlatos. A seção 6 expõe as principais atividades realizadas e os resultados alcançados. Fechando o corpo do trabalho, a seção 7 insere as considerações finais. Por fim, o trabalho é complementado com as referências.

2 I APRESENTAÇÃO DO PROBLEMA

A ISO (International Organization for Standardization) criou a Família de normas 27000 que versam sobre a segurança da informação. Sendo esse um dos principais mecanismos na área de segurança da informação no que tange, especialmente, aos aspectos táticos e operacionais. Apesar destes modelos serem muito bem estruturados, o formalismo, por algumas vezes excessivo, tem tornado a adoção e melhoria contínua de seus processos uma tarefa complexa (PRADO *et al.*, 2016; SILVA NETO; ALENCAR;

QUEIROZ, 2015).

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

Formas de mensuração da governança de TIC de uma corporação têm sido exploradas (ALMEIDA NETO *et al.*, 2015a) como meios de se analisar a situação da instituição, assim como possibilitando a comparação dos níveis de governança entre corporações distintas. 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 de software é outro exemplo, pois utiliza com constância níveis de qualidade e maturidade para diferenciar empresas e produtos.

Diante do contexto citado, esta pesquisa pretende explorar a área respondendo o questionamento: "Como mensurar e priorizar a segurança da informação corporativa com base nos atuais arcabouços existentes na área?"

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

3 I 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 27000 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. Esta estratégia, através, principalmente, da ISO/IEC 27001 (ABNT, 2013a) e 27002 (ABNT, 2013b) que abordam a implantação e gestão da segurança da informação, bem como a ISO/IEC 27005 (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 maturidade 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;

Além dos pontos expostos, percebe-se, como já apresentado na problemática em questão, a burocracia existente nos processos atuais. 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 esta 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 (2015b) e Luna *et al.* (2016).

Desta forma, a estratégia proposta também se debruçará sobre o ramo da praticidade e agilidade de forma 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.

Sintetizando a proposta de solução, 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.

4 I METÓDO DA PESQUISA

Para atender aos objetivos propostos, a pesquisa em questão é categorizada como Exploratória e Descritiva, utilizando os procedimentos técnicos de Pesquisa Bibliográfica, Revisão e Mapeamento Sistemático da Literatura, *survey* e Grupo Focal. Sendo Quanti-qualitativa e concentrada na área de Ciência da Computação: Sistemas de Informação e Segurança da Informação.

De acordo com WOHLIN e AURUM (2015), a presente pesquisa se classifica como exposto na Figura 1.

