Revista Gestão & Tecnologia
e-ISSN: 2177-6652
revistagt@fpl.edu.br
http://revistagt.fpl.edu.br/

Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições Federais do Ensino Superior

Orlivaldo Kléber Lima Rios
Mestre em Ciência da Computação na Universidade Federal de Pernambuco, Pernambuco, Brasil
okleberios@gmail.com

Vânia Patrícia da Silva Rios
Licencianda em Ciência da Computação, Instituto Federal de Educação, Ciência e Tecnologia Baiano – Campus Sr. do Bonfim, Pernambuco, Brasil
vanipaty@yahoo.com.br

José Gilson de Almeida Teixeira Filho
Professor, Doutor em Ciência da Computação na Universidade Federal de Pernambuco, Pernambuco, Brasil
gilson.teixeira@ufpe.br

Editor Científico: José Edson Lara
Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em 19.10.2016
Aprovado em 16.03.2017

Resumo

Manter a segurança das informações das Instituições Federais do Ensino Superior é um fator preponderante para se alcançar os objetivos do planejamento estratégico institucional. Entretanto, tal segurança deve ser mantida através de ações que possibilitem a confiabilidade, a autenticidade, a integridade e a disponibilidade das informações, tendo seu início com a implantação da política de segurança da informação. O objetivo principal do estudo consistiu em definir as melhores práticas em gestão de segurança da informação para implantação e revisão de PoSIC. A pesquisa utilizou-se de dados documentais e da revisão sistemática da literatura para a produção de um Guia de melhores práticas para Implantação de PoSIC nas Intituições Federais do Ensino Superior - IFES. Após sua elaboração, o Guia foi avaliado, utilizando-se o Modelo de Aceitação de Tecnologia, o qual sugere que fatores como a facilidade de uso percebida e a utilidade percebida influenciam na intenção de uso de um novo sistema ou abordagem teórica e metodológica. Gestores de segurança da informação acreditam que esse documento pode ser utilizado nas instituições de ensino como forma de agregar valor no processo de implantação da política de segurança da informação.

Palavras-Chave: Gestão de Segurança da Informação; Política de Segurança da Informação; Melhores Práticas.

Best practices of COBIT, ITiL and ISO / IEC 27002 for implementation of information security policy in federal Institutions of Higher Education

Abstract

Maintaining the security of information in Federal Institutions of Higher Education is an important factor to achieve the objectives of the institutional strategic planning. However, this security should be kept through actions which will make possible to offer reliability, authenticity, integrity and availability of information, having its starting process through the implantation of information security policy. The main purpose of this study has been to define the best practices for implantation and review of information security policy. The research used documentary data and systematic review of literature to produce a Guide of best practices to the implantation of information security policy in the Federal Institutions of Higher Education - IFES. After its elaboration, the Guide was evaluated using the Model for Technology Acceptance, which suggests that both factors such as perceived easiness of use and perceive utility will influence in the intention of using either a new system or theoretical and methodological approach. Managers of information security believe that this document may be used in educational institutions as a way to add value in the process of implantation of information security policy.

Keywords: Security Information Management; Security Information Policy; Best Practices.

Mejores prácticas del COBIT, ITiL e ISO / IEC 27002 para la implantación de la política de seguridad de la información en las Instituciones Federales de Educación Superior

Resumen

El mantenimiento de la seguridad de la información de las Instituciones Federales de Educación Superior es un factor clave para alcanzar los objetivos de la planificación estratégica institucional. Sin embargo, dicha garantía debe mantenerse a través de acciones que permitan a la fiabilidad, autenticidad, integridad y disponibilidad de la información, y su comienzo con la puesta en práctica de la política de seguridad de la información. El objetivo principal del estudio fue definir las mejores prácticas en la información de gestión de la seguridad para el despliegue y revisión Posit. Los datos de la investigación utilizado documental y revisión sistemática de la literatura para la elaboración de una guía de mejores prácticas para Posit Aplicación de las intitutions Federales de Educación Superior - IFES. Después de su preparación, la guía se evaluó utilizando la tecnología de Modelo de Aceptación, lo que sugiere que los factores tales como la facilidad de uso y utilidad percibida percibidos influencia el uso previsto de un nuevo sistema o enfoque teórico y metodológico. Gestores de seguridad de la información creen que este documento puede ser utilizado en las instituciones educativas como una manera de agregar valor en el proceso de implementación de la política de seguridad de la información.

