DOI: 10.5748/9788599693148-15CONTECSI/PS-5783

Scientific Production about Governance, Management and Maturity of Information Security in the Main Computing-Related Brazilian Journals and Conferences

Gliner Dias Alencar, https://orcid.org/0000-0002-7879-4766 (Instituto Brasileiro de Geografia e Estatística, Pernambuco, Brasil / Universidade Federal de Pernambuco, Pernambuco, Brasil) – gda2@cin.ufpe.br
Everton Silva de Amorim, https://orcid.org/0000-0001-8097-1189 (Universidade de São Paulo, São Paulo, Brasil) - everton.amorim@outlook.com
Breno Pinho Menezes, https://orcid.org/0000-0003-4463-8447 (Universidade Tiradentes, Sergipe, Brasil) - brenosampaiopinho@gmail.com
Hermano Perrelli de Moura, https://orcid.org/0000-0001-5992-2171 (Universidade Federal de Pernambuco, Pernambuco, Brasil) – hermano@cin.ufpe.br

The lack of security in information systems has caused a lot of moral and financial losses for the organizations. Many are the challenges to establish and maintain the Information Security effective and adds value. 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. But the organizations should implement the information security in a consistent, systematic manner in order to achieve compliance with current laws, standards and regulations. These difficulties demonstrate the need for a research focused on new ways to overcome such deficiency. This work shows the results about a systematic mapping of governance, management and maturity of information security. Method: Systematic Mapping Study. Results: 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.

Keywords: Information Security, Governance, Management, Maturity, Scientific Production.

Produção Científica sobre Governança, Gestão e Maturidade da Segurança da Informação nos Principais Periódicos e Eventos Brasileiros Relacionados à Computação

A falta de segurança em Sistemas de Informação tem provocado inúmeros prejuízos financeiros e morais para as organizações. Muitos são os desafios enfrentados para estabelecer e manter a Segurança da Informação eficaz e que de fato agregue valor. A adoção da segurança da informação, implementação de políticas e adequação a alguma norma não é algo simples. Mas as organizações precisam implementar a segurança da informação de forma consistente e sistemática, para buscar conformidades com leis, normas e regulamentações vigentes. 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. Utilizou-se o Método: Mapeamento sistemático. Resultados: Verificou-se o aumento do número de trabalhos nos últimos 5 anos e a utilização maciça das normas ISO/IEC 27001, 27002 e 27005.

Palavras-chave: Segurança da Informação, Governança, Gestão, Maturidade, Produção Científica.

1. INTRODUÇÃO

No decorrer dos anos o mercado vem modificando sua concepção de valor. Com estas mudanças, a informação tem tomado posição de destaque no meio corporativo, sendo considerada essencial para a tomada de decisões e para a continuidade dos negócios, atuando de forma estratégica e possibilitando análises internas e do mercado, configurando-se um novo ambiente, denominado por Castells (2009) como "Era da Informação". Podendo-se considerar a informação como uma commodities (como a eletricidade), sem a qual muitas empresas e organizações não funcionam (Silva & Barros, 2017).

Como grande fator dessa mudança da cultura decisória e, consequentemente, da utilização maciça das informações, está a evolução das Tecnologias da Informação e Comunicação (TICs), possibilitando o processamento de grandes volumes de dados e acesso às informações em todas as partes da empresa de forma rápida. Porém, essa mesma facilidade, e atual dependência, pode se tornar uma fragilidade gerando erros e danos em grande proporção.

Tal pensamento é compartilhado por Fontes (2006) quando o mesmo ressalta que a informação é um recurso que, atualmente, move o mundo, dando conhecimento do passado e guiando para onde seguir, sendo um recurso crítico para realização do negócio e execução das mais diversas missões da corporação, necessitando assim ser protegido. Diante disto, se faz necessário a implementação de ações de segurança da informação nas diversas etapas de criação, armazenamento, manipulação e utilização dos dados e da informação.

Diferente do que se aborda em algumas empresas, a pura aplicação de tecnologia não é suficiente para o tratamento da segurança da informação (Da Silva & Stein, 2007), corroborado, também, por Marciano & Lima-Marques (2006). No viés corporativo, isso se traduz na aplicação de segurança da informação de forma holística, abordando os aspectos relacionados à tecnologia, aos processos e às pessoas.

Ciente de tal necessidade, o primeiro ponto é verificar que materiais e estudos existem para que os órgãos, instituições e empresas, neste trabalho abordado como meio corporativo, possam obter o conhecimento sobre a área e, posteriormente, tenha embasamento suficiente para aplicação da segurança da informação. Bem como para que a área tenha sua evolução de forma a atender as necessidades mutantes do meio corporativo.

Enfatizando a segurança da informação na área de pesquisa da Computação, pode-se verificar duas vertentes. Uma linha técnica: abordando segurança de redes, criptografia, aplicativos de segurança, backup, redundância, segurança física e etc. E uma segunda linha: abordando aspectos humanos, de capacitação, governança, gestão, maturidade, normas, políticas, etc.

Este artigo é resultado de uma pesquisa com objetivo de analisar as publicações nos principais eventos e periódicos nacionais da área de computação com relação ao tema de segurança da informação, nos últimos 10 anos, que tratem a área de Governança, Gestão e Maturidade da Segurança da Informação. A intenção de tal análise é estratificar e identificar a evolução quantitativa dos trabalhos, quais os principais meios utilizados para divulgação das pesquisas, a região dos pesquisadores, o contexto em que cada trabalho foi realizado, entre outras características para exibir e representar a amostra colhida. Os eventos e periódicos selecionados, bem como o detalhamento metodológico são descritos em seção específica.

Acredita-se que esta análise apontará o estado atual das publicações nacionais na área em epígrafe, incentivando a realização de pesquisas sobre segurança da informação e contribuindo para a evolução e amadurecimento da área no meio corporativo e acadêmico.

Este artigo está organizado em mais quatro seções e as referências ao final. Na próxima seção é apresentado um pequeno referencial teórico para definir os conceitos de Segurança da Informação, abordando, mais precisamente, as áreas de Governança, Gestão e Maturidade. Na terceira seção é apresentado o método de pesquisa utilizado, os eventos e periódicos selecionados e todo o restante do processo. Os resultados e suas análises são exibidos na quarta seção. Finalizando o conteúdo produzido, o artigo aponta, em sua quinta seção, as considerações finais e trabalhos futuros.

2. SEGURANÇA DA INFORMAÇÃO

Ao analisar a evolução das espécies animais, inclusive da espécie humana, é notável a busca por segurança em seus diversos aspectos. No caso específico da segurança da informação, mesmo já existindo o pensamento há centena de anos, tem ganhado mais destaque quando formalizou-se a Era da informação (Castells, 2009).

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

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

Alencar, Tenorio Junior & Moura (2017a) corroboram com o assunto ao explanar que o aumento exponencial do número de dispositivos computacionais, de usuários e com as informações assumido o papel estratégico, gerou-se a necessidade de compartilhamento, disponibilidade e, consequentemente, de segurança.

Ciente que a ausência de segurança da informação pode acarretar em danos irreparáveis, até mesmo falência, bem como que. no mundo atual, globalizado e de grande concorrência, todo investimento carece de justificativas e alinhamentos, cresce a demanda por um olhar sistêmico e organizacional em todas as áreas. Na perspectiva da segurança da informação no ambiente corporativo, se reflete, diretamente, na Governança, Gestão e Maturidade da segurança da informação, temas que serão tratados na sequência.

2.1 Gestão da Segurança da Informação

Amorim & Bernardes (2017) apontam que 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".

Menezes, Rocha, Menezes & Nascimento (2017) seguem a mesma linha de pensamento, abordando, também, que gestão da segurança da informação deve ser realizadas em etapas, visando proteger as informações. Sendo necessário que todos os usuários com acesso às informações, saibam o limite do que é permitido e as responsabilidades tanto pela informação quanto por qualquer ativo a ela relacionado (Menezes et al., 2017).

