Governança, Gestão e Maturidade da Segurança da Informação: um mapeamento sistemático do cenário nacional

Governance, Management, and Maturity of Information Security: a systematic mapping of national scenario

Gliner Dias Alencar[1], Breno Pinho Menezes[2], Everton Silva de Amorim[3], Ivaldir Honório de Farias Júnior[1], Hermano Perrelli de Moura[1]

[1]Centro de Informática – Universidade Federal de Pernambuco
Recife, PE – Brasil

[2] Universidade Tiradentes
Aracaju, SE – Brasil

[3]Universidade de São Paulo
São Paulo, SP – Brasil

{gda2,ihfj,hermano}@cin.ufpe.br, brenopinhomenezes@gmail.com, everton.amorim@outlook.com

Abstract. *The adoption of information security, along with the implementation of its policies and the required adjustments to some of its norms are not simple tasks. These difficulties demonstrate the need for a research focused on new ways to overcome such deficiency. This work shows the results of a systematic mapping of governance, management, and maturity of information security of the last 10 years in the Brazilian journals and conferences. Method: Systematic Mapping Study and snowball. Results: More than 7600 articles were analyzed and 35 works were selected in the area. There has been an increase in the number of works in the last 5 years and the massive use of ISO / IEC 27001, 27002 and 27005 standards. Conclusion: This research provides a basis for new research related to governance, management, and maturity of information security.*

Resumo. *A adoção da segurança da informação, implementação de políticas e adequação a alguma norma não é algo simples. Estas dificuldades demonstram a necessidade de pesquisar formas para tentar suprir esta carência. Este trabalho apresenta os resultados de um mapeamento sistemático da literatura sobre governança, gestão e maturidade de segurança da informação dos últimos 10 anos em periódicos e eventos nacionais. Método: Mapeamento sistemático e snowball. Resultados: Analisou-se mais de 7600 artigos e foram selecionados 35 trabalhos na área. Verificou-se o aumento do número de trabalhos nos últimos 5 anos e a utilização maciça das normas ISO/IEC 27001, 27002 e 27005. Conclusão: Esta pesquisa provê uma base para novas pesquisas relacionadas à governança, gestão e maturidade da segurança da informação.*

1. Introdução

No decorrer dos anos o mercado vem modificando sua concepção de valor, com a informação tomando posição de destaque no meio corporativo. Sendo considerada essencial para as tomadas de decisões e para a continuidade dos negócios, atuando de forma estratégica e possibilitando análises internas e do mercado. A evolução das Tecnologias da Informação e Comunicação (TICs), pode ser vista como uma mola propulsora nessa mudança. Porém, essa mesma facilidade, e atual dependência, pode se tornar uma fragilidade gerando erros e danos em grande proporção.

Ciente da necessidade crescente de segurança da informação, as organizações estão buscando formas inovadoras de proteção na tentativa de gerenciar ameaças e criar vantagens, entre elas: programas de sensibilização sobre privacidade; políticas e procedimentos de privacidade; análises críticas da situação e da maturidade; e respostas a incidentes de privacidade [PWC 2017]. Sendo importante a implementação de ações e pesquisas de segurança da informação nas diversas etapas de criação, armazenamento, manipulação e utilização dos dados e da informação, bem como na governança, gestão e maturidade da segurança da informação.

Grande parte das pesquisas na área de segurança da informação tem focado, prioritariamente, no desenvolvimento, melhoramento e aplicação de aspectos técnicos nos sistemas, redes, segurança física e criptografia, por exemplo, [Junior et al. 2017; Rodrigues 2017]. Porém, a pura aplicação de tecnologia não é suficiente para o tratamento da segurança da informação. Para os novos desafios, torna-se igualmente necessário abordar outras áreas, vendo a segurança da informação de forma mais ampla e alinhando-a ao negócio. Dentro desta visão holística da segurança da informação, encaixa-se a área relacionada a processos, procedimentos e controles, governança, gestão, auditoria, conformidade, política e maturidade em segurança da informação.

No que tange aos resultados das pesquisas, observa-se preferência pela publicação em eventos e periódicos internacionais em detrimento aos eventos e periódicos nacionais. Tal constatação mobiliza alguns questionamentos: por que há preferência por periódicos e eventos internacionais? Não se tem eventos e periódicos com bom nível Qualis no Brasil? E os trabalhos aqui publicados não são de boa qualidade para servir de embasamentos teóricos?

Para melhor entender o atual contexto, o presente trabalho teve como principal pergunta de pesquisa: Qual é o atual estado da arte das publicações nos principais eventos e periódicos nacionais na área de Governança / Gestão / Maturidade em Segurança da Informação no meio Corporativo nos últimos anos?

Diante do explicitado, o presente estudo teve por objetivo analisar as publicações científicas nos principais periódicos e eventos nacionais, entre 2008 e 2017 (10 anos), que tratem a área de Governança, Gestão e Maturidade da Segurança da Informação. Além disso, buscou-se compreender quais são modelos, padrões ou frameworks utilizados, como também quais são os principais desafios para sua implantação. Para atender o objetivo proposto e responder à pergunta de pesquisa foi realizado um mapeamento sistemático da literatura (MSL).

Este artigo está organizado em mais cinco seções e as referências ao final. A próxima seção apresenta um referencial teórico sobre as áreas de Governança, Gestão e Maturidade da Segurança da Informação. Na terceira seção é apresentado o método de pesquisa. Os resultados e suas análises são exibidos nas seções quatro e cinco. A sexta seção finaliza o conteúdo produzido com as considerações finais e trabalhos futuros.

2. Fundamentação Teórica

2.1. Governança de Segurança da Informação

A Governança de TIC pode ser vista como uma visão de governança que garante que a informação e a tecnologia relacionada apoiem e possibilitem a estratégia da organização e a consecução dos objetivos corporativos. Também inclui a governança funcional de TI, ou seja, garantindo que as capacidades de TI sejam fornecidas com eficiência e eficácia [Isaca 2012]. O mesmo pensamento pode ser focado e aplicado à Governança de Segurança da Informação (GSI). Portanto, a GSI pode ser entendida com um conjunto de ações e práticas para o alinhamento das atividades da área de segurança da informação com a estratégia da corporação [Alencar et al. 2017b]. A GSI é uma parte da Governança de TIC, podendo haver sobreposição entre as duas [Manoel 2014].

A GSI deve ter objetivo de: alinhar os objetivos de negócio com a estratégia da segurança da informação; garantir que os riscos da informação sejam elucidados e encaminhados aos responsáveis; assim como, aditar valor para o negócio, para a alta direção e para as partes interessadas. Tendo como princípios: estabelecer a segurança da informação em toda a organização; adotar uma abordagem baseada em riscos, recomendando-se a utilização em conjunto da ISO/IEC 27005; 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; e analisar criticamente o desempenho e resultado das ações de segurança da informação em relação aos resultados de negócios [ABNT 2013a].

Aplicando corretamente a GSI, além de atingir os objetivos supracitados, tende-se a encaminhar a organização ao atendimento e conformidade com requisitos externos, por exemplo, legais [Manoel 2014].