Palabras clave: Gestión de la Información de Seguridad; Información Política de Seguridad; Mejores practicas.

1 Introdução

Proteger informações, em organizações de qualquer segmento, é um desafio que requer de seus gestores alguns procedimentos, estratégias e diretrizes que devem ser seguidos para a sua sobrevivência (Tuyikeze & Flowerday, 2014). Nesse cenário, surge a importância de uma política de segurança da informação (PoSIC) que forneça diretrizes, critérios e normas que representem os princípios básicos de segurança da informação e do funcionamento de uma organização. Entende-se por PoSIC, o documento que estabelece quais medidas de segurança da informação uma organização deve proceder para proteger seus bens, quer sejam valores em *hardware*, *software* ou pessoais (Editora ABNT, 2013b).

O governo federal brasileiro promove ações de segurança da informação nos órgãos da Administração Pública Federal (APF), no intuito de estabelecer o compromisso com a proteção das informações, na tentativa de manter sua

disponibilidade, integridade, confiabilidade e autenticidade. Para isso, as ações que norteiam tais práticas precisam ser documentadas por meio de diretrizes que assegurem os objetivos das organizações. Um dos documentos que promove a existência de ações de segurança nos órgãos da APF é a Norma Complementar 03/IN01/DSIC/GSIPR (Presidência da República, 2009) e tem o objetivo de estabelecer diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da PoSIC nos órgãos e entidades da APF, direta e indireta.

Entretanto, mesmo com ações do governo federal que promovam a implantação de PoSIC, algumas Instituições Federais do Ensino Superior (IFES) ainda não disponibilizam desse documento em caráter institucionalizado (Brasil, 2016). Tal informação é exposta pelo Levantamento de Governança de TI, realizada pela Secretaria de Fiscalização de Tecnologia da Informação (Tribunal de Contas da União [TCU], 2015). Segundo TCU (2016), 98 IFES participaram daquele levantamento (TCU, 2015), porém, apenas 47 instituições declararam ter a PoSIC em suas instituições (ver Figura 1). Daquelas, apenas 34 instituições (35%) declararam utilizá-la de forma integral, outras 13 instituições (13%) ainda estão em fase de finalização ou seguem a PoSIC parcialmente. Outras 51 instituições (52%) declararam que ainda não dispõe de uma PoSIC.

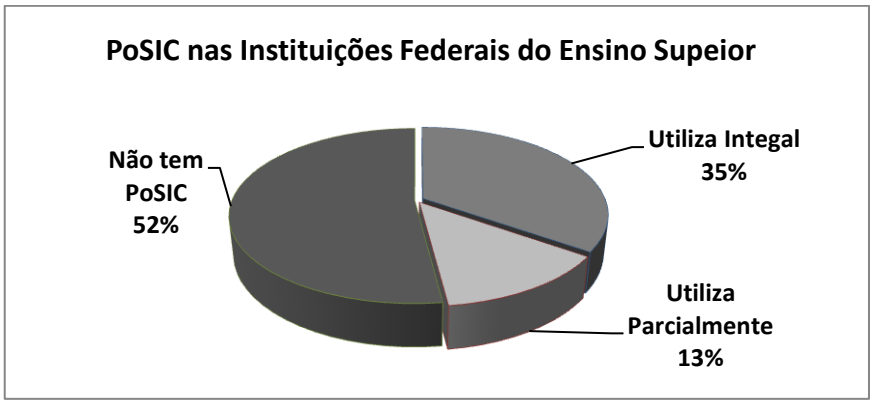

Figura 1
Uso da PoSIC nas IFES.
Fonte: BRASIL. Demanda TCU nº 265-54 [mensagem pessoal]. Mensagem recebida por no-replay@tcu.gov.br em 30 maio de 2016.

Considerando que há recomendações e orientações do governo federal para a institucionalização de uma PoSIC em todos os órgãos da APF, direta e indireta, compreendeu-se a necessidade de identificar as melhores práticas em gestão de segurança da informação para elaboração e implantação de uma PoSIC nas IFES,

considerando que tais instituições estão inseridas nesse panorama de fiscalização do TCU. Nesse cenário, surge o seguinte problema a ser pesquisado: Quais são as práticas em Gestão de Segurança da Informação utilizadas por IFES para implantação de PoSIC? Em resposta a tal questionamento, essa pesquisa teve como objetivo geral a definição de um Guia de melhores práticas para implantação de PoSIC em Instituições Federais do Ensino Superior.