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 (Alencar et al., 2017a). Os autores ainda colocam que, para que isso ocorra, é fundamental a elaboração, publicação e implantação do principal documento para a área: a Política de Segurança da Informação (PSI), devendo esta ser amplamente divulgada e apoiada pelo alto escalão. Para construção da PSI e de um Sistema de Gestão de Segurança da Informação (SGSI), os normativos da ISO/IEC 27001 e 27002 são os mais utilizados.

Segundo a norma de segurança ABNT NBR ISO/IEC 27001:2013 (ABNT, 2013a), um sistema de gestão da segurança da informação preserva 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. Sendo importante que o SGSI seja parte e esteja integrado com os processos da organização e com a estrutura de administração global. Bem como, que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles.

Desta forma, a gestão da segurança da informação pode ser entendida como um conjunto de ações para buscar, de forma contínua, a segurança da informação e dos ativos, principalmente nos níveis operacional e tático, visando atender e apoiar as ações organizacionais.

2.2 Governança de Segurança da Informação

Governança de Segurança da Informação (GSI), pode ser entendida com um conjunto de ações e práticas para o alinhamento das ações da área de segurança da informação com a estratégia da corporação (Alencar, Tenorio Junior, & Moura, 2017b). Manoel (2014) corrobora com o assunto ao citar que a GSI é uma parte da Governança de TIC, podendo haver sobreposição entre as duas. Mas se a Governança de TIC não existir, não é um impeditivo para as ações da Governança de Segurança da Informação. Nesta última situação, a GSI deverá estar vinculada à autoridade de maior escalão na tomada de decisão, por exemplo, o presidente da instituição.

A ISO/IEC 27014, publicada em 2013, traduzida no Brasil como ABNT NBR ISO/IEC 27014:2013, trata, exclusivamente, da Governança de Segurança da Informação, sendo um dos principais arcabouços para a área, apontando que 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, onde recomenda-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, 2013b).

Manoel (2014) acredita nos princípios citados pelo normativo ISO/IEC 27014 e enfatiza que aplicando tais preceitos de forma eficiente tende-se a ter tomadas de decisões na área de segurança da informação de forma mais rápida e acertadas; apresenta-se para a alta direção e demais envolvidos a situação concreta da área; tende-se a ter subsídios para investimentos mais eficientes e eficazes em segurança da informação; e encaminha à organização ao atendimento e conformidade com requisitos externos, por exemplo, legais, regulamentares ou contratuais.

Nesta área também pode-se citar o COBIT, sendo, segundo Gomes, Goulart Júnior, Simeão, de Sousa & Santana (2016), um dos importantes documentos da área e que aborda, de forma geral, a Governança de TIC, apontando melhores práticas para ser usada em todas as áreas citadas (serviço de TIC, Segurança da informação, Projetos, Fornecedores e Software). O COBIT foi desenvolvido e é mantido pela ISACA, atualmente em sua versão 5 (Isaca, 2012). Ciente da necessidade para a área de segurança da informação, duas extensões o COBIT 5 for Risk e o COBIT 5 for Information Security foram lanaçadas.

O COBIT 5 for Information Security é um guia para a área de Segurança da informação, fornecendo orientações para as organizações e seus profissionais a entender, utilizar e implementar atividades relevantes relacionadas à segurança da informação, bem como tomar decisões mais embasadas, mantendo a consciência sobre tecnologias emergentes e as ameaças que as acompanham (Isaca, 2012b). Já o COBIT 5 for Risk, complementa a visão de segurança abordando a área de Riscos. Não apenas sobre o risco de TIC, mas sobre os riscos do negócio, mais detalhadamente aos riscos de negócios associados ao uso, posse, operação e envolvimento de TIC e informações na empresa. Atuando como um facilitador em sua área, visto que já aponta cenários genéricos de riscos que podem ser ajustados ao ambiente (Isaca, 2013; Thomas, 2015).

Com a visão explanada até o momento, é possível perceber que Gestão da Segurança da Informação é diferente da Governança de Segurança da Informação. De forma geral, pode-se verificar que as duas se completam, a gestão trabalhando mais voltada para os aspectos táticos e operacionais, enquanto a governança nas camadas táticas e estratégicas. Diferença entre as áreas, com esta mesma abordagem, também é enfatizada e demonstrada por Amorim & Bernardes (2017).

2.3 Maturidade em Segurança da Informação

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 passos para se chegar a um nível mais avançado (Alencar et al., 2017b). Sendo o modelo de maturidade propício para isto.

Um modelo de maturidade deve ter objetivo de auxiliar as empresas na avaliação da segurança da informação. Para a avaliação, o modelo de maturidade apontará o estágio atual, bem como deixa claro o caminho para se chegar a níveis mais avançados (Silva & Barros, 2017).

Gomes et al. (2016) corroboram com a área ao apontar que um modelo de maturidade tem por objetivo auxiliar na melhoria contínua, por meio de processos, para que possam ser implementadas as melhores práticas. Rigon, Westphall, Dos Santos & Westphall (2014) e Isaca (2012) seguem por pensamentos semelhantes aos já apresentados, afirmando que o uso de um modelo de maturidade permite a identificação de lacunas que

representam risco e como mostrá-las a equipe de gestão. Com base nesta análise, planos de ação podem ser avaliados e desenvolvidos para a melhoria dos processos e controles considerados deficientes até o nível de desenvolvimento desejado.

Karokola, Kowalski & Yngström (2011) ressaltam a importância da implantação de um modelo de maturidade e afirma que diversas abordagens para gestão ou maturidade que apoiam a segurança da informação já estão disponíveis no mercado. Entre aquelas mais específicas para a área de segurança, pode-se apontar, conforme classificação de Rigon et al. (2014): Orientadas a Processo: COBIT e ITIL; Orientadas a Controle: ISO/IEC 27001; Orientadas a Produtos: como a ISO/IEC 15408; Orientadas a Gerenciamento de Risco: como OCTAVE e ISO 27005; e, por fim, Orientadas a Melhores Práticas: como ISO/IEC 27002.

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

2.4 Trabalhos Correlatos

Com a grande quantidade de materiais encontrados atualmente, sejam acadêmicos ou não, bem como a necessidade de uma formalização da revisão literária, é crescente a quantidade de trabalhos que buscam, como forma de contribuição para a área, consolidar os trabalhos existentes ou apontar a evolução da pesquisa em determinada área. Neste contexto, as pesquisas que abordam, por exemplo, análises bibliométricas, mapeamento sistemático e revisão sistemática são utilizadas.

Apesar de acreditar que a pesquisa não exauriu toda a literatura existente, não foi encontrado nenhum trabalho que tem como área de atuação Governança, Gestão e Maturidade da Segurança da Informação para anos recentes, até 2017. O que caracteriza a contribuição do presente trabalho para a área.

Ao se pesquisar sobre um levantamento com características semelhantes, pode-se citar os trabalhos de Albuquerque Junior e Santos (Albuquerque Junior & Santos, 2013, 2014a, 2014b). Os três trabalhos de Albuquerque Junior e Santos abordam a produção científica de segurança da informação, porém sobre um viés social, tendo ênfase no ambiente das Ciências Sociais.

Em Albuquerque Junior & Santos (2013) foi verificada a produção científica sobre segurança da informação em anais de Eventos da ANPAD (Associação Nacional de Pós-graduação e Pesquisa em Administração), sendo pesquisado de 2002 até 2012. O trabalho pesquisou o quantitativo de artigos em quase todas as áreas de segurança, utilizando as palavras “segurança”, “privacidade”, “confidencialidade”, “disponibilidade”, “integridade”, “risco”, “vigilância”, “fraude” e “proteção" (em português, inglês e espanhol) para buscar os trabalhos. De um total de 10.248 artigos publicados nos eventos da ANPAD pesquisados, resultou 1.075 na área de Sistemas de informação ou Tecnologia da Informação e 24 na área de segurança da informação.

Em Albuquerque Junior & Santos (2014a), agora utilizando as palavras “segurança”, “informação”, “privacidade”, “confidencialidade”, “disponibilidade”, “integridade”, “risco”, “segurança+informação”, “risco+informação”, “confidencialidade+informação”, “disponibilidade+informação” e “integridade+informação”, também em português, espanhol e inglês os autores realizaram uma análise das publicações brasileiras sobre segurança da informação sob a ótica social

em periódicos científicos entre 2004 e 2013, buscando em periódicos das áreas de Administração, Sistemas de Informação e Ciência da Informação. Utilizando esse vasto conjunto de palavras, o estudo resultou em 59 trabalhos, sendo considerado apenas 20 por tratarem a segurança da informação com enfoque social.