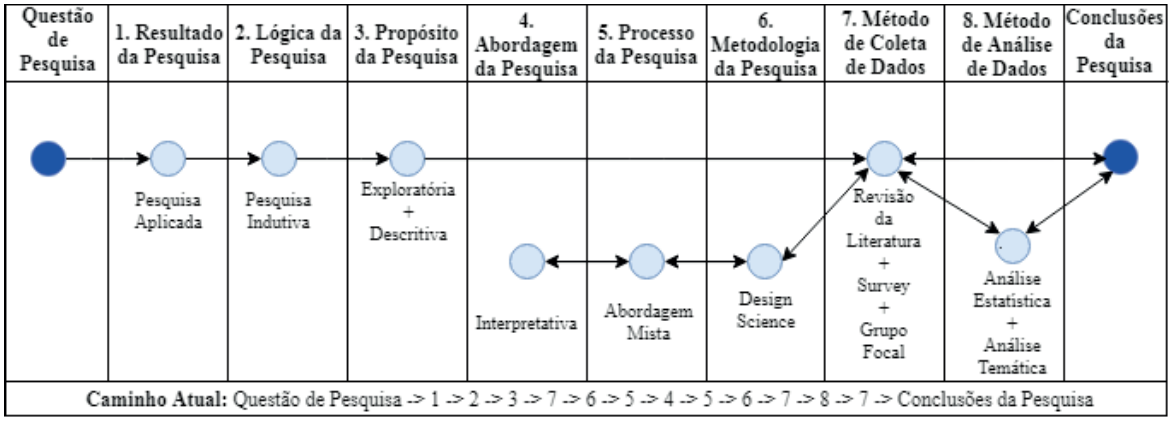

Figura 1. Estrutura de Tomada de Decisão Metodológica

A execução da pesquisa será realizada em atividades divididas em duas fases distintas, conforme Figura 2. A primeira etapa consiste em uma fase exploratória e tem por objetivo a construção de uma base teórica consistente para suportar a etapa seguinte. A etapa 2, apresenta uma característica mais descritiva e visa a real construção do modelo proposto.

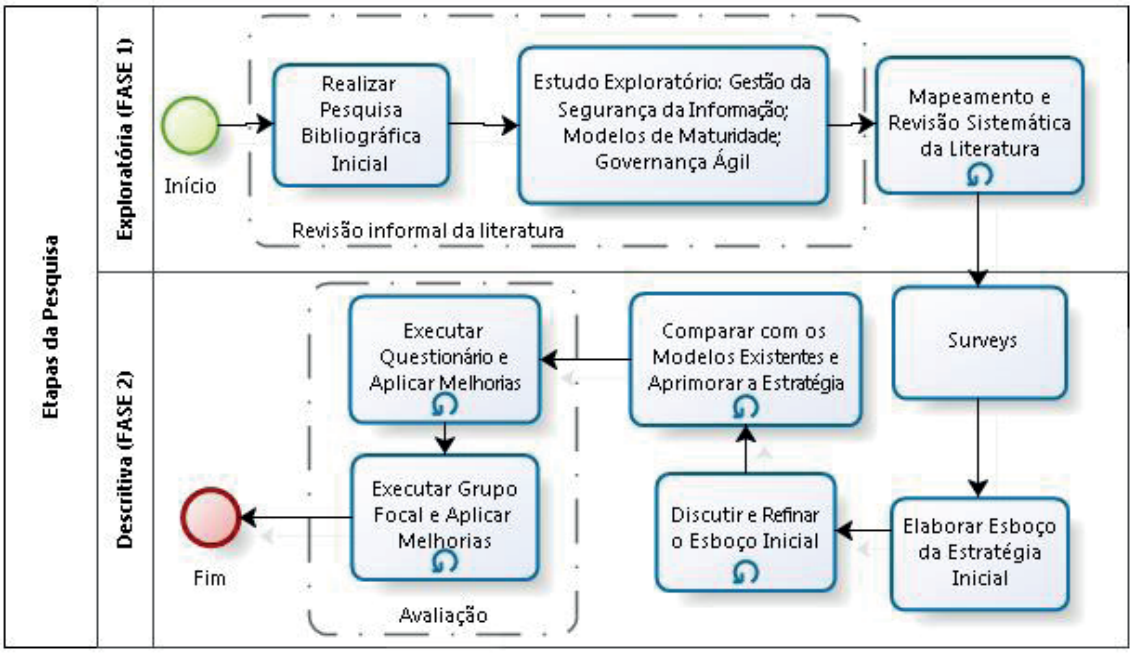

Figura 2. Etapas da Pesquisa

A Revisão Sistemática da Literatura foi baseada no método de Kitchenham (2004) em bases nacionais e internacionais.

A fase de *surveys* consiste no levantamento de características das empresas participantes e da sua visão quanto a importância de cada controle das ISO 27001 e 27002, para isso foram utilizados dois *surveys*.

O primeiro *survey* é uma aplicação do documento já utilizado outras vezes, entre elas Alencar, Queiroz e De Queiroz (2013a; 2013b) e que baseou o questionário utilizado por Silva Neto, Alencar e Queiroz (2015). Sendo composto por 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; e Segurança da informação corporativa. Ao final foram adicionadas mais cinco questões inerentes a amplitude da pesquisa atual.