2 Referencial Teórico

2.1 Política de Segurança da Informação

Em segurança da informação, a definição de uma política deve ser estruturada a partir do entendimento da missão da organização, atendendo aos requisitos legais e normativos que regem a mesma (Monteiro, 2009). Consiste em conjuntos de declarações de alto nível das crenças das organizações (Sengupta, Mazumdar & Bagchi, 2011), “compreendendo políticas, diretrizes, normas, procedimentos e memorandos que contribuem coletivamente para a proteção dos ativos da organização” (Tuyikeze & Flowerday, 2014, p. 12). Esta fornece à direção uma intenção da administração para a proteção das informações na organização (Veiga, 2015) e especifica o que fazer ou não, em uma determinada instituição (Sengupta et al., 2011). Entretanto, a PoSIC deverá ser um documento simples e de fácil entendimento, pois deverá ser lida por todos na organização.

2.1.1 PoSIC na Administração Pública Federal

O Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança da Informação da presidência da república (DSIC/GSIPR), adota o termo Política de Segurança da Informação e Comunicações por compreender que uma PoSIC é mais do que somente tecnologia, ou seja, abrange pessoas, o meio no qual trafegam as informações, os recursos tecnológicos, a infraestrutura da segurança da informação, entre outros. Cardoso (2011) relata que, em se tratando de uma instituição da APF, o uso da PoSIC se justifica na própria Constituição federal, artigo 37, *caput*, que vincula a administração pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Considerando o atendimento

de tais princípios, a própria Constituição institui o uso de PoSIC nos órgãos e entidades da APF (Decreto nº 3.505, 2000).

Assim, o governo brasileiro tem demonstrado sua preocupação com a segurança da informação na APF por meio de diferentes instrumentos normativos. Fato é que a Lei 8.159 (1991) afirma que: é dever do poder público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação.

O governo federal brasileiro, preocupado em manter a propriedade intelectual e a segurança da informação das organizações e instituições vinculadas aos órgãos da APF, estabeleceu em 13 de junho de 2000, o Decreto .5305 (2000) com a finalidade de instituir a política de segurança da informação nos órgãos e nas entidades da APF. Dessa forma, o TCU, mediante o Acórdão 2471/2008-TCU-Plenário, recomendou ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR, que orientasse os órgãos e entidades da APF sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que tenham como um dos objetivos estabelecer e/ou aperfeiçoar a política de segurança da informação.

Assim, no intuito de atingir esses objetivos nos órgãos e entidades da APF, o GSI/PR, por meio da Norma Complementar nº 03/IN01/DSIC/GSIPR, estabelece diretrizes, critérios e procedimentos para a elaboração, institucionalização, divulgação e atualização da PoSIC nos órgãos e entidades da APF (Araujo, 2012). Essa Norma Complementar relata que “as diretrizes constantes na política de segurança da informação e comunicações no âmbito do órgão ou entidade visam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação” (Al-Hamdani & Dixie, 2009; Presidência da República, 2009, p. 2).

2.2 Melhores Práticas

Qualquer que seja a organização, é necessário cumprir com as melhores práticas, detalhadas nos padrões de segurança da informação, implementando ações e técnicas aceitas e reconhecidas no cenário internacional (Sengupta et al.,

2011). Tais práticas procuram mesclar as ações de governança e gestão eficiente e eficaz de TI da organização em uma abordagem holística, levando em conta seus diversos componentes interligados (Editora ISACA, 2012b).

As melhores práticas de gestão em segurança da informação exigem que todas as políticas que fazem parte de um quadro político global, proporcionem uma estrutura hierárquica para que as demais políticas se encaixem e façam claramente a ligação aos princípios subjacentes da organização (Editora ISACA, 2012a)

2.2.1 ISO/IEC 27002:2013

A família da norma ISO/IEC 27000 é um conjunto de normas para regular os aspectos da segurança da informação, podendo ser aplicadas em qualquer organização. Nessa família, existe a NBR ISO/IEC 27002, podendo ser considerada como um ponto de partida para o desenvolvimento de diretrizes e princípios gerais sobre metas geralmente aceitas para a gestão da segurança da informação (Monteiro, 2009).

A NBR ISO/IEC 27002 tem como objetivo “fornecer diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização” (Editora ABNT, 2013a, p. 1).