Como caminho para se buscar a GSI tem-se o normativo da ISO/IEC 27014:2013, nomeado como Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação e tratando esclusivamente desta área.

Governança e Gestão da Segurança da Informação são diferentes, porém se complementam. A gestão trabalhando mais voltada para os aspectos táticos e operacionais, enquanto a governança para as camadas táticas e estratégicas [Amorim and Bernardes 2017].

2.2. Gestão da Segurança da Informação

A gestão implica o uso ponderado dos meios (recursos, pessoas, processos, práticas, etc.) para atingir um determinado objetivo. É o meio ou instrumento pelo qual o órgão

de governança alcança um resultado ou objetivo. A gestão é responsável pela execução da orientação definida pelo órgão de governança [Isaca 2012].

A gestão da segurança da informação deve ser um conjunto de ações e documentos que, incorporadas à cultura da organização, funcionam como facilitadora do gerenciamento de recursos, sendo fundamental a elaboração, publicação e implantação da Política de Segurança da Informação (PSI), devendo esta ser amplamente divulgada e apoiada pelo alto escalão [Alencar et al. 2017a].

Um sistema de gestão da segurança da informação deve preservar a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados [ABNT 2013b].

A gestão da segurança da informação deve atuar na ligação entre os níveis tático e operacional da organização, traduzindo o que foi definido no nível estratégico, de Governança de TIC, em ações práticas, definindo assim o "como fazer"[Amorim and Bernardes 2017]. A gestão da segurança da informação deve ser realizada em etapas, visando proteger as informações incluindo, também, os limites e conscientização dos usuários [Menezes et al. 2017].

Como forma de auxílio para se buscar a gestão da segurança da informação tem-se os normativos da ISO/IEC 27001:2013 (Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos) e o 27002:2013 (Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação) que, até 2007, era tratada como 17799. Tais normas direcionam a criação de uma PSI e de um sistema de gestão da segurança da informação (SGSI). Esses normativos apontam a necessidade de se fazer, em conjunto, o gerenciamento de riscos de segurança da informação. Citando a norma ISO/IEC 27005:2011 (Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação) como caminho. Por fim, tratando de requisitos para auditorias externas em um SGSI tem-se a ISO/IEC 27006:2015 (Tecnologia da informação - Técnicas de segurança - Requisitos para organismos que fornecem auditoria e certificação de SGSI).

Diante do exposto, têm-se as ações de governança para atingir os objetivos estratégicos, sendo operacionalizada pela gestão. Porém, para completar o ciclo, torna-se necessário saber em que estágio se está, quais os estágios existentes e como chegar ao nível mais avançado. Para isso surge os modelos de maturidade, explicados a seguir.

2.3. Maturidade em Segurança da Informação

Um modelo de maturidade é um conjunto de características, atributos, indicadores ou padrões que representam a capacidade e a progressão em uma determinada disciplina. Apontando, normalmente, as melhores práticas para a área [Rea-Guaman et al. 2017].

Para um correto alinhamento da área de TIC ao negócio, torna-se essencial métricas e modelos para se definir o estágio atual, bem como os próximos passos para se chegar a um nível mais avançado [Alencar et al. 2017b] [Silva and Barros 2017]. Sendo o modelo de maturidade propício para isto.

O uso de um modelo de maturidade permite uma avaliação contínua e a identificação de lacunas que representam riscos. Auxiliando, também, na explicitação dos riscos e fragilidades à equipe e envolvidos. Baseado nesta análise, planos podem ser avaliados e desenvolvidos para a melhoria dos processos e de controles considerados deficientes, buscando-se o nível desejado [Rigon et al. 2014].

Com esta apresentação, percebe-se que um modelo de maturidade em segurança da informação é essencial para se obter uma governança e gestão da área eficaz e eficiente, trabalhando em conjunto.

2.4. Trabalhos Correlatos

Dentro dos trabalhos mais próximos pode-se citar a pesquisa de Rea-Guaman et al. [Rea-Guaman et al. 2017] que, através de uma revisão sistemática da literatura, aponta os principais modelos de maturidade utilizados para segurança cibernética, diferenciando da presente por tratar apenas da área de maturidade para cibersegurança e pesquisando trabalhos entre 2012 e 2016. Já Albuquerque Junior e Santos [Albuquerque Junior and Santos 2014] fazem um levantamento da produção científica sobre segurança da informação em eventos nacionais de administração e áreas afins, no período de 2004 a 2013, verificando o contexto de realização, os modelos ou teorias utilizadas, suas referências e etc. Com isto, analisam a quantidade de publicações sobre o tema, principalmente em trabalhos que utilizam teorias das ciências sociais.

3. Método

Esta pesquisa foi conduzida por meio de um mapeamento sistemático da literatura, uma forma de identificar, avaliar e interpretar todas as pesquisas ou fenômenos disponíveis relevantes para uma questão de pesquisa específica, área temática, ou fenômeno de interesse [Kitchenham and Charters 2007]. Para Petersen et al.[Petersen et al. 2008], o MSL é definido como um estudo secundário, pois analisa estudos primários visando sintetizar ou integrar as evidências. Com base nos guias propostos por Petersen et. al [Petersen et al. 2008] e Kitchenham e Charters [Kitchenham and Charters 2007], foi gerado um processo para operacionalizar a presente pesquisa (Quadro 1).

Quadro 1. Etapas do processo de MSL

Planejamento	Execução	Análise e Divulgação
- Formulação da questão de pesquisa - Elaboração do Protocolo	- Identificação dos trabalhos - Avaliação crítica dos trabalhos - Extração dos dados	- Sintetização dos resultados - Interpretação dos resultados - Exposição dos resultados

Neste contexto, as perguntas que cercaram esta pesquisa foram:

P1. Qual é o atual estado da arte das publicações nos principais eventos e periódicos nacionais na área de Governança / Gestão / Maturidade em Segurança da Informação no meio Corporativo?

P2. Quais são os principais desafios na implantação da Governança / Gestão / Maturidade em Segurança da Informação no meio Corporativo?

P3. Quais são os principais modelos, padrões ou frameworks utilizados para implantar a Governança / Gestão / Maturidade em Segurança da Informação no meio Corporativo?

P4. Quais são os principais modelos, padrões ou frameworks utilizados para avaliar a Governança / Gestão / Maturidade em Segurança da Informação no meio Corporativo?

Para se chegar aos principais eventos e periódicos da área de Computação, buscou-se a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), fundação vinculada ao Ministério da Educação (MEC). Na Capes verificou-se a classificação Qualis mais recente dos eventos[1] e periódicos[2] em Ciência da Computação.

Com as listas citadas, foram analisados os eventos e periódicos nacionais de maior relevância (classificados com Qualis) e que tiveram em suas chamadas correlação com a área de pesquisa, sendo definido, como temporalidade para a pesquisa os últimos 10 anos (2008-2017). Os eventos e periódicos selecionados são exibidos no Quadro 2.