O segundo consta do nome da empresa (para correlacionar com o primeiro) e os 114 controles da versão de 2013 da 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. Nas questões o respondente marcará a importância de cada controle para o seu ambiente. Mesmo método utilizado por Silva Neto, Alencar e Queiroz (2015), porém os autores colocavam a versão anterior da ISO/IEC 27002 (de 2005) com 133 controles.

A amostra foi composta por empresas de todas as regiões do Brasil, bem como com abrangência de atuação local, regional, nacional e multinacional, sendo contabilizada apenas uma resposta por empresa. Os respondentes deverão ser da área de TIC e, preferencialmente, o responsável pela área de segurança da informação.

Após a análise, os resultados dos controles foram ordenados de acordo com sua média das notas de importância. Posteriormente verificado se existe algum pré-requisito entre os controles e, neste caso, os pré-requisitos foram inseridos antes. Essa fase gerou o Esboço do Modelo Inicial que, posteriormente, foi debatido e refinado. Após superada esta etapa, foi comparado com os modelos de maturidade existentes e ajustado. Estas etapas poderão ser repetidas.

Em diversas etapas, a versão atual da estratégia ou algum de seus componentes, foi enviado aos especialistas na área, procurando obter, ao menos, 5 respostas, e também enviado às empresas respondentes junto com o *survey* 3. Este terceiro *survey* questionou sobre a sua adequação, sendo a primeira etapa de validação. Após receber as respostas dos especialistas e empresas, é analisada e aplicada as melhorias propostas. Esta etapa poderá ser repetida.

Tendo o modelo pré-avaliado e melhorado pela indicação das empresas e especialistas, será realizado grupo focal para a validação final do mesmo (ainda em fase preparatória, não realizada). Esta etapa, semelhante a validação do modelo de maturidade de Almeida Neto *et al.* (2015b), poderá ser repetida.

Desta forma, acredita-se que objetivo principal seja atingido pela criação, ao final do trabalho, da estratégia para mensurar a maturidade e priorizar a segurança da informação atendendo aos princípios da governança ágil.

Esperar-se, também, que os demais objetivos específicos propostos, não atendidos com o modelo de maturidade formulado, sejam solucionados com as etapas intermediárias para a construção do trabalho e da estratégia: a análise dos dados coletados e da revisão da literatura. Como consequência dos passos realizados e da solução dos objetivos propostos, acredita-se que o problema de pesquisa seja resolvido a contento.

5 I BASES TEÓRICAS E TRABALHOS CORRELATOS

A presente pesquisa baseia-se, principalmente, nos conhecimentos das áreas de Governança de Segurança da Informação (ABNT, 2013c; MANOEL, 2014), Governança Ágil (LUNA *et al.*, 2014; LUNA *et al.*, 2016), Modelos de Maturidade (KAROKOLA; KOWALSKI; YNGSTRÖM, 2011; RIGON *et al.,* 2014) e normas ISO/IEC 27001 (ABNT, 2013a), 27002 (ABNT, 2013b) e 27005 (ABNT, 2011).

Na literatura percebe-se um conjunto de trabalhos que tratam de melhorias e maturidade para segurança da informação que podem ser inseridos como correlatos, entre os trabalhos pode-se citar: Rigon *et al.* (2014), Karokola; Kowalski e Yngström (2011) e Mahopo, Abdullah e Mujinga (2015). Porém eles ainda sofrem com os já citados problemas de burocracia e formalismo.

O modelo de maturidade de Almeida Neto et al. (ALMEIDA NETO *et al.*, 2015a, 2015b) tenta solucionar os problemas da burocracia e formalismo, baseando-se nos princípios da Governança Ágil, porém não tem foco em segurança da informação. Já Silva Neto, Alencar e Queiroz (2015), propõe uma simplificação da segurança, mas apresenta apenas uma visão inicial de uma política de segurança da informação simplificada, não formulando um modelo de maturidade. Assim, acredita-se que os trabalhos encontrados não atendem, por completo, todos os objetivos específicos propostos nesta presente pesquisa e problemas expostos.