A Norma é estruturada com 14 seções de controles de segurança da informação de um total de 35 objetivos de controles e 114 controles. Cada seção, definindo os controles de segurança da informação, contém um ou mais objetivos de controle. “A ordem em que se encontram as seções não implica nem significa o seu grau de importância” (Editora ABNT, 2013a, p. 1).

Conforme consta no documento ABNT NBR ISO/IEC 27002:2013, a Norma fornece códigos de boas práticas para a gestão de segurança. Está organizada em capítulos de 0 a 18; os capítulos de 0 a 4 apresentam os temas de introdução da Norma e a partir do capítulo 5, orienta-se a criação de normas mais específicas e procedimentos para o tratamento seguro das informações e de outros ativos organizacionais que processam ou armazenam informações.

Uma das seções que trata das práticas para elaboração da PoSIC é a sessão 5 – *Política de Segurança da Informação* – e tem como objetivo “prover orientação

da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes" (Coelho, 2014, p. 20). Convém que um conjunto de políticas de segurança da informação sejam definidos e aprovados pela direção, publicados e comunicados para todos os funcionários e partes externas relevantes (Editora ABNT, 2013a).

2.2.2 ITIL v3

O *Information Technology Infrastructure Library (ITIL)* é uma biblioteca de melhores práticas para o gerenciamento de serviços de Tecnologia da Informação. Sua estrutura é reconhecida, internacionalmente, como o padrão de boas práticas para gerir os serviços de TI de uma organização (Gehrmann, 2015). Por se tratar de uma biblioteca que contém um conjunto de diretivas e melhores práticas, o ITIL descreve todos os processos necessários para promover o suporte adequado à utilização e ao gerenciamento de TI em diversas áreas.

Segundo Taylor (2011), o gerenciamento dos serviços de TI é contemplado pelo ITIL em cinco publicações principais que descrevem os princípios fundamentais do gerenciamento de serviços de TI e fornecem uma visão de alto nível, cada uma possuindo um conjunto de funções (Fontes, 2012), a saber: *Service Strategy* (Estratégia de Serviços), *Service Design* (Desenho de Serviços), *Service Transition* (Transição de serviços), *Service Operation* (Operação de serviços) e *Continual Service Improvement* (Melhoria contínua de serviço). A segurança da informação aparece no ITIL como uma função do *Service Design* e a PoSIC aparece como um elemento importante na função de Gerenciamento de Segurança da Informação.

O documento do *Service Design* trata e detalha a PoSIC como uma atividade de grande importância na gestão de segurança da informação. Entretanto, quando estabelecido que a segurança da informação deva ser orientada e acompanhada por uma PoSIC, Fontes (2012) e Taylor (2011) dizem que o próprio ITIL em relação à produção, análise e revisão de uma política global de segurança da informação deve ser apoiada pela existência de outras políticas específicas, abrangendo todas as áreas de segurança e satisfazendo às necessidades do negócio.

A política de segurança da informação aparece no ITIL como um elemento de suma importância na função de gerenciamento da segurança da informação, assegurando que os aspectos de segurança, no que diz respeito aos serviços e

todas as atividades de gerenciamento dos serviços, sejam adequadamente geridos e controlados de acordo com as necessidades do negócio e dos riscos.

2.2.3 COBIT 5

O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI (Editora ISACA, 2012c), mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e o uso de recursos (Editora ISACA, 2012b). Entretanto, o COBIT não define como os processos serão executados, mas possibilita controles básicos para que a Tecnologia da Informação alcance seus objetivos alinhados aos objetivos de negócio da organização (Gehrmann, 2012).

Para integração da governança corporativa de TI com toda a organização, o COBIT 5 utiliza um conjunto de guias, ou publicações, que fornecem uma série de informações, orientações e práticas detalhadas para aplicação das atividades de gestão de TI. Um desses guias é o *COBIT 5 for Information Security*, destinado para profissionais de segurança da informação ou demais partes interessadas (Editora ISACA, 2012b), reunido em seu conjunto de publicações os conhecimentos relacionados à segurança da informação e os controles relacionados à elaboração de PoSIC.

Entre o conjunto de habilitadores para apoiar a implementação de uma governança e gestão corporativa de segurança da informação, o habilitador *Princípios, políticas e frameworks* descreve os veículos utilizados pela gestão para traduzir o comportamento desejado dos funcionários da organização, tanto para com a segurança da informação quanto às orientações formais, porém práticas, relacionadas às atividades desenvolvidas no dia-a-dia. Em um desses veículos está a utilização da PoSIC, com o propósito de ajudar a organização a articular adequadamente o comportamento desejado, reduzir riscos e contribuir para atingir os objetivos (Carrillo, 2013).