Em Albuquerque Junior & Santos (2014b) foi avaliada a produção científica sobre segurança da informação em eventos científicos brasileiros. Utilizando a mesma *string* de busca do trabalho de Albuquerque Junior & Santos (2013), escolheu-se os eventos que apresentaram trabalhos sobre sistemas de informações e sobre o tema segurança da informação, tanto com enfoque tecnológico quanto utilizando alguma abordagem social, sendo selecionado oito eventos pesquisados no período entre 2004 e 2013. O estudo resultou em 67 trabalhos que apontavam para as palavras de busca.

Pela natureza da pesquisa ser da área de segurança da informação, e ter a semelhança de três periódicos analisados em Albuquerque Junior & Santos (2014a), e de dois eventos também analisados por Albuquerque Junior & Santos (2014b), percebe-se que os trabalhos de Albuquerque Junior e Santos tem correlação com este, mas não inviabiliza a importância desta pesquisa. O presente trabalho aborda uma atualização da literatura, analisando eventos mais recentes (2008-2017), bem como incorpora outras palavras-chave e uma base diferente de eventos e periódicos. O enfoque pesquisado também é distinto. Enquanto Albuquerque Junior e Santos aderem à área das Ciências Sociais, este trabalho é mais aderente a área de Ciência da Computação, o que não inviabiliza a utilização, também, em outras áreas.

3. MÉTODO UTILIZADO

Esta pesquisa é conduzida por meio de um mapeamento sistemático da literatura (MSL), 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, como aborda Kitchenham & Charters (2007). Para Petersen, Feldt, Mujtaba & Mattsson (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. (2008) e Kitchenham & Charters (2007), foi gerado um processo para operacionalizar a presente pesquisa (Quadro 1).

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

Quadro 1. Etapas do processo.

Para que um mapeamento seja realizado, algumas características necessitavam ser definidas, destacando-se: a área de interesse, eventos e periódicos a serem pesquisados (base de dados) e temporalidade. Neste contexto, a pergunta que cerca esta pesquisa é: *Qual o estado atual e a evolução das publicações nos principais eventos e periódicos nacionais da área de computação com relação ao tema de segurança da informação, mais especificamente nas áreas de Governança, Gestão e Maturidade da Segurança da Informação?*

Diante da formulação da pergunta já se tem a área de interesse delimitada, bem como a base de dados (principais eventos e periódicos nacionais da área de computação). Para se chegar aos principais eventos e periódicos da área de Computação, buscou-se a entidade nacional responsável pela análise e classificação dos eventos e periódicos: a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), fundação vinculada ao Ministério da Educação (MEC). Na Capes verificou-se a lista mais recente da classificação Qualis dos eventos em Ciência da Computação, sendo a análise referente ao ano de 2016 a mais atual (disponível em: https://www.capes.gov.br/images/documentos/Qualis_periodicos_2016/Qualis_conferencia_ccomp.pdf), e dos periódicos, classificação do quadriênio 2013-2016 a vigente (disponível em: https://sucupira.capes.gov.br/sucupira/public/consultas/coleta/veiculoPublicacaoQualis/listaConsultaGeralPeriodicos.jsf).

Com as listas dos eventos e periódicos citados, foram analisados os eventos e periódicos nacionais de maior relevância 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 quatro eventos e os nove periódicos selecionados foram os apresentados no Quadro 2.

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

Periódico	1983-5604	Sistemas de Informação (Macaé) / Revista de Sistemas de Informação da FSMA	20ª Edição	B5

Quadro 2. Eventos e periódicos selecionados.

Mesmo não estando na lista de eventos da Capes, o Simpósio Brasileiro de Tecnologia da Informação foi selecionado pelos autores para entrar na base de dados, como uma forma, inicial, de aumentar a base de eventos e, também, por ser um evento que vem crescendo na área. Com relação aos periódicos, a Revista IEEE América Latina, mesmo não sendo explicitamente uma revista nacional, tem grande correlação com o Brasil, por exemplo: sua equipe editorial, frequentemente, é composta por pesquisadores brasileiros, a plataforma de submissão de artigos é em parceria com a Universidade de São Paulo (USP), tem um grande número de publicações de pesquisadores nacionais, aceita publicação em língua portuguesa e etc.

Percebe-se também que o evento CONTECSI apresenta os anais de seus trabalhos com ISSN, sendo o único evento da base selecionada com esse diferencial. Por fim, ressalta-se que a Revista de Sistemas de Informação da FSMA é a única da base selecionada que separa seus exemplares por edição e não por volume anual, tendo, cada ano duas edições.

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. Nesta pesquisa, 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, a língua inglesa); 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, todos da área de segurança, envolvidos no projeto, bem como analisado outros trabalhos semelhantes na área e as publicações de 2016 de cada periódico e evento selecionados em busca dos trabalhos da área em questão e, posteriormente, das strings utilizadas em seu título e palavras-chave. Sendo utilizada as strings de busca expostas no Quadro 3.

Palavras Base	Palavras Complementar	String de Busca
- “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	- 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	[“qualquer palavra base”] ou [“Segurança” e “qualquer palavra complementar”] ou [“Security” e “qualquer palavra complementar”] ou [“Risco” e “qualquer palavra complementar”]

	- 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	ou [“Risk” e “qualquer palavra complementar”]

Quadro 3. Strings de busca.

Após a definição do conjunto de string de pesquisa a ser utilizada (conforme detalhamento supracitado) a mesma foi testada 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, três pesquisadores buscaram os trabalhos referentes à área de pesquisa manualmente em cada evento e periódico e o resultado foi comparado 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.

Com o conjunto de string de busca formado, foi buscado, no título dos artigos, aqueles que se enquadram nas características desejadas no período de 10 anos (2008-2017), sendo incluído, em 2017, todos os trabalhos que se enquadrem na pesquisa e publicados e disponibilizados até 30/12/2017. O estudo foi realizado por três pesquisadores da área de segurança da informação.

3.2 Critérios de Inclusão e Exclusão

Segundo Kitchenham & 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 abaixo:

Critérios de Inclusão:

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

Critérios de Exclusão:

- CE 1: Pesquisas não relacionadas à Gestão, Governança ou Maturidade de Segurança da Informação Corporativa;
- CE 2: Pesquisas se referindo a Gestão, Governança 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: Gestão, Governança 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 critérios de inclusão e exclusão 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 critérios de inclusão e exclusão, verificando se o trabalho passará para a próxima etapa ou será eliminado.

A condução da pesquisa será realizada em dois blocos. O primeiro bloco consiste:

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

Com base nos procedimentos metodológicos explicitados o trabalho foi realizado e os resultados são exibidos nas seções posteriores.

4. A PRODUÇÃO CIENTÍFICA ENCONTRADA

Com a realização da pesquisa, foram encontrados 32 artigos aderentes ao escopo definido, 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 4 demonstra o resultado dos artigos após cada etapa.

Nos 10 anos de anais analisados, pelo menos um artigo foi publicado por ano e foram publicados em média 3,2 artigos por ano. Foram publicados apenas um artigo nos anos de 2008, 2011 e 2012, sendo estes os anos com menor quantidade de publicações. Já o ano de 2017 foi o que mais teve publicações sobre o tema, com 6 artigos. Como pode ser visto no Gráfico 1.