Mesmo não estando na lista da Capes, o SBTI foi selecionado pelos autores como uma forma, inicial, de aumentar a base de eventos e, também, por ser um evento novo que vem crescendo na área e que aceita submissões na área da presente pesquisa. Com relação aos periódicos, a Revista IEEE América Latina, mesmo não sendo explicitamente uma revista nacional, tem grande correlação com o Brasil: sua equipe editorial, frequentemente, é composta por pesquisadores brasileiros, a plataforma de submissão de artigos é em parceria com a Universidade de São Paulo, tem um grande número de publicações de pesquisadores nacionais e aceita publicação em língua portuguesa. Por isso, a Revista IEEE América Latina também foi incluída no estudo.

Quadro 2. Eventos e Periódicos selecionados

ISSN	Nome	Em 2017	Qualis
-	Simpósio Brasileiro de Sistemas de Informação (SBSI)	13ª edição	B2
-	Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)	17ª edição	B3
1041-2448	International Conference on Information Systems and Technology Management (CONTECSI)	14ª edição	B4
-	Simpósio Brasileiro de Tecnologia da Informação (SBTI)	6ª edição	-
1678-4804	Journal of the Brazilian Computer Society	23º volume	B1
1984-2902	ISys: Revista Brasileira de Sistemas de Informação	10º volume	B3
2175-2745	Revista de Informática Teórica e Aplicada: RITA	24° volume	B3
1548-0992	Revista IEEE América Latina	15º volume	B4
1807-1775	Revista de Gestão da Tecnologia e Sistemas de Informação (JISTEM)	14º volume	B5
2237-2903	Revista de Sistemas e Computação - RSC	7º volume	B5
2237-5112	Revista de Tecnologia da Informação e Comunicação (RTIC)	7º volume	B5
1677-3071	Revista Eletrônica de Sistemas de Informação (RESI)	16º volume	B5
1983-5604	Sistemas de Informação (Macaé) / Revista de Sistemas de Informação da FSMA	20ª edição	B5

[1] https://www.capes.gov.br/images/documentos/Qualis_periodicos_2016/Qualis_conferencia_ccomp.pdf

[2] https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsf

3.1. Estratégia de Busca

De uma forma geral, na estratégia de busca, procura-se criar a string de pesquisa seguindo um conjunto de passos para que se consiga extrair os resultados esperados. Neste trabalho, a string de pesquisa foi concebida através das seguintes etapas: divisão da questão de pesquisa em termos individuais; definição de um conjunto de sinônimos e termos associados; tradução dos termos para a língua desejada (neste caso, português e inglês); e, por fim, agrupamento dos termos através de aspas e operadores lógicos E (and) e OU (OR).

No estudo buscou-se criar uma string de pesquisa ampla na tentativa de contemplar, nesta etapa, a maior quantidade de trabalhos da área, sendo, se necessário, eliminados em etapas posteriores. Para a criação da string de busca foi utilizada a expertise de três pesquisadores envolvidos no projeto, todos com formação na área de computação (1 graduado, 1 especialista e 1 doutorando), com experiência profissional de, no mínimo, dois anos na área de segurança da informação e com publicação acadêmica na área de segurança da informação. Além disso, os três pesquisadores analisaram outros trabalhos semelhantes e as publicações em 2016 de cada periódico e evento selecionados em busca das expressões utilizadas no título e palavras-chave dos trabalhos da área em questão.

O conjunto de string de pesquisa utilizado foi testado nas publicações de 2015 (ano anterior a base que formulou a string de pesquisa) de todos os periódicos e eventos da base selecionada. Para isso, os pesquisadores buscaram os trabalhos referentes à área de pesquisa manualmente em cada evento e periódico e o resultado foi comparando com o resultado da string de pesquisa. Devido a amplitude da string de pesquisa, este método encontrou todos os trabalhos levantados pelos pesquisadores e ainda inseriu outras pesquisas que deveriam ser eliminadas em etapas posteriores. Esse teste atendeu às expectativas dos pesquisadores, sendo utilizada a estrutura de busca a seguir.

String de Busca: [“qualquer palavra base”] ou [“Segurança” e “qualquer palavra complementar”] ou [“Security” e “qualquer palavra complementar”] ou [“Risco” e “qualquer palavra complementar”] ou [“Risk” e “qualquer palavra complementar”].

Palavras Base: “Segurança da Informação” ou “Information Security”, 17799 ou 17.799, 27001 ou 27.001, 27002 ou 27.002, 27005 ou 27.005, 27006 ou 27.006, 27014 ou 27.014.

Palavras Complementares: Alinhamento ou Alignment, Ameaça ou Threat, Auditoria ou Audit, Framework, Gerência ou Gerenciamento ou Gestão ou Management, Governança ou Governance, Impacto ou Impact, Incidente ou Incident, Maturidade ou Maturity, Medida ou Measure, Método ou Method, Métrica ou Metric, Modelo ou Model, Planejamento ou Planning, Política ou PSI ou Policy ou ISP, Vulnerabilidade ou Vulnerability.

Com o conjunto de string de busca formado, foi pesquisado, no título dos artigos, aqueles que se enquadram nas características desejadas no período de 10 anos (2008-2017). Sendo esta a Fase 1 do MSL. Esta Fase 1 foi realizada pelos três pesquisadores da área de segurança da informação envolvidos no projeto.

Após realizar a análise da base de dados até a etapa final, foi criada a base de artigos resultantes. Nessa nova base, como uma segunda fase de busca, foi aplicada a técnica de snowball [Biernacki and Waldorf 1981], que pode ser vista como uma técnica de amostragem que utiliza cadeias de referência, uma espécie de rede, sendo os artigos encontrados as sementes e suas referências as indicações. Ou seja, será utilizada o conjunto de string de busca nas referências dos artigos selecionados.

A técnica de snowball foi planejada para ser aplicada em até 10 ciclos ou até o seu esgotamento, o que acontecer primeiro. O esgotamento é o ponto de saturação que ocorre quando as referências do trabalho analisado não retornam mais pesquisas para o presente trabalho. Os ciclos podem ser entendidos como a aplicação da técnica em um bloco de artigos. Por exemplo, a aplicação da técnica de snowball na base de artigos resultado da pesquisa é o 1º ciclo, gerando a base de resultado (nomeada, por exemplo, de snow1). A aplicação da técnica na base de resultados snow1, é o 2º ciclo, gerando a base snow2. E assim sucessivamente.

Na técnica de snowball foi utilizado o mesmo conjunto de string de busca e os mesmos critérios e fases da etapa anterior. Esta etapa visou buscar outros artigos relevantes para a área dos eventos e periódicos já buscados e que, por qualquer falha, não foram catalogados ou, e principalmente, artigos de outras bases de dados que atendam aos critérios. O resultado do snowball (Fase 2) será somado aos artigos encontrados na Fase 1, completando o MSL.

3.2. Critérios de Inclusão e Exclusão

Segundo [Kitchenham and Charters 2007], a estratégia de seleção deve ser feita a partir de critérios de inclusão (CI) e de exclusão (CE). Os critérios balizadores desta pesquisa são expostos a seguir.