O COBIT 5 *for information security* norteia os profissionais da área de segurança da informação e usuários da PoSIC sobre a maneira de se buscar

orientações por meio de uma politica disponível em uma organização (Editora ISACA, 2012b).

Todo o conjunto de política (diretrizes, normas, procedimentos e princípios) devem proporcionar orientações táticas sobre uma determinada área, fornecendo instruções técnicas de como proceder com a segurança da informação.

O uso do COBIT nas práticas de gestão de segurança da informação possibilitará às IFES identificar suas PoSIC relevantes e necessárias, bem como seguir as recomendações para sua elaboração e implantação.

2.2.4 Relação de práticas da PoSIC

Organizações atuais precisam cumprir com as melhores práticas, detalhados nos padrões de segurança da informação (Sengupta et al., 2011), implementando ações e técnicas aceitas e reconhecidas no cenário internacional, na tentativa de mesclar as ações e práticas de governança e gestão eficiente e eficaz de TI da organização, requerendo uma abordagem holística, levando em conta seus diversos componentes interligados (Editora ISACA, 2012b).

A Tabela 1 apresenta algumas das práticas recomendadas pelo COBIT 5 *for Information Security*, ITIL v3 e ISO/IEC 27002:2013 para a implantação de PoSIC.

Tabela 1
Quadro comparativo das melhores práticas para PoSIC

N.	Prática	COBIT 5	ITL v3	ISO 27002
01	Deve ter o apoio da Alta Gestão	x	x	x
02	Deve ser clara e objetiva	x	x	x
03	Deve estear alinhada com os objetivos da organização	x		x
04	Deve abranger todas as áreas da segurança da informação		x	x
05	Deve realizar análise de riscos antes da implementação	x		x
06	Deve estar em conformidade com a legislação da organização	x	x	x
07	Deve referenciar Leis e regulamentos federais		x	x
08	Deve indicar atribuições e responsabilidades de seus participantes	x	x	x
09	Deve ser apoiada por outras políticas da organização	x	x	x
10	Deve fazer parte de uma política maior da organização	x	x	x
11	Pode ser elaborada em um único documento	x	x	x
12	Deve definir meios para tratamento de exceções	x		
13	Pode ser desmembrada em diretrizes, normas e procedimentos	x	x	x
14	Deve ser analisada criticamente em intervalos planejados	x	x	x
15	Deve ser revisada periodicamente	x	x	x
16	Deve ser desenvolvida em conformidade com o SGSI	x	x	x
17	Deve ser elaborada com um plano de capacitação dos usuários		x	x
18	Deve obter a aprovação da direção para ser revisada	x	x	x

19	O Gestor de segurança da informação deve ser o responsável pelo ciclo de vida da PoSIC	x	x	x
20	Deve ser desenvolvida pelo Comitê de Segurança Informação	x	x	x
21	Deve ter a participação da área jurídica da organização	x		x
22	Sugere-se um plano de orçamento o ciclo de vida	x	x	
23	Sugere-se um catálogo de serviços a ser protegido		x	
24	Deve criar o Termo de Responsabilidade do usuário			x
25	Deve ter um Termo de Aprovação da Alta Direção			x
26	Deve apresentar itens de segurança em Recursos Humanos	x		x
27	Deve ser fiscalizada em intervalos planejados	x		x
28	Deve estabelecer uma fiscalização de conformidade	x		x
29	Deve identificar a validade (período) de aplicação	x	x	x
30	Precisa ser gerenciada durante todo seu ciclo de vida	x	x	x
31	Deve garantir a operação dos recursos e processamento da informação			x
32	Deve descrever as consequências do não cumprimento da PoSIC	x	x	x
33	Deve ser comunicada para todos os funcionários e partes externas	x	x	x
34	Deve ser identificada a área de abrangência	x	x	x
35	Deve ser referenciada em todas as SLR, SLA, contratos e acordos		x	
36	Deve estar amplamente disponível para todos os clientes e usuários	x	x	x
37	Deve ser aprovada pela Alta Direção	x	x	x

Fonte: Estudos identificados na revisão sistemática – elaborada pelos autores (2016).