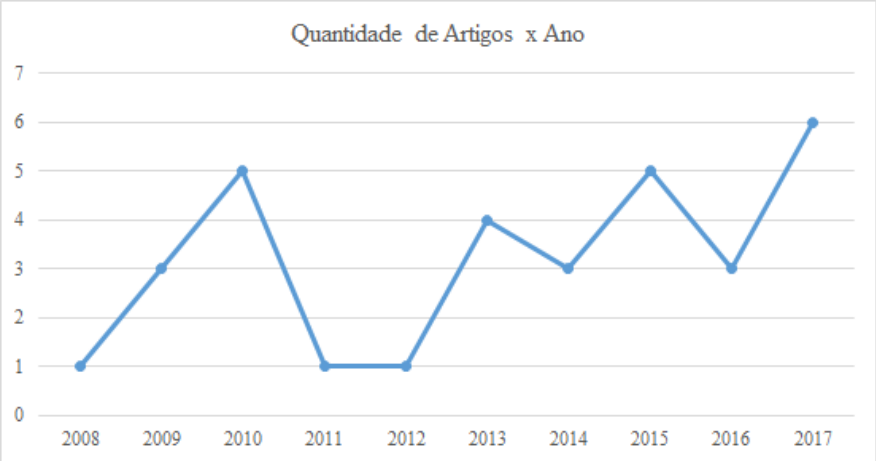

Gráfico 1. Evolução temporal da quantidade de artigos.

O SBTI 2017 foi realizado nos dias 30/10, 31/10 e 01/11/2017, porém até o dia 30/12/2017 não havia disponibilizado seus anais. Pela lista de artigos aprovados, disponibilizada no site do evento, foi possível perceber que um artigo se encaixaria na string de busca, porém, por não ser possível o acesso ao mesmo, este foi desconsiderado, conforme CE 4. Pelo mesmo motivo, não se sabe se o mesmo passaria pelas demais etapas ou seria eliminado.

Ressalta-se também que o SBTI, a Revista de Sistemas e Computação e a Revista de Tecnologia da Informação e Comunicação não foram computados seus dados desde 2008, visto que os mesmos não existiam. O SBTI começou a ser contabilizado no estudo em 2012, sua primeira edição, e as Revistas em 2011, quando lançaram seus primeiros volumes. Os demais eventos e periódicos tem produção desde 2008 e foi possível analisar a década planejada neste estudo (2008-2017).

Evento / Periódico	**Quantidade de Artigos**	**Etapa 1: String de Busca**	**Etapa 2: Leitura do Resumo**	**Etapa 3: Leitura da Introdução e Conclusão**	**Etapa 4: Leitura completa**
Simpósio Brasileiro de Sistemas de Informação (SBSI)	605 (100%)	12 (1,98%)	10 (1,65%)	6 (0,99%)	6 (0,99%)
Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)	542 (100%)	14 (2,58%)	8 (1,48%)	3 (0,55%)	3 (0,55%)
International Conference on Information Systems and Technology Management (CONTECSI)	2.591 (100%)	35 (1,35%)	22 (0,85%)	18 (0,69%)	16 (0,62%)
Simpósio Brasileiro de Tecnologia da Informação (SBTI)	114 (100%)	3 (2,63%)	1 (0,88%)	1 (0,88%)	0 (0,0%)
Journal of the Brazilian Computer Society	229 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
ISys: Revista Brasileira de Sistemas de Informação	112 (100%)	1 (0,89%)	1 (0,89%)	1 (0,89%)	1 (0,89%)
Revista de Informática Teórica e Aplicada: RITA	197 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
Revista IEEE América Latina	2.519	9	5	3	3

	(100%)	(0,36%)	(0,20%)	(0,12%)	(0,12%)
Revista de Gestão da Tecnologia e Sistemas de Informação	269 (100%)	8 (2,97%)	3 (1,11%)	3 (1,11%)	0 (0,0%)
Revista de Sistemas e Computação - RSC	110 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
Revista de Tecnologia da Informação e Comunicação	83 (100%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
Revista Eletrônica de Sistemas de Informação (RESI)	140 (100%)	3 (2,14%)	3 (2,14%)	3 (2,14%)	3 (2,14%)
Sistemas de Informação (Macaé) / Revista de Sistemas de Informação da FSMA	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%)**

Quadro 4. Quantitativo de trabalhos resultantes em cada etapa.

O SBSEG contempla, anualmente, um conjunto de workshops da área de segurança, tendo os artigos também publicado em seus anais. Por ser inerente à área foram inseridos. Tendo, inclusive, contribuído com dois artigos para o resultado final do SBSEG.

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 o que aponta que a área pretendida está mais voltada para Sistemas de Informação do que, propriamente, nos eventos que Segurança da Informação. Em termos absolutos, quantitativo, tem-se a grande contribuição do CONTECSI e do SBSI para esta área, sendo os que mais tiveram artigos encontrados, com, respectivamente, 50% e 18,75% dos resultados, novamente eventos de Sistemas de Informação. Destaca-se também, em 2017, a grande contribuição do CONTECSI, com 5 publicações dos 6 encontrados. O Quadro 5 mostra as quantidades de artigos publicados entre 2008 e 2017 nos eventos que se obteve retorno.

	2008	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**TOTAL**
CONTECSI	1		1	1	1	1	3	2	1	5	**16**
SBSEG		1	1					1			**3**
SBSI		1	2			1		2			**6**
IEEE									2	1	**3**
ISys						1					**1**
RESI		1	1			1					**3**
TOTAL	**1**	**3**	**5**	**1**	**1**	**4**	**3**	**5**	**3**	**6**	**32**

Quadro 5. Quantidade de artigos por ano e evento.

Os artigos encontrados seriam classificados nas quatro áreas do escopo da pesquisa: Gestão, Governança e Maturidade da segurança da informação. Com base nos 32 trabalhos selecionados, mais três áreas de pesquisa, dentro da segurança da informação, emergiram, totalizando a classificação em seis temáticas principais: Aspectos Humanos, Gestão, Governança, Maturidade, Política de Segurança da Informação (PSI) e Riscos. Ciente da correlação entre as áreas temáticas encontradas, frequentemente, um artigo trata, diretamente, mais de uma delas. Por conta deste motivo, o Quadro 6 excede o quantitativo dos 32 artigos encontrados.

Área/Ano	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	**TOTAL**
Aspectos Humanos			1			1				1	**3**

Gestão	1	1	3		1	3	1	2	0	2	**14**
Governança		2		1	1		1	2	0	3	**10**
Maturidade			1			1	1			3	**6**
PSI			1			2	1	1		2	**7**
Riscos			1			1	2	1	3		**8**

Quadro 6. Quantidade de artigos por área temática e ano.

Percebe-se um crescimento na quantidade de artigos na área pesquisada nos últimos anos. Onde, tem-se 65,62% (21 artigos) do resultado encontrado nos últimos cinco anos (50% do espaço temporal pesquisado). Todas as áreas temáticas tiveram mais publicações nos últimos cinco anos (2013-2017), mas destaca-se as áreas temáticas de Riscos com 87,50% das publicações nos últimos cinco anos, PSI com 85,71% e Maturidade com 83,33%.

Os trabalhos encontrados estão listados no Quadro 7.

Nº	Evento/ Periódico	Título	Autores e ano
1	CONTECSI	Information Security Policy: A Simplified Model Based on ISO 27002	(Alencar et al., 2017a)
2	CONTECSI	Theoretical Guidelines for an Agile Model of Governance, Management and Maturity for Information Security	(Alencar et al., 2017b)
3	CONTECSI	Um Modelo Para Governança Da Segurança Da Informação Em Empresas De Varejo	(Amorim & Bernardes, 2017)
4	CONTECSI	Strategic Planning Methodology For Information Security – PESEG 1.0	(Menezes et al., 2017)
5	CONTECSI	Segurança Da Informação Nas Corporações: Um Estudo Dos Impactos Do Comportamento Da Média E Alta Gerência	(Moreira & Almeida, 2017)
6	CONTECSI	Gestão De Riscos De Segurança Da Informação E Sua Aplicação Numa Instituição Pública Federal	(Arima, Akabane, Souza, Kussama, & Oliveira, 2016)
7	CONTECSI	Adoption Of Information Security Measures In Public Research Institutes	(Albuquerque Junior & Santos, 2015)
8	CONTECSI	Information Security Framework For Brazilian Small Business	(Freitas, Moraes, Miranda, Santana, & Sousa, 2015)
9	CONTECSI	Gestão De Segurança Da Informação: Estudo De Caso Em Uma Instituição Financeira	(Fernandes, Carpes, & Diel, 2014)
10	CONTECSI	Alinhamento Da Segurança Da Informação Com As Áreas De Negócio: Contribuição Da NBR ISO/IEC 27002:2013	(Fontes, 2014)
11	CONTECSI	Analysis Of Maturity Levels In IT Process Related To Information Systems Security	(Weber, da Silva, Vanti, & Brum, 2014)
12	CONTECSI	Segurança Da Informação Contábil: Procedimentos Para Elaboração De Uma Política De Segurança Com Base Na ISO 27001	(Mattes & Petri, 2013)