Critérios de Inclusão:

- CI 1: Pesquisas que identificam fatores que levam a Governança, Gestão ou Maturidade da Segurança da Informação no meio Corporativo;
- CI 2: Pesquisas que identificam técnicas que levam a Governança, Gestão ou Maturidade da Segurança da Informação Corporativa;
- CI 3 Pesquisas que argumentam sobre Governança, Gestão ou Maturidade da Segurança da Informação Corporativa;
- CI 4: O Resumo (ou introdução no caso de inexistência de resumo) menciona ações para Governança, Gestão ou Maturidade da Segurança da Informação Corporativa;
- CI 5: Pesquisa publicada em evento ou periódico nacional ou demais previamente delimitados no escopo da pesquisa.

Critérios de Exclusão:

- CE 1: Pesquisas não relacionadas à Governança, Gestão ou Maturidade de Segurança da Informação Corporativa;
- CE 2: Pesquisas se referindo a Governança, Gestão ou Maturidade de Segurança da Informação apenas como projetos de pesquisa futuros;
- CE 3: Documentos incompletos, rascunhos, documentos de compilação dos anais de conferências (proceedings), tutoriais e apresentações em slides;

- CE 4: Pesquisas não acessíveis, de forma gratuita, pela Internet;
- CE 5: Pesquisa com Título e resumo não escritos em Português ou Inglês;
- CE 6: Pesquisa não escrita em Português, Inglês ou espanhol;
- CE 7: Pesquisas Duplicadas, resultantes de uma mesma pesquisa ou com pequenas mudanças para uma publicação anterior (será selecionada a pesquisa mais recente);
- CE 8: Governança, Gestão ou Maturidade da Segurança da Informação Corporativa não ser parte das contribuições do estudo ou não ter diretrizes para o mesmo no resumo;
- CE 9: Documentos que não foram publicados nos últimos 10 anos do evento ou periódico (de 01/01/2008 até 30/12/2017);
- CE 10: Pesquisas voltadas para área técnica de segurança (como redes de computadores, firewall, criptografia, banco de dados, ferramentas, etc) ou aplicadas, exclusivamente, em um contexto específico (por exemplo, gestão de segurança no desenvolvimento de softwares);
- CE 11: Livros, dissertações ou teses.

3.3. Condução do Mapeamento

A etapa de condução do mapeamento envolve a seleção e avaliação das fontes de informação através dos CI's e CE's definidos, ou seja, durante a execução os trabalhos são expostos aos critérios, com intuito de filtrar, deixando apenas aqueles que estão de acordo com as definições metodológicas do trabalho. Em todas as etapas são averiguados todos os CI's e CE's, verificando se o trabalho passará para a próxima fase.
A condução da pesquisa foi realizada em dois blocos. O primeiro bloco consiste:

- Etapa 1: seleção, através do conjunto de string de busca, no título dos artigos dos eventos e periódicos selecionados (Quadro 2);
- Etapa 2: leitura do resumo dos artigos resultantes da Etapa 1;
- Etapa 3: leitura da introdução e conclusão dos trabalhos resultantes da etapa anterior;
- Etapa 4: leitura completa dos artigos resultantes da Etapa 3.

No segundo bloco foi realizado a técnica de snowball:

- Etapa 5: aplicação da técnica de snowball. Seleção, através do conjunto de string de busca, no título dos artigos referenciados.
- Etapa 6: leitura do resumo dos artigos resultantes da Etapa 5;
- Etapa 7: leitura da introdução e conclusão dos trabalhos resultantes da etapa anterior;
- Etapa 8: leitura completa dos artigos resultantes da Etapa 7.

O segundo bloco foi repetido até o esgotamento da técnica ou por até 10 ciclos. Na Etapa 5 foi analisado se o trabalho selecionado já tinha sido inserido anteriormente.

4. Resultados: Trabalhos Obtidos

Com a realização da pesquisa, foram encontrados 32 artigos aderentes ao escopo definido na Fase 1, sendo 78,12% (25 artigos) oriundos dos eventos e 21,87% (7 artigos) de periódicos. Dos quatro eventos, 3 (75%) retornaram artigos para esta

pesquisa. Enquanto dos nove periódicos, apenas 33,33% (3 periódicos) contribuíram. O Quadro 3 demonstra o resultado dos artigos após cada etapa.

O SBTI 2017, até o dia 30/12/2017 não havia disponibilizado seus anais. Sendo desconsiderado, conforme CE 4. Exceto o SBTI, a RSC e RTIC, todos os demais têm produção desde 2008. No SBSEG também foram computados os workshops, tendo, inclusive, contribuído com dois artigos para o resultado final do SBSEG.

Finalizada a primeira etapa do processo, resultando em 32 trabalhos, foi aplicada a técnica de snowball nos mesmos. Os critérios continuavam os mesmos, utilizando o conjunto de string de busca predefinido para analisar as referências de cada um dos artigos resultantes da primeira etapa.

Quadro 3. Trabalhos resultantes por etapa (Fase 1)

Evento / Periódico	Base de Artigos	Etapa 1: String de Busca	Etapa 2: Resumo	Etapa 3: Intro. e Conclusão	Etapa 4: Leitura completa
SBSI	605 (100%)	12 (1,98%)	10 (1,65%)	6 (0,99%)	6 (0,99%)
SBSeg	542 (100%)	14 (2,58%)	8 (1,48%)	3 (0,55%)	3 (0,55%)
CONTECSI	2.591 (100%)	35 (1,35%)	22 (0,85%)	18 (0,69%)	16 (0,62%)
SBTI	114 (100%)	3 (2,63%)	1 (0,88%)	1 (0,88%)	0 (0,0%)
Brazilian Computer Society	229 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
ISys	112 (100%)	1 (0,89%)	1 (0,89%)	1 (0,89%)	1 (0,89%)
RITA	197 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
IEEE América Latina	2.519 (100%)	9 (0,36%)	5 (0,20%)	3 (0,12%)	3 (0,12%)
JISTEM	269 (100%)	8 (2,97%)	3 (1,11%)	3 (1,11%)	0 (0,0%)
RSC	110 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
Revista de TIC	83 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
RESI	140 (100%)	3 (2,14%)	3 (2,14%)	3 (2,14%)	3 (2,14%)
Sistemas de Informação (Macaé)	115 (100%)	4 (3,48%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
TOTAL	**7.614 (100%)**	**89 (1,17%)**	**53 (0,70%)**	**38 (0,50%)**	**32 (0,42%)**

Realizado o primeiro ciclo da snowball, com os 32 artigos anteriores, encontrou-se, pela string de busca, 19 trabalhos diferentes, porém, apenas 7 (36,84%) ainda não tinham sido catalogados na fase anterior. Analisando os demais critérios de inclusão e

exclusão, restaram apenas 2 trabalhos que atendem ao critério da presente pesquisa. Tendo esses 2 artigos como base, um novo ciclo (2º) da snowball foi realizado. Resultando em mais 2 trabalhos diferentes encontrados, porém, 1 já havia sido contabilizado, resultando em 1 trabalho novo encontrado. Neste trabalho, o 3º ciclo da snowball foi executado, não retornando mais nenhum trabalho que atendesse aos critérios da presente pesquisa. Encerrando-se a etapa da snowball pelo esgotamento da amostra com 3 novos trabalhos acrescentados (Quadro 4).