Todas as práticas identificadas na Tabela 4 foram utilizadas e distribuídas na produção do Guia de melhores práticas para implantação de PoSIC, de acordo com as etapas, as ações e o ciclo de sua implementação, o que permitiu a integralidade e o alinhamento da produção do Guia.

3 Metodologia

A definição do instrumento metodológico em uma pesquisa está diretamente relacionada com o problema a ser estudado. Para Kauark, Manhaes e Medeiros (2010, p. 53), “a metodologia é a explicação minuciosa, detalhada, rigorosa e exata de toda ação desenvolvida no método (caminho) do trabalho de pesquisa”. Adotar uma metodologia significa escolher um caminho, um percurso global a ser percorrido.

A realização desse estudo seguiu uma abordagem qualitativa, pois através de informações adquiridas por meio dos procedimentos da revisão sistemática e de um levantamento documental (Lei No 8.159, 1991; Decreto nº 3.505, 2000; Presidência da República, 2009; Tribunal de Contas da União, 2015 e 2016) tronou-se possível a produção do Guia de melhores práticas para implantação de PoSIC nas IFES, oferecendo ações práticas cujas informações disponíveis ainda são pouco exploradas nessas instituições.

No estudo da revisão sistemática, foi feito um levantamento de referências e

evidências relacionadas a uma estratégia de intervenção específica, mediante a aplicação de métodos explícitos e sistematizados de busca, apreciação crítica e síntese da informação selecionada (Teixeira Filho, 2010). Essa pesquisa se caracterizou por buscar os dados ou as categorias teóricas já trabalhadas por outros pesquisadores devidamente registrados, investigando evidências em estudos científicos relacionados às práticas para implantar PoSIC. A revisão foi conduzida por 03 (três) fases preestabelecidas, seguindo as orientações de Biolchini, Mian, Natali e Travassos (2005): Planejamento, Execução e Análise/Divulgação dos resultados.

A busca por estudos foi realizada de forma eletrônica, entre os anos de 2010 e 2015, através de mecanismos de busca de sites web especializados e de renome científico-acadêmico, tais como ACM, IEEE Xplore, Science Direct, Google Scholar e Scopus. Foram utilizadas as seguintes *strings* de buscas nas fontes já mencionadas*: Information Security Management OR information security policy OR management risk security information; information security polity; COBIT OR ITIL OR ISO/IEC 27002; best practice.* O resultado da busca retornou um quantitativo de 1.420 resultados, sendo conduzidos a filtragem em 5 etapas de seleção:

Etapa 1 – realizar a pesquisa de acordo com as *strings* de busca;

Etapa 2 – seleção dos estudos por relevância do título;

Etapa 3 – leitura de *abstract* e seleção dos artigos por relevância;

Etapa 4 – leitura da introdução, conclusão e seleção dos artigos relevantes;

Etapa 5 – leitura completa dos estudos considerados aptos e fichamento em formulário de estudos aprovados em consonância com a questão de pesquisa inicial.

Para o desenvolvimento e execução da revisão sistemática, todas as atividades de seleção e leitura foram compreendidas entre o período de 17/12/2015 à 26/02/2016. Todos os estudos foram identificados, coletados e organizados em uma lista estruturada, passando por revisões, a cada etapa, para a certificação de que os estudos relevantes não foram eliminados ou passados despercebidos pelos pesquisadores. Concluindo essa fase, as informações foram extraídas somente dos estudos selecionados.

Ao término da revisão sistemática, apenas 15 estudos apresentaram relevância quanto às melhores práticas de gestão de segurança da informação para implantação de PoSIC.

4 Apresentação dos Resultados

Os resultados obtidos com a pesquisa permitiram a elaboração do Guia de melhores práticas para implantação de PoSIC nas IFES, em 05 etapas distintas, detalhadas em um conjunto de ações práticas para que as IFES estejam em conformidade com a segurança da informação e a própria legislação específica que a normatiza.

4.1 Guia para implantação de POSIC

O Guia tem a finalidade de promover as etapas de levantamento, planejamento, desenvolvimento, execução e revisão da PoSIC, de forma clara, objetiva e consistente, em conformidade com a legislação e padrões relacionados à segurança da informação, dada sua importância para as instituições que ainda não dispõem desse documento integralmente instituído ou que necessitem utilizá-lo nas práticas e processos de sua manutenção e revisão.

O Guia sugere um conjunto de ações práticas, definidas em consulta aos frameworks do COBIT 5 for *Information Security*, ITIL v3 e ISO/IEC 27002:2013.