		e ISO 27002	
13	CONTECSI	A Picture Of Information Security In Public Institutions Of Scientific Research In Brazil	(Alexandria, 2012)
14	CONTECSI	Strategic Alignment Between Business Goals And Information Security In The Context Of Information Technology (IT) Governance: A Study In The Industrial Automation Sector	(Knorst & Vanti, 2011)
15	CONTECSI	Proposta Para A Estruturação Da Gestão Da Segurança Da Informação Em Um Ambiente De Pesquisa Científica	(Alexandria & Quoniam, 2010)
16	CONTECSI	ITIL Na Gestão Da Segurança Da Informação	(Mendes & Moreira, 2008)
17	SBSEG / WRAC	Uma Iniciativa Para Aprimorar a Gestão de Riscos de Segurança da Informação na Administração Pública Federal	(Bueno et al., 2015)
18	SBSEG / WTICG	Definição de uma Política de Segurança para um Ambiente de Desenvolvimento Distribuído de Software	(Zanichelli & Martimiano, 2010)
19	SBSEG	Uma Metodologia Seis Sigma para Implantação de uma Gestão de Segurança da Informação Centrada na Percepção dos Usuários	(Oliveira, Nunes, & Ellwanger, 2009)
20	SBSI	Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro	(Fazenda & Fagundes, 2015)
21	SBSI	Proposal for Simplified Security Model for Small and Medium Business	(Silva Neto, Alencar, & Queiroz, 2015)
22	SBSI	Insiders: Um Fator Ativo na Segurança da Informação	(Alencar, Queiroz, & Queiroz, 2013)
23	SBSI	Usando Padrões para o Desenvolvimento da Gestão da Segurança de Sistemas de Informação baseado na Norma ISO/IEC 21827:2008	(Kroll, Fontoura, Wagner, & D'Ornellas, 2010)
24	SBSI	Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação	(Mayer & Fagundes, 2010)
25	SBSI	Fatores Organizacionais e sua Influência na Segurança da Informação em Universidades Públicas: Um Estudo Empírico	(Machado, Cabral, Santos, & Motta, 2009)
26	IEEE	Maturity Model of Information Security for Software Developers	(Silva & Barros, 2017)
27	IEEE	DSR Approach to Assessment and Reduction of Information Security Risk in TELCO	(Montenegro, Murillo, Gallegos, & Albuja, 2016)
28	IEEE	Methodology for Dynamic Analysis and Risk Management on ISO27001	(Santos-Olmo, Sánchez, Álvarez, Huerta, & Fernandez-Medina, 2016)
29	iSys	Proposic□ão de uma Ontologia de Apoio à	(Gualberto, Sousa Jr,

		Gestão de Riscos de Seguranc□a da Informac□ão	De Deus, & Duque, 2013)
30	RESI	Modelo De Avaliação Da Maturidade Da Segurança Da Informação	(Rigon & Westphall, 2013)
31	RESI	Proposição De Um Modelo Dinâmico De Gestão De Segurança Da Informação Para Ambientes Industriais	(Roque, Nunes, & Silva, 2010)
32	RESI	Gerenciamento De Segurança Segundo Itil Um Estudo De Caso Em Uma Organização Industrial De Grande Porte	(Breternitz, Navarro Neto, & Navarro, 2009)

Quadro 7. Lista dos artigos resultantes.

Ao analisar os trabalhos encontrados quanto às normas, padrão, modelo, *framework*, documento, metodologia ou teoria utilizado pelos autores para criação de sua metodologia ou execução da pesquisa, percebe-se a predominância da utilização das normas ISO/IEC da família de segurança da informação, família de normas 27000, mais especificamente, as normas ISO/IEC 27002, ISO/IEC 27001 e ISO/IEC 27005 com 15, 10 e 8 utilizações respectivamente.

O Quadro 8 detalha as respectivas quantidades. Ressalta-se que diversos artigos utilizam mais de uma norma, padrão, modelo, framework, documento, metodologia ou teoria, por isso que o somatório apontado no Quadro 8 excede os 32 artigos encontrados na busca. Também é importante colocar que os itens selecionados foram agrupados, contendo todas as suas versões e nas diferentes línguas, por exemplo, ao abordar no quadro ISO/IEC 27002 trata-se do agrupamento de todas suas versões (por exemplo, ISO/IEC 17799:2000, ISO/IEC 27002:2005 e ISO/IEC 27002:2013) bem como suas versões internacionais (por exemplo, ISO/IEC 27.002:2013) e as versões nacionais (por exemplo, ABNT NBR ISO/IEC 27.002:2013).

Quantidade de Artigos	**Norma, Padrão, Modelo, Framework, Documento, Metodologia ou Teoria**
15	ISO/IEC 27002, 17799:2005
10	ISO/IEC 27001
8	ISO/IEC 27005
6	COBIT
3	ITIL
2	Balanced Scorecard
1	ISO/IEC 27014
1	eTOM Level 2
1	ISO/IEC 21827:2008
1	ISO/IEC 27011
1	IT-Grundschutz - BSI 100-2
1	MAGERIT v3.0
1	MGR-SISP
1	NIST 800-30
1	NIST 800-39
1	NIST Cybersecurity Framework
1	PCI-DSS
1	Seis Sigma
7	Não menciona explicitamente /não utiliza

Quadro 8. Arcabouços utilizados nas pesquisas.

Os 32 artigos foram analisados individualmente a fim de identificar a quantidade de autores de cada um deles. Os artigos encontrados tiveram uma média de 2,97 autores por trabalho. Tendo um trabalho com seis autores (máximo encontrado) e dois trabalhos com, apenas, um autor (mínimo encontrado). O resultado está representado no Quadro 9, que mostra que 37,5% dos artigos são assinados por dois autores, sendo esse o maior grupo. Isso pode significar que este grupo de trabalhos sejam resultado de trabalhos de conclusão, dissertações ou teses, que são, por esse motivo, assinados por orientandos e orientadores, mas pode significar, também, que há pouca colaboração em pesquisas sobre o tema, o que precisa ser comprovado por maiores análises.

Quantidade de Autores	**6**	**5**	**4**	**3**	**2**	**1**
Quantidade de Artigos	1	3	6	8	12	2

Quadro 9. Distribuição de autores por artigo.

Ao analisar os autores, verificou-se 83 pesquisadores distintos. Sendo que 10 deles se destacaram por ter mais de uma publicação encontrada, conforme Quadro 10. A afiliação inserida no quadro é referente à última publicação.

Quantidade de Artigos (anos)	**Autor**	**Afiliação**
4 (2013, 2015, 2017 e 2017)	Gliner Dias Alencar	Instituto Brasileiro de Geografia e Estatística (IBGE) e Universidade Federal de Pernambuco (UFPE), PE, Brasil.
2 (2011 e 2014)	Adolfo Alberto Vanti	Universidade do Vale do Rio dos Sinos, RS, Brasil.
2 (2017 e 2017)	Alcides Jeronimo de Almeida Tenorio Junior	Instituto Brasileiro de Geografia e Estatística (IBGE), AL, Brasil.
2 (2013 e 2015)	Anderson Apolonio L. Queiroz	Instituto Federal do Rio Grande do Norte (IFRN), RN, Brasil
2 (2017 e 2017)	Hermano Perrelli de Moura	Universidade Federal de Pernambuco (UFPE), PE, Brasil.
2 (2010 e 2012)	João Carlos Soares de Alexandria	Instituto de Pesquisas Energéticas e Nucleares (IPEN), SP, Brasil.
2 (2010 e 2015)	Leonardo Lemes Fagundes	Universidade do Vale do Rio dos Sinos (Unisinos), RS, Brasil.
2 (2008 e 2017)	Márcio Aurélio Ribeiro Moreira	Faculdades Pitágoras de Uberlândia, MG, Brasil.
2 (2017 e 2017)	Mauro Cesar Bernardes	Centro Universitário Estácio Radial de São Paulo, SP, Brasil.
2 (2009 e 2010)	Raul Ceretta Nunes	Universidade Federal de Santa Maria (UFSM), RS, Brasil.