Quadro 4. Resultado dos trabalhos inseridos na Fase 2 (Snowball)

Snowball	Ciclo 1	Ciclo 2	Ciclo 3	Total
Artigos Analisados	32	2	1	**35**
Artigos Resultantes	2	1	0	**3**

Os três artigos resultantes pela snowball são oriundos da Revista Formadores (ISSN 1806-5457), Revista de Informática Aplicada (RIA - ISSN 1809-5585) e do Encontro da ANPAD, publicados, respectivamente, em 2014, 2008 e 2010.

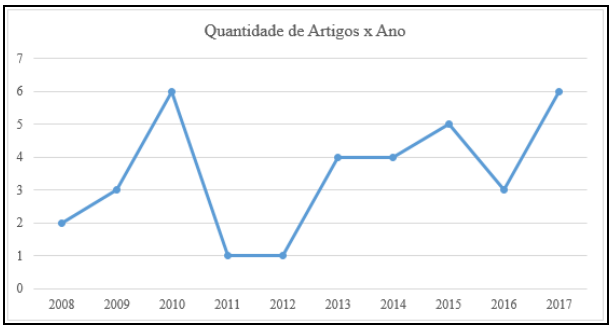
Ao analisar os autores dos trabalhos encontrados, verificou-se 90 pesquisadores distintos, doze destacaram-se com mais de uma publicação (Quadro 5).

Quadro 5. Principais autores

Quantidade de Artigos	Autores
4	Gliner Dias Alencar
2	Adolfo Alberto Vanti
2	Alcides Jeronimo de Almeida Tenorio Junior
2	Anderson Apolonio L. Queiroz
2	Antonio Eduardo de Albuquerque Junior
2	Ernani Marques dos Santos
2	Hermano Perrelli de Moura
2	João Carlos Soares de Alexandria
2	Leonardo Lemes Fagundes
2	Márcio Aurélio Ribeiro Moreira
2	Mauro Cesar Bernardes
2	Raul Ceretta Nunes

Somando a primeira fase (32 artigos), resultado da busca nas bases de dados de eventos e periódicos pré-selecionados, com a Fase 2 (snowball) obteve-se 35 trabalhos resultantes, distribuído, temporalmente, conforme Gráfico 1.

Gráfico 1. Distribuição temporal dos trabalhos resultantes



Percebe-se, em termos percentuais, que a área de pesquisa selecionou 2,14% dos artigos da RESI, 0,99% do SBSI e 0,89% da ISys (Quadro 3) o que aponta que a área pretendida está mais voltada para Sistemas de Informação do que, propriamente, nos eventos de Segurança da Informação. Em termos absolutos, quantitativo, tem-se a grande contribuição do CONTECSI e do SBSI para esta área, com, respectivamente, 45,71% e 17,14% dos resultados, novamente eventos de Sistemas de Informação.

4.1. Áreas Temáticas Encontradas

Os artigos encontrados seriam classificados nas três áreas do escopo da pesquisa: Governança, Gestão e Maturidade. Após a análise dos 35 trabalhos selecionados, mais três áreas de pesquisa, emergiram. As seis áreas temáticas são apresentadas, por ordem alfabética, no Quadro 6, que excede o quantitativo dos artigos encontrados por se ter artigos trabalhando, diretamente, mais de uma área.

Percebe-se um crescimento na quantidade de artigos na área pesquisada nos últimos cinco anos (2013-2017), apresentando 62,86% dos trabalhos encontrados. Todas as áreas temáticas tiveram mais publicações no último quinquênio, destacando-se as áreas temáticas de Riscos com 87,50% das publicações nos últimos cinco anos, PSI com 85,71% e Maturidade com 83,33%.

Quadro 6. Trabalhos encontrados por área temática e ano

	Aspectos Humanos	Gestão	Governança	Maturidade	PSI	Riscos
2008		[Mendes and Moreira 2008][Vianez et al. 2008]				
2009		[Oliveira et al. 2009]	[Machado et al. 2009][Breternitz et al. 2009]			
2010	[Roque et al. 2010]	[Alexandria and Quoniam 2010][Kroll et al. 2010] [Roque et al. 2010][Nobre et al. 2010]		[Mayer and Fagundes 2010]	[Zanichelli and Martimiano 2010]	[Mayer and Fagundes 2010]
2011			[Knorst and Vanti 2011]			

2012		[Alexandria 2012]	[Alexandria 2012]			
2013	[Alencar et al. 2013]	[Mattes and Petri 2013] [Alencar et al. 2013][Gualberto et al. 2013]		[Rigon and Westphall 2013]	[Mattes and Petri 2013] [Alencar et al. 2013]	[Gualberto et al. 2013]
2014		[Fernandes et al. 2014] [Albuquerque Junior et al. 2014]	[Fontes 2014]	[Weber et al. 2014]	[Fontes 2014]	[Fernandes et al. 2014] [Weber et al. 2014]
2015		[Silva Neto et al. 2015] [Fazenda and Fagundes 2015]	[Freitas et al. 2015][Albuquerque Junior and Santos 2015]		[Silva Neto et al. 2015]	[Bueno et al. 2015]
2016						[Arima et al. 2016] [Montenegro et al. 2016] [Santos-Olmo et al. 2016]
2017	[Moreira and Almeida 2017]	[Amorim and Bernardes 2017][Alencar et al. 2017a]	[Alencar et al. 2017b] [Amorim and Bernardes 2017] [Menezes et al. 2017]	[Alencar et al. 2017b] [Menezes et al. 2017] [Silva and Barros 2017]	[Moreira and Almeida 2017] [Alencar et al. 2017a]	
Total	**3**	**17**	**10**	**6**	**7**	**8**

5. Análise das Áreas Temáticas

5.1. Aspectos Humanos

Como principais desafios nesta área, [Moreira and Almeida 2017] abordam a necessidade de conscientização daqueles que utilizam os recursos e tecnologias, principalmente dos funcionários de maior escalão. Já [Alencar et al. 2013] apontam, também, a restrição orçamentária e ausência de priorização para a área. Por fim, [Roque et al. 2010] citam que as normas e padrões atuais são técnicos, não garantindo a sustentação da cultura de segurança, sendo necessário requisitos humanos (responsabilidade, confiança e ética).

Apenas [Roque et al. 2010] apresentam soluções para implantação e avaliação da segurança da informação, neste caso citando um modelo próprio.

5.2. Gestão da Segurança da Informação

Os principais desafios apontados nesta área foram: entendimento e atendimento às normas vigentes [Amorim and Bernardes 2017]; falta de apoio em nível estratégico ou de áreas de negócio [Alexandria 2012] [Amorim and Bernardes 2017] [Fazenda and Fagundes 2015] [Nobre et al. 2010]; cultura organizacional [Amorim and Bernardes 2017]; complexidade das normas de segurança [Alencar et al. 2017a]; conhecimento da organização e de sua cultura para definir padrões que realmente as atendam [Kroll et al.