6 I ATIVIDADES JÁ REALIZADAS E RESULTADOS ALNCAÇADOS

Dentro das atividades propostas no método de pesquisa, expostas na Figura 2, apenas a última avaliação, através do Grupo Focal, não foi realizada. Os principais resultados das etapas já desenvolvidas são exibidos a seguir.

A estratégia consiste, inicialmente, em levantar a visão das empresas quanto a criticidade para cada um dos 114 controles da ISO/IEC 27001 (Anexo I) e 27002, pontuando em uma escala de 1 (pouco importante) até 5 (muito importante). Após a resposta, em uma segunda fase, os controles serão classificados em quartis. Para isto 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 Quadro 1.

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

Quadro 1. Divisão dos controles por quartis

Porém a divisão dos quartis pode não ser tão exata quanto a proposta, visto que após a primeira divisão dos quartis deverá ser analisado se existe alguma dependência ou pré-requisito entre algum controle. Existindo, o controle pré-requisito deverá estar no mesmo quartil ou em um quartil anterior. Caso ele esteja em um quartil posterior, o controle pré-requisito será colocado no mesmo quartil do seu dependente. Por exemplo, uma situação que, inicialmente, o controle da ISO/IEC 27001 "A.5.1.1 - Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para os funcionários e partes externas relevantes" está no 3º quartil, enquanto o controle ISO/IEC 27001 "A.5.1.2 - As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia" está no 2º quartil. Percebe-se que o controle A.5.1.1 (definição da política de segurança da informação) é pré-requisito para o controle A.5.1.2 (análise da política de segurança da informação), neste caso o controle A.5.1.1 será inserido no 2º quartil, mesmo do controle A.5.1.2. Esta análise de pré-requisitos é a terceira etapa.

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 da posição 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, exemplificados no Quadro 1.

A quarta etapa consiste em definir os níveis de maturidade. Esta proposta utiliza os níveis de maturidade e definições do COBIT (ISACA, 2007), são eles: Nível 0 (Inexistente), Nível 1 (Inicial), Nível 2 (Repetível), Nível 3 (Definido), Nível 4 (Gerenciado), Nível 5 (Otimizado).

Como quinto passo tem-se a definição do nível mínimo de maturidade para cada controle. Uma forma é elencar um padrão, por exemplo, todos os controles deverão alcançar, no mínimo, o nível 3 (definido). Uma outra opção, mais recomendada, é realizar uma análise de risco na empresa, como sugere a ISO/IEC 27005, e categorizar o nível mínimo de cada controle de acordo com sua probabilidade e impacto.

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 3.

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 prioritariamente pela empresa. Desta forma os controles que suas ausências geram riscos com maior probabilidade e maior impacto deverão ser tratados de forma diferenciada.

Probabilidade	Impacto		
Alta (3)	4 - Gerenciado	5 - Otimizado	6 - Otimizado
Média (2)	3 – Definido	4 - Gerenciado	5 - Otimizado
Baixa (1)	2 - Repetível	3 – Definido	4 - Gerenciado
	Baixo (1)	Médio (2)	Alto (3)

Figura 3. Nível de maturidade mínimo de acordo com o impacto e probabilidade

Os controles não aplicáveis deverão ser devidamente justificados no relatório a ser apresentado no final da avaliação. Tendo como nível mínimo o 0 (inexistente) e não sendo contabilizados na estratégia.

A escolha do COBIT, bem como das ISO/IEC 27001, 27002 e 27005 se deu devido a sua consolidação na área.

Após as definições iniciais, tem-se a aplicação da estratégia como o sexto passo. As 6 etapas supracitadas são ilustradas na Figura 4.