Quadro 10. Principais autores.

Analisando apenas o primeiro autor de cada artigo, tem-se 29 pesquisadores diferentes nos 32 trabalhos. Neste contexto, destaca-se, por ter mais de uma publicação, os pesquisadores Gliner Dias Alencar, sendo primeiro autor em três trabalhos, e João Carlos Soares de Alexandria, encabeçando duas pesquisas, ambos presentes, no Quadro 10.

Dos 32 artigos, 10 (31,25%) apresentam autores com a citação de afiliação no diferente entre eles, o que pode demonstrar parcerias externas, mas também pode ser um

trabalho isolado, autores com mais de uma afiliação (sendo uma delas em comum, não colocada no artigo), ou, até mesmo, casos de orientador e orientando (e este último inseriu sua vinculação profissional, por exemplo). Este é um ponto que necessita ser analisado com maior detalhamento para averiguação da existência de parcerias externas, o que é um fato bastante salutar para a evolução das pesquisas e deveria ter um maior incentivo. No caminho oposto, foi verificado a maioria dos artigos (68,75%) com autores vinculados à mesma instituição, o que indica que a maioria das pesquisas na área é realizada por grupos sem maiores parcerias e contribuições de pesquisadores externos, sendo a publicação uma das formas de divulgação do trabalho.

Daqueles autores que identificaram a sua afiliação no trabalho (em dois trabalhos os autores não se identificaram), percebe-se a contribuição de pesquisadores de 37 instituições diferentes. As instituições que mais contribuíram (mais do que um trabalho) são apresentadas no Quadro 11.

Instituição	Quantidade de Trabalhos
Universidade Federal de Pernambuco (UFPE), Pernambuco, Brasil	5
Universidade do Vale do Rio dos Sinos (UNISINOS), Rio Grande do Sul, Brasil	3
Universidade Federal de Santa Maria (UFSM), Rio Grande do Sul, Brasil	3
Instituto Brasileiro de Geografia e Estatística (IBGE), Alagoas, Brasil	2
Instituto de Pesquisas Energéticas e Nucleares (IPEN), São Paulo, Brasil	2
Universidad de las Fuerzas Armadas (ESPE), Sangolquí, Ecuador,	2
Universidade Federal de Santa Catarina (UFSC), Santa Catarina, Brasil.	2

Quadro 11. Principais instituições.

No que tange a região de afiliação dos autores, os estados do Rio Grande do Sul (com 6 artigos), Pernambuco (com 5) e São Paulo (também com 5) foram os que se destacaram, representando três regiões distintas (Sul, Nordeste e Sudeste, respectivamente), como pode ser visto no Quadro 12.

Região	Quantidade de Artigos
Rio Grande do Sul, Brasil	6
Pernambuco, Brasil	5
São Paulo, Brasil	5
Santa Catarina, Brasil	3
Alagoas, Brasil	2
Distrito Federal, Brasil	2
Equador	2
Minas Gerais, Brasil	2
Paraná, Brasil	2
Sergipe, Brasil	1
Bahia, Brasil	1
Espanha	1
França	1
Goiás, Brasil	1
Paraíba, Brasil	1
Rio Grande do Norte, Brasil	1

Quadro 12. Distribuição dos artigos por região.

A soma dos artigos produzidos pelas regiões (estados e países), exibidas no Quadro 12 extrapolam os 32 artigos iniciais por se ter artigos com autores de localidades distintas. Com 31% das publicações (11 artigos), tem-se as regiões brasileiras do nordeste e sul (cada). Destaca-se, também, como um fato não esperado pelos autores, 11% das publicações terem autores estrangeiros. Por outro lado, não foi encontrado nenhuma publicação da região norte do Brasil, conforme Gráfico 2.

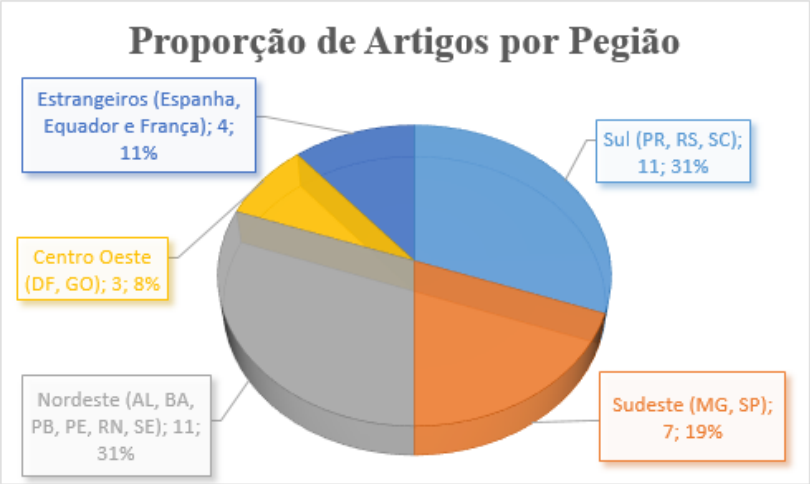

Gráfico 2. Distribuição regional dos artigos.

No que tange as referências utilizadas, averiguou-se que os trabalhos encontrados utilizam, em média, 25,44 referências. Nos extremos tem-se um artigo com 5 referências, sendo o trabalho com menor quantidade de referências, e outro com 73 referências utilizadas no trabalho, sendo a pesquisa com o maior referencial teórico.

As referências foram categorizadas em oito classes:

- Artigos, envolvendo trabalhos em congressos e periódicos;
- Capítulos de livros e livros;
- Leis, normativos (com efeito legal ou oriundos de meios jurídicos, legislativo ou de órgãos de controle), resoluções e legislação em geral;
- Monografias (de graduação e especialização), dissertações de mestrado e teses de doutorado;
- Normas, guias e padrões (envolvendo, principalmente as publicações da ABNT, ISO/IEC, COBIT, ITIL e etc);
- Relatório técnicos e de iniciação científica;
- Revistas não acadêmicas;
- Sites.

O quantitativo de cada categoria é descrito no Quadro 13.

Categorias	Quantidade	Percentual
Artigos (Congressos e Periódicos)	321	39,43%
Capítulos de Livro / Livros	188	23,10%
Sites	111	13,64%
Normas / Guias / Padrões	106	13,02%
Monografias, Dissertações ou Teses	63	7,74%

Relatórios Técnicos ou de Iniciação Científica	16	1,97%
Leis / Normativos / Resoluções / Legislação	8	0,98%
Revista não acadêmica	1	0,12%
TOTAL	**814**	**100,00%**

Quadro 13. Distribuição de referências.

As referências mais antiga utilizada nos trabalhos pesquisados é de 1974, enquanto a mais nova é de 2017. A maior quantidade de referências são de 2012, seguida pelas referências de 2006 e 2008, como pode ser visto no Gráfico 3.

Gráfico 3. Distribuição das referências utilizadas por ano.

Ao se analisar apenas as referências categorizadas como artigos acadêmicos (congressos e periódicos), tem-se destaque, novamente, para o ano de 2012, mas agora seguido por 2008, e, logo após, pelos artigos produzidos em 2006 e 2007 (Gráfico 4).

Gráfico 3. Distribuição dos artigos citados por ano.

Entre os cinco trabalhos mais referenciados, os quatro primeiros encontram-se categorizados como Normas, Guias ou Padrões, sendo eles: a ISO/IEC 27002 com 28 citações; a ISO/IEC 27001, 20 citações; COBIT, 15 vezes mencionado; ISO/IEC 27005, com 9 citações; e, um livro, Gestão da Segurança da Informação: uma visão executiva (Autor: Marcos Sêmola), com 6 citações. Em todos os casos foram considerados todas as versões, edições e linguagens do mesmo trabalho.

Entre os trabalhos acadêmicos (artigos de eventos e congressos) a maioria é referenciado apenas uma vez. Porém, seis trabalhos se destacaram, sendo citado três ou mais vezes. Sendo três publicações em eventos (um evento nacional) e três publicações em periódicos (duas revistas nacionais). No que tange ao primeiro autor de cada trabalho, 3 são brasileiros (Quadro 14).