2010] [Mattes and Petri 2013] [Silva Neto et al. 2015]; conscientização dos usuários [Alexandria and Quoniam 2010] [Nobre et al. 2010]; limitações financeiras [Silva Neto et al. 2015]; falta de metodologias voltadas "ao como fazer" [Oliveira et al. 2009] e que abordem requisitos de responsabilidade, confiança e ética dos usuários [Roque et al. 2010]; complexidade do ambiente e modelos de risco [Gualberto et al. 2013]; demonstrar a utilidade de sua aplicação [Nobre et al. 2010]; heterogeneidade do ambiente [Albuquerque Junior et al. 2014].

Para implantação e avaliação foram citados: as normas ISO/IEC da família de segurança 27001 e 27002 em suas diversas versões [Alexandria 2012; Bueno et al. 2015; Fazenda and Fagundes 2015; Manoel 2014; Nobre et al. 2010; Silva and Barros 2017], ITIL [Mayer and Fagundes 2010]; ISO/IEC 21827 [Knorst and Vanti 2011] e Seis Sigma [Nobre et al. 2010]. Além de alguns modelos próprios [Alencar et al. 2017a] [Alexandria and Quoniam 2010] [Amorim and Bernardes 2017] [Gualberto et al. 2013] [Roque et al. 2010] baseados, principalmente, nos arcabouços aqui citados.

5.3. Governança de Segurança da Informação

Os principais desafios para os trabalhos desta área foram: custo [Alencar et al. 2017b] [Menezes et al. 2017]; entendimento e atendimento as normas vigentes [Amorim and Bernardes 2017]; falta de apoio em nível estratégico e de áreas de negócio [Alencar et al. 2017b] [Alexandria 2012] [Amorim and Bernardes 2017] [Fontes 2014]; cultura organizacional [Amorim and Bernardes 2017] [Knorst and Vanti 2011]; Complexidade das normas [Alencar et al. 2017b] [Freitas et al. 2015]; qualificação dos profissionais [Freitas et al. 2015]; conscientização dos usuários [Freitas et al. 2015]; falta de padronização dos procedimentos internos [Breternitz et al. 2009].

Para implantação e avaliação foram citados: aplicação direta da ISO/IEC 27001, 27002 ou 27005 [Albuquerque Junior and Santos 2015] [Alexandria 2012], ISO/IEC 9000 [Knorst and Vanti 2011], ITIL [Breternitz et al. 2009], NIST CSF e Cobit [Freitas et al. 2015]; três trabalhos também citam arcabouços próprios [Alencar et al. 2017b] [Amorim and Bernardes 2017] [Menezes et al. 2017], baseados, principalmente, nos normativos e modelos citados neste parágrafo.

5.4. Maturidade da Segurança da Informação

Os trabalhos categorizados nesta área temática apontaram como principais desafios o custo [Alencar et al. 2017b] [Menezes et al. 2017]; alcançar a eficiência da infraestrutura de gestão de riscos de TI para garantir a gestão de vulnerabilidade e segurança de sistemas de informação [Weber et al. 2014]; a não existência de modelos de maturidade na área [Mayer and Fagundes 2010] [Rigon and Westphall 2013]; falta de conhecimento por parte das empresas e a segurança da informação limitada ao setor de informática [Silva and Barros 2017]; abrangência da área de segurança da informação [Rigon and Westphall 2013]; e, por fim, a complexidade das normas e falta de apoio ou definição estratégica por parte do alto escalão [Alencar et al. 2017b].

Para implantação e avaliação da maturidade foram cogitados o COBIT [Weber et al. 2014], os demais trabalhos utilizam modelos próprios baseados nas normas da família de segurança (ISO/IEC 27001, 27002, 27005 ou 27014 em suas diversas versões).

5.5. Política de Segurança da Informação

Os principais desafios para os trabalhos desta área foram: conscientização e comprometimento do alto escalão e áreas de negócio para priorização da segurança da informação [Alencar et al. 2013; Fontes 2014; Moreira and Almeida 2017]; restrições orçamentárias [Alencar et al. 2013; Silva Neto et al. 2015]; complexidade das normas de segurança [Alencar et al. 2017a]; conhecimento da organização e sua cultura para definir padrões que realmente atendam [Mattes and Petri 2013; Silva Neto et al. 2015; Zanichelli and Martimiano 2010].

As normas da ISO/IEC 27001 e 27002 em suas diversas versões foram os únicos arcabouços citados explicitamente nos trabalhos [Alencar et al. 2013, 2017a; Mattes and Petri 2013; Silva Neto et al. 2015; Zanichelli and Martimiano 2010].

5.6. Riscos

Os principais desafios para os trabalhos desta área foram: alcançar a eficiência da infraestrutura de gestão de riscos de TI para garantir a gestão de vulnerabilidade e segurança de sistemas de informação [Weber et al. 2014]; a não existência de modelos na área para medir e avaliar aderentes ao SGSI [Mayer and Fagundes 2010]; complexidade e entendimento do ambiente [Fernandes et al. 2014] [Montenegro et al. 2016]; custo e necessidade de pessoas e ferramentas especializadas [Santos-Olmo et al. 2016]; falta de ações estratégicas [Zanichelli and Martimiano 2010]; complexidade do ambiente e modelos de risco [Gualberto et al. 2013] [Montenegro et al. 2016].

Para implantação e avaliação foram cogitados, principalmente, o COBIT [Weber et al. 2014], a ISO/IEC 27002 (ainda em sua "versão" 17799) [Fernandes et al. 2014]; a ISO/IEC 27005 [Zanichelli and Martimiano 2010]; e modelos próprios [Gualberto et al. 2013; Mayer and Fagundes 2010; Montenegro et al. 2016; Santos-Olmo et al. 2016] baseados, sobretudo, nas variadas versões da ISO/IEC 27001, 27002, 27005 e COBIT.

6. Considerações Finais

Ao analisar os trabalhos encontrados acredita-se ter respondido as quatro perguntas propostas no mapeamento. Verificou-se que a publicação na área buscada ocorreu mais em eventos de sistemas de informação, do que em eventos de segurança da informação. Ademais, observou-se um crescimento de publicações na área, especialmente nos últimos cinco anos (Gráfico 1).

A pergunta principal do trabalho, *P1. Qual é o atual estado da arte das publicações nos principais eventos e periódicos nacionais na área de Governança / Gestão / Maturidade em Segurança da Informação no meio Corporativo?*, de forma sucinta pode ser respondida com a análise realizada e exibida nas Seções 4 e 5, que resultou em 35 trabalhos categorizados em seis áreas temáticas: Aspectos Humanos, Gestão da Segurança da Informação, Governança de Segurança da Informação, Maturidade da Segurança da Informação, Política de Segurança da Informação e Riscos (Quadro 6). Tendo os principais autores expostos no Quadro 5.