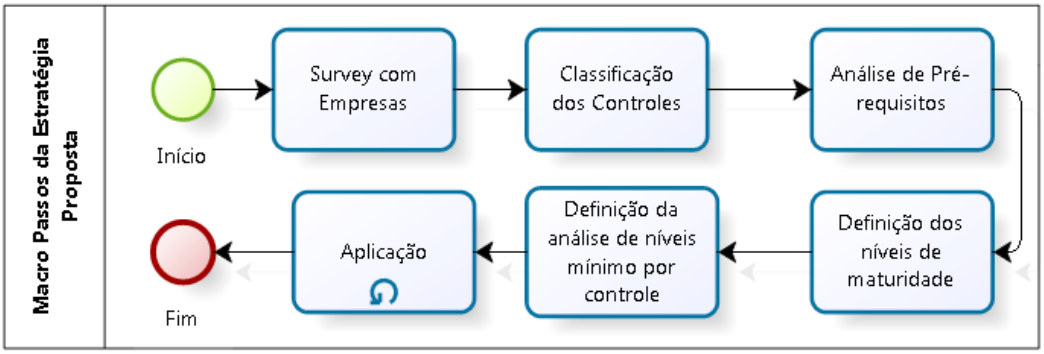

Figura 4. Macro passos da estratégia

A fase de aplicação da estratégia consiste em analisar e aplicar cada controle ordenados nos estágios até o estágio pretendido, conforme Figura 5.

Ressalta-se que o alcance de níveis e estágios de maturidade mais avançados geram custos e demandam tempo, podendo não ser do interesse de todas as empresas alcançar o Estágio Completo e o nível de maturidade 5 (Otimizado) em todos seus controles.

Também importante mencionar a etapa final da aplicação. Que consiste na geração do Relatório da Avaliação e da Comunicação aos Stakeholders das análises feitas, níveis a ser alcançados, pontos fortes e fracos da empresa.

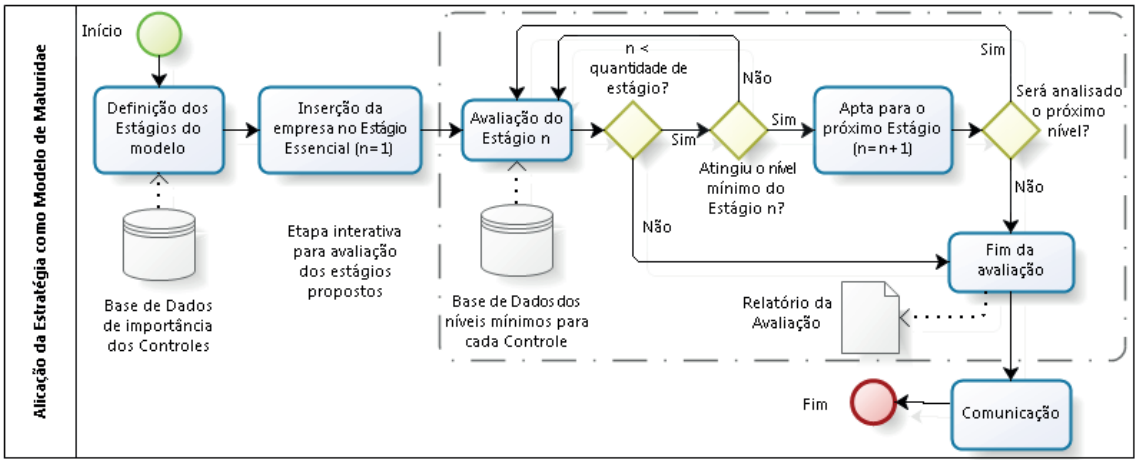

Figura 5. Fase de aplicação da Estratégia

6.1 Modelo de Maturidade

Os modelos de maturidade em segurança da informação, como os citados na Seção de trabalhos correlatos, utilizam, por exemplo, os controles da ISO/IEC 27001 ou 27002 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 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 6.

Figura 6. Estágios e níveis do modelo de maturidade

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 para todos os controles, sendo este o parâmetro da Base de Dados dos níveis mínimo para cada Controle (Figura5). Ou seja, se a empresa é categorizada como Avançada Nível 2, significa que a média dos controles do grupo Avançado obteve a 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.

Para verificar quais controles da ISO/IEC 27001 e 27002 são os mais importantes, foi utilizado um *survey* com empresas brasileiras. Obtendo resposta de 157 empresas distintas, sendo 23 de atuação multinacional, conforme descrição no Gráfico 1.