Citações	Artigo
5	Marciano, J. L., & Marques. M. L. (2006, Dezembro). O Enfoque Social da Segurança da Informação. *Ci. Inf. Brasília*, 35(3), (pp. 89-98).
4	Posthumus, S., & Von Solms, R. (2004). A Framework for the Governance of Information Security. *Computers & Security*, 23(8), (pp. 638-646).
3	Diniz, I. J. D., Medeiros, M. F. M., & Sousa Neto, M. V. (2012). Governanc□a de TI: a visão dos concluintes de Administrac□ão e Cie□ncias da Computac□ão. *Revista Brasileira de Administrac□ão Científica*, 3(2), (pp. 7-24).
3	Karokola, G., Kowalski, S, & Yngström, L. (2011). Towards an information security maturity model for secure e-government services: a stakeholders view. In *International Symposium on Human Aspects of Information Security & Assurance - HAISA*, (pp. 58-73).
3	Park, J. O., Kim, S. G., Choi, B. H., & Jun, M. S. (2008, August). The study on the maturity measurement method of security management for ITSM. In *International Conference on Convergence and Hybrid Information Technology – IEEE ICHIT*, (pp. 826-830).
3	Rigon, E. A., & Westphall, C. M. (2011). Modelo de avaliação da maturidade da segurança da informação. In *Simpósio Brasileiro de Sistemas de Informação - SBSI*, (pp. 93-104).

Quadro 14. Artigos mais citados.

Por fim, o Quadro 15 aponta os eventos e periódicos mais citados. Verificou-se 6 meios nacionais e 7 internacionais, sendo quatro eventos (dois nacionais) e nove periódicos (quatro nacionais).

Evento ou Periódico	Citações
Computers & Security	19
International Conference on Information Systems and Technology Management (CONTECSI)	14
Simpósio Brasileiro de Sistemas de Informação (SBSI)	13
Ci. Inf. Brasília	7
Journal of Information Systems and Technology Management: JISTEM	6
Information Management & Computer Security	6
Revista Eletrônica de Sistemas de Informação (RESI)	5
Revista Brasileira de Administração Científica	5
IEEE Security & Privacy	5

MIS Quarterly	4
ARES - International Conference on Availability, Reliability and Security	4
Information Security Technical Report	4
Hawaii International Conference on System Sciences.	4

Quadro 15. Eventos e periódicos mais citados.

5. CONSIDERAÇÕES FINAIS

É crescente a necessidade e importância da segurança das informações ao considerar, principalmente, os riscos trazidos pela utilização das TICs e a dependência delas para as pessoas e corporações. Fato corroborado no presente trabalho ao apresentar 65,62% dos resultados (21 trabalhos) nos últimos cinco anos (metade do espaço temporal pesquisa), se destacando 2017, último ano pesquisado, como o ano com mais trabalhos, seis (18,75%). Fatos que demonstrando uma tendência de crescimento das pesquisas nesta temática.

A pesquisa abordou a base de dado dos últimos dez anos de quatro eventos e nove periódicos, totalizando a busca em 7.614 artigos. Destacando o baixo percentual de trabalhos na área pesquisada publicados nos eventos e periódicos, visto que, apenas 1,17% (89 trabalhos) das pesquisas publicadas foram selecionados inicialmente, resultando, após todas as etapas de análises, em, apenas, 0,42% (32 artigos) da base original buscada.

Também mostrou-se que as pesquisas são baseadas, principalmente, nas normas ISO/IEC de Segurança da Informação, em especial as normas ISO/IEC 27002, 27001 e 27005. Bem como que esses são os arcabouços mais referenciados, em conjunto com o COBIT e o livro Gestão da Segurança da Informação: uma visão executiva, do autor Marcos Sêmola.

O que pode ser um indicador de que há necessidade de se desenvolver trabalhos científicos baseados em lentes teóricas já existentes e também estabelecer novas teorias que sirvam para nortear a realização de outras pesquisas. Isso é reforçado pela quantidade de livros e sites que figuram entre as referências e, principalmente, por não se ter nenhum artigo entre os trabalhos mais citados.

Verificou-se, também, que a maioria dos artigos (68,75%) tem seus autores vinculados a uma mesma instituição, o que aponta que a maioria das pesquisas na área é realizada por grupos sem maiores parcerias e contribuições de pesquisadores externos. As instituições dos pesquisadores foram distribuídas, principalmente entre as regiões brasileiras do nordeste e sul tendo, cada uma, 31% dos trabalhos e o sudeste com 19% das publicações. Sendo relevante também o aparecimento, em 11% dos casos, de instituições estrangeiras.

O presente trabalho foi norteado pela pergunta de pesquisa: "*Qual o estado atual e a evolução das publicações nos principais eventos e periódicos nacionais da área de computação com relação ao tema de segurança da informação, mais especificamente nas áreas de Governança, Gestão e Maturidade da Segurança da Informação?"* e pelo objetivo de "*analisar as publicações nos principais eventos e periódicos nacionais da área de computação com relação ao tema de segurança da informação, nos últimos 10 anos, que tratem a área de Governança, Gestão e Maturidade da Segurança da Informação*". Pelo método utilizado, detalhado na seção 3, resultados exibidos na seção 4 e suas considerações finais na presente seção, acredita-se que tenha-se atingido o objetivo proposto e, consequentemente, respondido satisfatoriamente a pergunta de pesquisa.

Este trabalho tem como limitação o fato de considerar apenas um conjunto de eventos e periódicos, que, apesar dos selecionados estarem, a princípio, entre os mais

relevantes para a área, não se pode excluir a importância dos demais não pesquisados. Outra limitação é o espaço de tempo (últimos 10 anos), visto que existem eventos e periódicos, mesmo dentro dos selecionados, com publicações anteriores ao escopo temporal desta pesquisa. Por fim, outra restrição é referente ao método selecionado, que utiliza um conjunto de palavras para a busca o que, por mais ampla e completa que seja, corre-se o risco de não incluir alguma pesquisa relevante.

Por fim, como forma de sanar as limitações do presente trabalho, bem como contribuir para a área de pesquisa, acredita-se ser relevante e consequentemente podem gerar trabalhos futuro a continuação da análise para os artigos produzidos a partir de 2017; analisar outros periódicos e eventos (da área de computação ou não); correlacionar outros temas na área de segurança da informação; investigar, mais detalhadamente, se os artigos são oriundos de trabalhos de conclusão de graduação mestrado ou doutorado; se existe, como funciona e como melhorar os grupos de pesquisas e sua ligação com pesquisadores externos e meio corporativo; entre outros temas.

REFERÊNCIAS

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

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

Albuquerque Junior, A. E., & Santos, E. M. dos. (2013). Produção Científica sobre Segurança da Informação em Anais de Eventos da ANPAD. In *IV Encontro de Administração da Informação - EnADI / ANPAD* (pp. 1–16).

Albuquerque Junior, A. E., & Santos, E. M. dos. (2014a). Análise das Publicações Brasileiras sobre Segurança da Informação sob a Ótica Social em Periódicos Científicos entre 2004 e 2013. In *XXXVIII Encontro da ANPAD* (pp. 1–16). Rio de Janeiro - RJ, Brasil.

Albuquerque Junior, A. E. de, & Santos, E. M. dos. (2014b). Scientific Production about Information Security on Brazilian Scientific Conferences. In *11th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI* (pp. 2085–2103). TECSI. https://doi.org/10.5748/9788599693100-11CONTECSI/PS-794

Albuquerque Junior, A. E. de, & 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* (Vol. 12). Retrieved from http://www.contecsi.fea.usp.br/envio/index.php/contecsi/12CONTECSI/paper/view/3155

Alencar, G. D., Queiroz, A. A. L., & Queiroz, R. J. G. B. (2013). Insiders: Um Fator Ativo na Segurança da Informação. In *IX Simpósio Brasileiro de Sistemas de Informação - SBSI* (pp. 61–72).