A abrangência da área de segurança da informação resultou em desafios com características bem distintas, sendo exibidos, de forma detalhada por área temática, na

Seção 5. Como principais desafios, cita-se: falta de recursos financeiros ou custo elevado; complexidade, não existência ou não aderência aos modelos ou arcabouços da área; complexidade e abrangência do ambiente e ações; falta de priorização ou comprometimento por parte do alto escalão; conscientização dos usuários; entre outros. Os desafios expostos respondem à Pergunta 2 e podem ser considerados uma contribuição relevante do trabalho para a área.

O próximo quadro (Quadro 7) sintetiza as 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. A tabulação contempla todas as suas versões de cada arcabouço citado, bem como a sua utilização direta ou indireta, quando o trabalho cita um modelo próprio, mas baseado em algum dos arcabouços tradicionais. Resumindo, assim, as respostas referentes às Perguntas 3 e 4 do método proposto. Ressalta-se que o somatório dos trabalhos no Quadro 7 ultrapassa os 35 artigos analisados. Tal fato se deve por, com frequência, um trabalho utilizar mais de um arcabouço.

Quadro 7. Principais arcabouços citados

Quantidade de Artigos		Norma, Padrão, Modelo, Framework, Documento, Metodologia ou Teoria
Implantação	Avaliação	
14	14	ISO/IEC 27002
10	10	ISO/IEC 27001
8	7	ISO/IEC 27005
5	5	COBIT
3	3	ITIL

Interessante demonstrar que dos 35 artigos analisados, nove (25,71%) apontam para arcabouços diferentes entre implantação e avaliação, porém, ao analisar os dados consolidados (Quadro 7), percebe-se números, praticamente, iguais. Percebe-se a grande influência para a área da família de segurança de normas ISO/IEC (família 27000), em especial as normas 27001, 27002 e 27005. Porém nos aspectos humanos elas não foram cogitadas diretamente, mesmo existindo uma seção específica de segurança em recursos humanos na ISO/IEC 27001 e 27002, além de abordar a temática em outros controles.

Verificou-se, também, que a temática de PSI é bem atendida pelas normas ISO/IEC 27001 e 27002, visto que todos os trabalhos apontaram a utilização de tais arcabouços e nenhum inseriu modelo próprio. No outro extremo tem-se a área de maturidade, com a maioria dos artigos (83,33%) apontando para a utilização de novos modelos, em vez da utilização de algo já existente. Indicando que a área se encontra em evolução para consolidação e atendimento aos anseios corporativos.

Por fim, ressalta-se o nível Qualis dos eventos e periódicos investigados (Quadro 2), encontrando evento com o nível B2 e periódico B1, bem com a qualidade do material encontrado. O que aponta que é possível publicar nacionalmente e utilizar como embasamento os trabalhos locais, em conjunto com os internacionais. Podendo ser uma prática para o crescimento da pesquisa brasileira e sua divulgação, visando, no futuro, que os eventos e periódicos nacionais alcancem o nível A do Qualis, fato ainda inexistente no Brasil para a área de pesquisa em questão.

Estudos mais aprimorados são necessários para verificar a escolha por periódicos internacionais em detrimento aos brasileiros por alguns grupos de pesquisadores nacionais. No caso da escolha de periódicos níveis A, fica evidente a busca pelas revistas mais conceituadas, respaldando o trabalho a ser publicado. Porém, no caso de periódicos com a mesma classificação dos nacionais, fica a dúvida pela escolha. Algumas hipóteses são: (i) os veículos internacionais escolhidos têm maior visibilidade, (ii) existe alguma facilidade para publicação nos periódicos internacionais (agilidade na publicação, menor custo, etc), (ii) existe pré-conceito com os periódicos nacionais (considerando-os de segunda linha?). Tais fatores, se melhores entendidos e sanados, poderão proporcionar avanços para a pesquisa nacional e seios meios de divulgação.

Mesmo a pesquisa apresentando limitações, por exemplo: analisar apenas um conjunto de eventos e periódicos nacionais, as restrições geradas pela seleção temporal e da string de busca; acredita-se que esta análise apontou o estado atual das publicações nacionais na área em epígrafe, incentivando a realização de pesquisas sobre segurança da informação. Bem como contribuindo para a evolução e amadurecimento da área no meio corporativo e acadêmico.

Como forma de continuidade ao presente trabalho, bem como para a área pesquisada, sugere-se, como trabalhos futuro, a continuação da análise para os artigos produzidos após 2017; analisar outros periódicos e eventos (da área de computação ou não); comparar o resultado obtido com pesquisas internacionais; e correlacionar outros temas na área de segurança da informação.

Referências

ABNT (2013a). *NBR ISO/IEC 27014 - Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação*.

ABNT (2013b). NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. . ABNT.

Albuquerque Junior, A. E., Santos, E. M. and Albuquerque, E. S. (2014). 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.

Albuquerque Junior, A. E. De and Santos, E. M. Dos (30 may 2014). Scientific Production about Information Security on Brazilian Scientific Conferences. In *11th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI*. . TECSI. http://www.contecsi.fea.usp.br/envio/index.php/contecsi/11contecsi/paper/view/794.

Albuquerque Junior, A. E. De and Santos, E. M. Dos (2015). Adoption of Information Security Measures in Public Research Institutes. In *12th International Conference on Management of Technology and Information Systems - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/12CONTECSI/paper/view/3155.

Alencar, G. D., Queiroz, A. A. L. and Queiroz, R. J. G. B. (2013). Insiders: Um Fator Ativo na Segurança da Informação. In *IX Simpósio Brasileiro de Sistemas de Informação - SBSI*.

Alencar, G. D., Tenorio Junior, A. J. de A. and Moura, H. P. (2017b). Theoretical Guidelines for an Agile Model of Governance, Management and Maturity for Information Security. In *14th International Conference on Information Systems & Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4799.

Alencar, G. D., Tenorio Junior, A. J. de A. and Moura, H. P. (2017a). Information Security Policy: A Simplified Model Based on ISO 27002. In *14th International Conference on Information Systems & Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4859.

Alexandria, J. C. S. De (2012). A Picture of Information Security in Public Institutions of Scientific Research in Brazil. In *9th International Conference on Information Systems and Technology Management - CONTECSI*.

Alexandria, J. C. S. De and Quoniam, L. M. (2010). Proposal to Structure the Information Security Management in a Scientific Research Environment. In *7th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI*.

Amorim, E. S. De and Bernardes, M. C. (2017). A Model for Information Security Governance in Retail Enterprises. In *14th International Conference on Information Systems & Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4541.

Arima, C. H., Akabane, G., Souza, J. G. S., Kussama, L. and Oliveira, R. (2016). Information Security Risk Management and its Application in a Federal Public Institution. In *13th International Conference on Information Systems & Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/13CONTECSI/paper/view/3757.

Biernacki, P. and Waldorf, D. (29 nov 1981). Snowball Sampling: Problems and Techniques of Chain Referral Sampling. *Sociological Methods & Research*, v. 10, n. 2, p. 141–163.