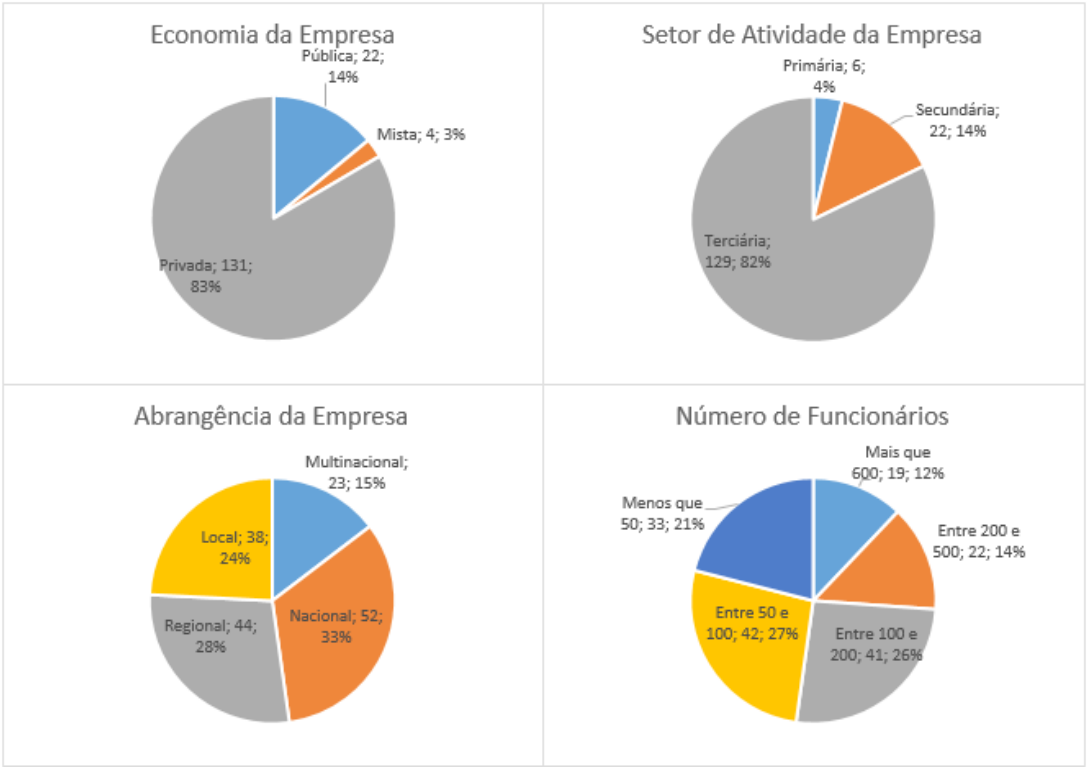

Gráfico 1. Classificação da Amostra

Todos os entrevistados eram funcionários ou sócios das empresas, sendo 69,43% 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. Dentre as empresas pesquisadas, 23,57% têm a TIC como área fim. Vale ressaltar que se alcançou empresas de todas as regiões do Brasil.

A quantidade de funcionários das empresas respondentes variou de 15 a 12 mil, enquanto a quantidade de computadores variou de 17 computadores a 7,7 mil máquinas.

Com base na média das respostas das empresas alcançadas, foi realizada a divisão dos controles entre os estágios, alcançado a configuração exposta no Quadro 2 que representa a Base de dados de importância dos controles (Figura 5). A numeração dos controles está de acordo com a exibida no Anexo A da ISO/IEC 27001.

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.

Quadro 2. Divisão dos controles por quartis

Periodicamente os controles de cada estágio são 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.

Maiores detalhes sobre a estratégia apresentada, bem como seu modo de aplicação independente e um exemplo de aplicação real são exibidos em Alencar *et al.* (2018b).