4.2 Processo de utilização do Guia

O Guia está organizado em cinco etapas ou estágios de implementação e apresenta, para cada etapa, um conjunto de controles práticos que possibilitará às instituições adquirirem maturidade necessária para institucionalizar o documento. As etapas estão definidas como: levantamento de requisitos, planejamento, desenvolvimento, execução e revisão.

4.3 Etapa de Levantamento de Requisitos

Para a realização da PoSIC é sugerido realizar um levantamento do que existe na instituição em relação à segurança da informação, para a definição dos regulamentos que serão contemplados naquele documento. Por isso, é necessário analisar o que existe e quais são as necessidades da instituição. Esse conjunto de

regulamento existente será um orientador para o planejamento do projeto de implantação da política. A Tabela 2 apresenta todas as práticas e ações para o desenvolvimento dessa etapa.

Tabela 2
Etapa de Levantamento de Requisitos PoSIC**.**

ETAPA 01 - LEVANTAMENTO DE REQUISITOS		
Objetivo: Obter informações acerca das ações de segurança da informação, já desenvolvidas na instituição, por meio dos processos estratégicos, táticos e operacionais, visando gerar o Termo de Aceitação e Cumprimento da Alta Gestão.		
Indicador de Desempenho: Analisar ambiente institucional e conscientizar a Gestão máxima da necessidade da implantação de PoSIC.		
ID	**PRÁTICA**	**DESCRIÇÃO**
LR1	Identificar a existência do setor responsável pelo processo de implantação da PoSIC.	A PoSIC deverá ser planejada, desenvolvida e apresentada pelo Comitê de Segurança da Informação (CGSI). Se a instituição não tiver instituído o CGSI, verificar etapa 02-P.1.
LR2	Identificar o Gestor de Segurança da Informação.	É necessário instituir o Gestor de Segurança da Informação, o qual presidirá a equipe que desenvolverá a implantação da PoSIC.
LR3	Verificar a legislação e normas vigentes que regulariza a IFES.	Realizar levantamento de toda a legislação que rege a instituição para que a PoSIC não venha infringir a qualquer uma delas.
LR4	Identificar padrões, normas e procedimentos de segurança da informação já utilizada na IFES.	Essa prática permitirá a implementação de código de práticas que atendam as diretrizes da instituição quanto à governança de TI, gerenciamento de serviços e os controles práticos de segurança nos mais diversos níveis.
LR5	Realizar estudo de campo sobre a segurança da informação em todas as áreas da IFES.	Convém averiguar criticamente, por meio de pesquisa de campo (entrevistas, questionários, formulários, etc.), as ações desenvolvidas na instituição necessárias para assegurar a continuidade do planejamento da PoSIC.
LR6	Analisar o Planejamento Estratégico Institucional - PEI	Verificar e identificar os objetivos do PEI para o desenvolvimento da PoSIC.
LR7	Solicitar aprovação da Gestão máxima.	Gerar documento de aprovação para implementação da PoSIC. O relatório apresentado ao gestor máximo deverá constar o conjunto ações identificadas na etapa 01 - LR6.

Fonte: Estudos identificados na revisão sistemática – elaborada pelos autores (2016).

4.4 Etapa de Planejamento

Ao desenvolver uma PoSIC é necessário tratar esse assunto como um projeto com início, meio e fim. Deve ser feito seu planejamento e a identificação de todas as suas etapas futuras, bem como seu patrocinador deve criar a documentação de aprovação necessária, os treinamentos, papéis e responsabilidades, concluir o planejamento e compartilhar as lições apreendidas. Nessa etapa deve ser feita a descrição das necessidades para a elaboração da PoSIC, deve-se elaborar o cronograma necessário, declarar seu objetivo, fazer uma justificativa e solicitar a

aprovação da gestão máxima da instituição. A Tabela 3 apresenta todas as práticas e ações para implementação dessa etapa.