Breternitz, V. J., Navarro Neto, F. and Navarro, A. F. (20 dec 2009). Gerenciamento de Segurança Segundo ITIL: Um Estudo de Caso em uma Organização Industrial de Grande Porte. *Revista Eletrônica de Sistemas de Informação*, v. 8, n. 2, p. 4.

Bueno, P. M. S., Ikuno, F. S., Araújo, A. S. De, et al. (2015). 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*.

Fazenda, R. V. and Fagundes, L. L. (2015). 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*.

Fernandes, F. C., Carpes, A. M. da S. and Diel, E. H. (2014). Information Security

Management: A Case Study in a Brazilian Financial Institution. In *11th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/11contecsi/paper/view/542.

Fontes, E. L. G. (2014). Alignment of Information Security with Business Areas - Contribution of NBR ISO/IEC 27002:2013. In *11th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/11contecsi/paper/view/714.

Freitas, R. B. De, Moraes, I. M. P. De, Miranda, F. P., Santana, A. C. and Sousa, T. de J. R. De (2015). Information Security Framework for Brazilian Small Business. In *12th International Conference on Management of Technology and Information Systems - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/12CONTECSI/paper/view/2326.

Gualberto, E. S., Sousa Jr, R. T. De, De Deus, F. E. G. and Duque, C. G. (2013). 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.

Isaca (2012). *COBIT 5: Modelo Corporativo para Governança e Gestão de TI da Organização*.

Junior, J. S. P., Silva, C. dos S. and Xavier, D. D. (2017). Segurança em Internet das Coisas : Um Survey de Soluções Lightweight. *Revista de Sistemas e Computação*, v. 7, n. 2, p. 365–384.

Kitchenham, B. and Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering. *EBSE Technical Report*. https://pdfs.semanticscholar.org/e62d/bbbbe70cabcde3335765009e94ed2b9883d5.pdf, [accessed on Jan 21].

Knorst, A. M. and Vanti, A. A. (2011). 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 and Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/8contecsi/paper/view/3299.

Kroll, J., Fontoura, L. M., Wagner, R. and D'Ornellas, M. C. (2010). 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*.

Machado, C. A. N., Cabral, L. A. F., Santos, J. P. and Motta, G. H. M. B. (2009). Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico. In *V Simpósio Brasileiro de Sistemas de Informação - SBSI*.

Manoel, S. da S. (2014). *Governança de Segurança da Informação: como criar*

oportunidades para o seu negócio. 1ª ed. Rio de Janeiro - RJ, Brasil: Brasport.

Mattes, I. V. and Petri, S. M. (2013). Accounting Information Security: Procedures for the Preparation of a Security Policy Based on ISO 27001 and ISO 27002. In *10th International Conference on Information Systems and Technology Management - CONTECSI*.

Mayer, J. and Fagundes, L. L. (2010). 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*.

Mendes, R. and Moreira, M. A. R. (2008). Itil on Security Information Management. In *5th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI*.

Menezes, B. P., Rocha, F. G., Menezes, P. M. and Nascimento, R. P. C. (2017). Strategic Planning Methodology for Information Security – PESEG 1.0. In *14th International Conference on Information Systems & Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4454.

Montenegro, C., Murillo, M., Gallegos, F. and Albuja, J. (2016). DSR Approach to Assessment and Reduction of Information Security Risk in TELCO. *IEEE Latin America Transactions*, v. 14, n. 5, p. 2402–2410.

Moreira, M. A. R. and Almeida, M. F. De (2017). 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*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/14CONTECSI/paper/view/4591.

Nobre, A. C. dos S., Ramos, A. S. M. and Nascimento, T. C. (2010). 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*. . https://repositorio.ufrn.br/jspui/bitstream/123456789/12138/1/AnnaCSN.pdf.

Oliveira, M. A. F., Nunes, R. C. and Ellwanger, C. (2009). 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*.

Petersen, K., Feldt, R., Mujtaba, S. and Mattsson, M. (2008). Systematic Mapping Studies in Software Engineering. In *12th International Conference on Evaluation and Assessment in Software Engineering - EASE*. . https://www.researchgate.net/profile/Michael_Mattsson/publication/228350426_Systematic_Mapping_Studies_in_Software_Engineering/links/54d0a8e90cf20323c218713d/Systematic-Mapping-Studies-in-Software-Engineering.pdf, [accessed on Jan 21].

PWC (2017). Pesquisa global de segurança da informação 2017. https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2017/pesquisa-global-seguranca-2017.html, [accessed on Feb 2].

Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S. and Calvo-Manzano, J. A. (jun 2017). Maturity models in cybersecurity: A systematic review. In *12th Iberian Conference on Information Systems and Technologies (CISTI)*. . IEEE. http://ieeexplore.ieee.org/document/7975865/, [accessed on Jan 21].

Rigon, E. A. and Westphall, C. M. (2013). Modelo de Avaliação da Maturidade da Segurança da Informação. *Revista Eletrônica de Sistemas de Informaçao*, v. v. 12, n. 1, p. 3.

Rigon, E. A., Westphall, C. M., Dos Santos, D. R. and Westphall, C. B. (2014). A Cyclical Evaluation Model of Information Security Maturity. *Information Management & Computer Security*, v. 22, n. 3, p. 265–278.

Rodrigues, C. K. da S. (2017). Uma análise simples de eficiência e segurança da Tecnologia Blockchain. *Revista de Sistemas e Computação*, v. 7, n. 2, p. 147–162.

Roque, A. dos S., Nunes, R. C. and Silva, A. D. (31 dec 2010). Proposition of a Dynamic Model for Managing Security Information on Industrial Environments. *Revista Eletrônica de Sistemas de Informação*, v. 9, n. 2, p. 7.

Santos-Olmo, A., Sánchez, L. E., Álvarez, E., Huerta, M. and Fernandez-Medina, E. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, v. 14, n. 6, p. 2897–2911.

Silva, M. P. Da and Barros, R. M. De (2017). Maturity Model of Information Security for Software Developers. *IEEE Latin America Transactions*, v. 15, n. 10, p. 1994–1999.

Silva Neto, G. M., Alencar, G. D. and Queiroz, A. A. L. (2015). Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In *XI Brazillian Symposium on Information Systems - SBSI*.

Vianez, M. de S., Segobia, R. H. and Camargo, V. (2008). Segurança de Informação: Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005. *Revista de Informática Aplicada*, v. 4, n. 1, p. 33–44.

Weber, E. L., Da Silva, M. H., Vanti, A. A. and Brum, M. C. da S. (2014). Analysis of Maturity Levels in IT Process Related to Information Systems Security. In *11th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI*. . http://www.contecsi.fea.usp.br/envio/index.php/contecsi/11contecsi/paper/view/758.

Zanichelli, A. de S. and Martimiano, L. A. F. (2010). Definição de uma Política de Segurança para um Ambiente de Desenvolvimento Distribuído de Software. In *Workshop de Trabalhos de Iniciação Científica e de Graduação - WTICG / X Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg*.