O alinhamento da estratégia com o pensamento da Governança Ágil, em especial seus meta-valores apontados por Luna *et al.* (2016) como, por exemplo, o meta-valor "Comportamento e prática do que processos e procedimentos", pode ser percebido ao se colocar a decisão das empresas sobre a criticidade de cada controle acima da necessidade de atendimento total dos normativos, bem como as diferentes formas de aplicação da estratégia (ALENCAR *et al.,* 2018b).

6.2 Evolução da Pesquisa e Publicações

Conforme exibido na Figura 1, a pesquisa utilizou-se do *Design Science Research* (DSR) como método. O DSR foi selecionado por ser propício para construção e avaliação de artefatos que visam atender aos requisitos de um problema real. Sendo o artefato de saída uma construção, modelo, método, instanciação ou estratégia nova.

Uma das características do método é a importância dada à divulgação e avaliação dos resultados encontrados. Visando o atendimento deste item, bem como analisar a aceitação deste trabalho por parte da comunidade científica e resultando como mais uma fase de avaliação, as etapas e evoluções deste projeto foram publicadas em congressos e periódicos nacionais e internacionais, totalizando nove publicações aceitas: Silva Neto, Alencar e Queiroz (2015), Alencar e Moura (2017a, 2017b), Alencar, Tenorio Junior e Moura (2017a, 2017b), Alencar e Moura (2018) e Alencar *et*

al. (2018a, 2018b, 2018c).

7 I CONSIDERAÇÕES FINAIS

O trabalho apresentou uma estratégia para a segurança da informação que pode ser aplicada como modelo de maturidade, bem como é possível sua aplicação independente focada em um alinhamento do negócio aos controles de segurança da informação, sendo testado com sucesso (ALENCAR *et al.*, 2018b).

A estratégia permite uma análise do nível de maturidade de forma mais aprimorada, fazendo com que se tenha uma maior visibilidade, através dos estágios, se os controles principais foram mensurados, não apenas analisando um nível de maturidade final da empresa.

A estratégia proposta consiste, basicamente, em um conjunto de módulos: Os 4 estágios propostos (Essencial, Intermediário, Avançado e Completo), os níveis de maturidade (baseado no COBIT), os aspectos e controles a analisar (utilizado os controles da ISO/IEC 27001 e 27002) e a definição do nível mínimo de cada controle, pré-definido ou baseado no risco inerente a cada um deles (ISO/IEC 27005). Acredita-se que essa estrutura seja um diferencial da estratégia proposta, visto que utiliza arcabouços consolidados, mas também possibilita, na aplicação independente, a troca de algum módulo por outro a 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, como abordam Alencar *et al.* (2018b).

O fato da possibilidade de se avaliar como uma aplicação independente, utilizar módulos e permitir ajustes ao negócio apontam a convergência aos pensamentos da governança ágil.

Por fim, espera-se que a estratégia proposta promova apoio significativo à adoção e melhorias contínuas à Segurança da Informação mensurando a maturidade da empresa; apontando as áreas com maior desenvolvimento em segurança da informação e as áreas que precisam de maior investimento; ter, de forma palpável, o impacto na segurança da informação de alterações (sejam elas pessoais, procedimentais ou tecnológicas) ocorridas na corporação; possibilidade de comparação do “nível de maturidade de segurança” entre setores ou empresas; diminuição da burocracia e formalismo na área gerando maior agilidade na gestão da segurança da informação corporativa.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro, p. 30. 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro, p. 99. 2013b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro, p. 87. 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27014: Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação**. Rio de Janeiro, p. 12. 2013c.

ALBUQUERQUE JUNIOR, A. E.; DOS 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; 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**, v. 8, n. 1, p. 153-173, 2018a.

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 (JCIT)**, v. 13, n. 2, p. 1-12, 2018b.

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 (CONTECSI)**, São Paulo – SP, 2018c. *Anais*... 2018c, USP. p. 2756-2782.

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, 2018. *Anais*... 2018, USP. p. 2801-2816.

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)**, São Paulo – SP, 2017a. *Anais*... 2017a, USP. p. 3661-3690.