Alencar, G. D., Tenorio Junior, A. J. de A., & Moura, H. P. (2017a). Information Security Policy: A Simplified Model Based on ISO 27002. In *14th International Conference on Information Systems & Technology Management - CONTECSI* (pp. 4135–4156). https://doi.org/10.5748/9788599693131-14CONTECSI/PS-4859

Alencar, G. D., Tenorio Junior, A. J. de A., & 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* (pp. 3661–3690). https://doi.org/10.5748/9788599693131-14CONTECSI/PS-4799

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* (pp. 4209–4215).

Alexandria, J. C. S. de, & 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* (pp. 2175–2197).

Amorim, E. S. de, & Bernardes, M. C. (2017). A Model for Information Security Governance in Retail Enterprises. In *14th International Conference on Information Systems & Technology Management - CONTECSI* (pp. 1062–1092). https://doi.org/10.5748/9788599693131-14CONTECSI/PS-4541

Arima, C. H., Akabane, G., Souza, J. G. S., Kussama, L., & 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* (pp. 730–743). https://doi.org/10.5748/9788599693124-13CONTECSI/PS-3757

Berners-Lee, T. (1996). WWW: past, present, and future. *Computer*, *29*(10), 69–77. https://doi.org/10.1109/2.539724

Breternitz, V. J., Navarro Neto, F., & Navarro, A. F. (2009). Gerenciamento de Segurança Segundo ITIL: Um Estudo de Caso em uma Organização Industrial de Grande Porte. *Revista Eletrônica de Sistemas de Informação*, *8*(2), 4. https://doi.org/10.5329/RESI.2009.0802004

Bueno, P. M. S., Ikuno, F. S., Araújo, A. S. De, Lima, J. N. de O., Moreira, J. R. M., & Melo, L. A. V. de. (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* (pp. 495–500).

Castells, M. (2009). *A Sociedade em Rede* (10ª). Paz e Terra.

Fazenda, R. V., & 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* (pp. 307–314).

Fernandes, F. C., Carpes, A. M. da S., & 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* (pp. 441–456). https://doi.org/10.5748/9788599693100-11CONTECSI/PS-542

Fontes, E. L. G. (2006). *Segurança da Informação - O Usuário Faz a Diferença* (1ª). Saraiva.

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* (pp. 1519–1530). https://doi.org/10.5748/9788599693100-11CONTECSI/PS-714

Freitas, R. B. de, Moraes, I. M. P. de, Miranda, F. P., Santana, A. C., & 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*. Retrieved from http://www.contecsi.fea.usp.br/envio/index.php/contecsi/12CONTECSI/paper/view/2326

Gomes, L. D., Goulart Júnior, C. R., Simeão, J. L. C., de Sousa, T. de J. R., & Santana, A. C. (2016). Best Practices in Governance of Information and Tecnology Management. In *13th International Conference on Information Systems & Technology Management - CONTECSI* (pp. 837–857). https://doi.org/10.5748/9788599693124-13CONTECSI/PS-3781

Gualberto, E. S., Sousa Jr, R. T. De, De Deus, F. E. G., & 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*, *6*(1), 30–43.

Joia, L. A., & Cavalcante Neto, A. A. (2004). Government-To-Government Enterprises In Brazil: Key Success Factors Drawn From Two Case Studies. In *17th Bled eCommerce Conference eGlobal* (pp. 1–13). Bled, Slovenia. Retrieved from https://pdfs.semanticscholar.org/422a/fed01b6ff30ad36caa1e7f4be7860c1c5be3.pdf

Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. *Proceedings of the 5th HAISA2011 Conference*, (58–73), 12. https://doi.org/urn:nbn:se:su:diva-67206

Kitchenham, B., & Charters, S. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. *EBSE Technical Report*. Durham, UK. Retrieved from https://pdfs.semanticscholar.org/e62d/bbbbe70cabcde3335765009e94ed2b9883d5.pdf

Knorst, A. M., & 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* (pp. 3710–3730). Retrieved from http://www.contecsi.fea.usp.br/envio/index.php/contecsi/8contecsi/paper/view/3299

Kroll, J., Fontoura, L. M., Wagner, R., & 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., & 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* (pp. 97–108).

Manoel, S. da S. (2014). *Governança de Segurança da Informação: como criar oportunidades para o seu negócio* (1ª). Rio de Janeiro - RJ, Brasil: Brasport.

Marciano, J. L., & Lima-Marques, M. (2006). O enfoque social da segurança da informação. *Ciência Da Informação*, *35*(3), 89–98. https://doi.org/10.1590/S0100-19652006000300009

Mattes, I. V., & 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 (pp. 90–110).

Mayer, J., & 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., & Moreira, M. A. R. (2008). Itil on Security Information Management. In *5th CONTECSI International Conference on Information Systems and Technology Management - CONTECSI* (pp. 3009–3029).

Menezes, B. P., Rocha, F. G., Menezes, P. M., & Nascimento, R. P. C. (2017). Strategic Planning Methodology for Information Security – PESEG 1.0. In *14th International Conference on Information Systems & Technology Management - CONTECSI* (pp. 303–330). https://doi.org/10.5748/9788599693131-14CONTECSI/PS-4454

Montenegro, C., Murillo, M., Gallegos, F., & Albuja, J. (2016). DSR Approach to Assessment and Reduction of Information Security Risk in TELCO. *IEEE Latin America Transactions*, *14*(5), 2402–2410. https://doi.org/10.1109/TLA.2016.7530438

Moreira, M. A. R., & 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* (pp. 1645–1661). https://doi.org/10.5748/9788599693131-14CONTECSI/PS-4591

Oliveira, M. A. F., Nunes, R. C., & 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* (pp. 173–186).

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic Mapping Studies in Software Engineering. In *12th International Conference on Evaluation and Assessment in Software Engineering - EASE* (pp. 68–77). Italy. Retrieved from https://www.researchgate.net/profile/Michael_Mattsson/publication/228350426_Systematic_Mapping_Studies_in_Software_Engineering/links/54d0a8e90cf20323c218713d/Systematic-Mapping-Studies-in-Software-Engineering.pdf

Rigon, E. A., & Westphall, C. M. (2013). Modelo de Avaliação da Maturidade da Segurança da Informação. *Revista Eletrônica de Sistemas de Informaçao*, *v. 12*(1), 3. https://doi.org/10.5329/RESI.2012.1101003

Rigon, E. A., Westphall, C. M., Dos Santos, D. R., & Westphall, C. B. (2014). A Cyclical Evaluation Model of Information Security Maturity. *Information Management & Computer Security*, *22*(3), 265–278. https://doi.org/10.1108/IMCS-04-2013-0025

Roque, A. dos S., Nunes, R. C., & Silva, A. D. (2010). Proposition of a Dynamic Model for Managing Security Information on Industrial Environments. *Revista Eletrônica de Sistemas de Informação*, *9*(2), 7. https://doi.org/10.5329/RESI.2010.0902007

Santos-Olmo, A., Sánchez, L. E., Álvarez, E., Huerta, M., & Fernandez-Medina, E. (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, *14*(6), 2897–2911. https://doi.org/10.1109/TLA.2016.7555273

Silva, M. P., & Barros, R. M. (2017). Maturity Model of Information Security for Software Developers. *IEEE Latin America Transactions*, *15*(10), 1994–1999. https://doi.org/10.1109/TLA.2017.8071246

Silva, D. R. P. da, & Stein, L. M. (2007). Segurança da informação: uma reflexão sobre o

componente humano. *Ciências & Cognição*, *10*, 46–53. Retrieved from http://www.cienciasecognicao.org/pdf/v10/m346130.pdf

Silva Neto, G. M., Alencar, G. D., & Queiroz, A. A. L. (2015). Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In *XI Brazillian Symposium on Information Systems - SBSI* (pp. 299–306).

Thomas, M. (2015). The Core COBIT Publications: A Quick Glance. Retrieved January 20, 2018, from http://www.isaca.org/COBIT/focus/Pages/the-core-cobit-publications-a-quick-glance.aspx

Weber, E. L., da Silva, M. H., Vanti, A. A., & 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* (pp. 1877–1890). https://doi.org/10.5748/9788599693100-11CONTECSI/PS-758

Zanichelli, A. de S., & 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* (pp. 11–20).