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)**, São Paulo – SP, 2017b. *Anais*... 2017b, USP. p. 4135-4156.

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)**, São Paulo – SP, 2017a. *Anais*... 2017a, USP. p. 4817-4832.

ALENCAR, G. D.; MOURA, H. P. Proposal of Information Security Maturity Model based on ISO/IEC 27001 and 27002 according to the Principles of Agile Governance. In**: XIII Simpósio Brasileiro de Sistemas de Informação (SBSI) / X Workshop de Teses e Dissertações em Sistemas de Informação (WTDSI)**, Lavras – MG, 2017b. *Anais...* 2017b, SBC. p. 80-84.

ALENCAR, G. D.; QUEIROZ, A. A. L,; DE 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, 2013.

ALENCAR, G. D.; QUEIROZ, A. A. L.; DE QUEIROZ, R. J. G. B. Insiders: Um Fator Ativo na Segurança da Informação. In: **IX Simpósio Brasileiro de Sistemas de Informação (SBSI),** João Pessoa – PB, 2013b. *Anais...* 2013b, SBC. p. 254-259.

ALMEIDA NETO, H. R.; DE MAGALHÃES, E. M. C.; DE MOURA, H. P.; DE ALMEIDA TEIXEIRA FILHO, J. G.; 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, 2015a.

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),** Goiânia – GO, 2015b. *Anais...* 2015b, SBC. p. 15-22.

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. Disponível em: <http://agilemanifesto.org>. Acesso em: 20 mar.2016.

CASTELLS, M. **Era da Informação: A Sociedade em Rede.** Volume 1. 10ª Edição. São Paulo: Editora Paz e Terra, 2007. 698 p.

ISACA. **COBIT 4.1: framework, control objectives, management guidelines and maturity models.** IT Governance Institute, 2007.

KAROKOLA, G.; KOWALSKI, S.; YNGSTRÖM, L. Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. In: **Fifth International Symposium on Human Aspects of Information Security and Assurance (HAISA)**, Londres – Inglaterra, 2011. *Proceedings...* 2011, p. 58-73.

KITCHENHAM, B. **Procedures for performing systematic reviews**. Technical Report. Keele University, 2004, 33 p.

KRUCHTEN, P. **The rational unified process: an introduction**. 3ª edição. Editora Addison-Wesley, 2004. 336 p.

LUNA, A. J. D. O.; KRUCHTEN, P.; PEDROSA, M. L. D. E.; NETO, H. R.; DE 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.

LUNA, A. J. H. O.; KRUCHTEN, P.; RICCIO, E. L.; DE MOURA, H. P. Foundations for an Agile Governance Manifesto: A Bridge for Business Agility. In: **13th International Conference on Information Systems and Technology Management (CONTECSI),** São Paulo – SP, 2016. *Proceedings...* 2016, USP. p. 4391-4404.

MAHOPO, B.; ABDULLAH, H.; MUJINGA, M. A formal qualitative risk management approach for IT security. In: **Information Security for South Africa (ISSA),** Joanesburgo - África do Sul, 2015. *Proceedings...* 2015, IEEE. p. 1-8.

MANOEL, S. S. **Governança de Segurança da Informação: Como criar oportunidades para o seu negócio**. Rio de Janeiro: Editora Brasport, 2014. 168 p.

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),** Florianópolis – SC, 2016. *Anais...*, SBC. p. 1-8.

PWC. PricewaterhouseCoopers. Pesquisa global de segurança da informação 2016. Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/ consultoria-negocios/2016/pwc-pesquisa-global-seguranca-informacao-16.html>. Acesso em: 04 jan. 2017

RIGON, E. A.; WESTPHALL, C. M.; SANTOS, D. R.; WESTPHALL, C. B. A cyclical evaluation model of information security maturity. **Information Management & Computer Security**, v. 22, n. 3, p. 265-278, 2014.

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),** Goiânia – GO, 2015. *Anais...* 2015, SBC. p. 299-306.

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, 2015.

Agência Brasileira do ISBN
ISBN 978-85-7247-046-9