Tabela 3

Etapa de Planejamento da PoSIC

ETAPA 02 - PLANEJAMENTO		
Objetivo: Estabelecer as práticas e ações necessárias para o desenvolvimento da PoSIC, identificando as necessidades de segurança da informação para a instituição.		
Indicador de Desempenho: Elaborar as práticas que serão executadas na etapa de desenvolvimento da PoSIC.		
ID	**PRÁTICA**	**DESCRIÇÃO**
P1	Instituir Comitê Gestor de Segurança da Informação.	Instituir Comitê Gestor de Segurança da Informação em atendimento à etapa 01 – LR1. Na ausência do Comitê Gestor de Segurança da Informação, o Comitê de TI solicitará ao Gestor máximo da instituição a criação desse Comitê.
P2	Produzir Plano de Capacitação.	Elaborar um plano de capacitação sobre segurança da informação para o CGSI ou GT que desenvolverá a PoSIC, criando e mantendo processos de incentivo e aprimoramento das competências necessárias para identificar as vulnerabilidades existentes na instituição e as ações para desenvolver um plano de segurança da informação dos ativos da instituição.
P3	Estabelecer orçamento para todo o processo de implantação da PoSIC.	É necessário refletir nas prioridades estabelecidas incluindo ações como: treinamento para o CGSI, reuniões, aquisição de ativos, produção de material para divulgação e conscientização, manutenção do processo de atualização, etc.
P4	Elaborar catálogo de serviços com os possíveis serviços de serem monitorados pela PoSIC.	Um catálogo de serviço tornará transparente para a gestão máxima da instituição a lista de todos os serviços possíveis e disponíveis para serem analisados na etapa de análise de risco e protegidos na própria implementação da política.
P5	Analisar os riscos de segurança da informação da instituição.	Primeiro passo a ser feito antes do desenvolvimento da PoSIC é identificar os recursos críticos da instituição. Poderá ser aplicado à toda instituição, uma área ou departamento, um sistema de informações, etc.
P6	Elaborar Cronograma de Implementação.	Documento contendo todas as etapas da implantação da PoSIC, constando o período de implementação das diretrizes, normas e procedimentos, e as definições dos papeis e responsabilidades de todo membro desse processo.
P7	Estabelecer prazo para todo processo de implantação	Sugere-se um período de médio prazo entre um a dois anos para execução das práticas em acordo as legislações internas de cada IFES, considerando mudanças de cultura organizacional durante todo processo de implantação.
P8	Elaborar Termo de Aprovação	Sensibilizar o apoio da Gestão máxima para assinar o Termo de Aprovação. Um programa desta natureza necessita de patrocínio e apoio para alcançar o sucesso previsto. Esse é o primeiro objetivo das práticas do COBIT, ITIL e ISO/IEC 27002:2013, no processo de criação da PoSIC.
P9	Elaborar Termo de Responsabilidade	É sugerido a elaboração de um "**Termo de Responsabilidade do Usuário**" para todos os servidores, onde declaram ter pleno conhecimento das normas vigentes e do uso dos ativos e recursos computacionais da instituição. Esta é uma forma de garantir validade jurídica ao documento elaborado. Esse Termo deverá ter citado o Termo de Aprovação da PoSIC, assinado pela gestão máxima, transmitindo a todos os usuários da instituição o compromisso da gestão com a política.

Fonte: Estudos identificados na revisão sistemática – elaborada pelos autores (2016).

4.5 Etapa de Desenvolvimento

Nessa etapa, o escopo deve ser definido com ampla abrangência aos documentos que serão gerados. Deverá ser definido se será desenvolvida a política principal e suas normas e procedimentos em um único documento ou em documentos separados.

É necessário que sejam registradas as restrições, isto é, os fatores que podem impactar o projeto e impedir a construção da política. Por fim, é preciso definir o produto a ser entregue. Essa definição deve ser a mais detalhada possível, utilizando linguagem clara e eficaz, evitando dúvidas ao usuário final. A Tabela 4 apresenta todas as práticas e ações para o desenvolvimento dessa etapa.

Tabela 4
Etapa de Desenvolvimento da PoSIC

ETAPA 03 - DESENVOLVIMENTO		
Objetivo: Promover ações que orientem o Comitê Gestor de Segurança da Informação na execução das práticas para elaboração da PoSIC.		
Indicador de Desempenho: Elaborar o documento PoSIC.		
ID	**PRÁTICA**	**DESCRIÇÃO**
D1	Executar Cronograma de Implementação.	Executar todo o cronograma de atividades proposto na etapa de planejamento (P6). Verificar alterações no PEI e no recurso orçamentário destinado para as ações de implantação.
D2	Executar Plano de Capacitação	Executar Plano de Capacitação desenvolvido na etapa de planejamento (P2).
D3	Referenciar outras PoSIC	É comum que a PoSIC utilize conteúdos de outros documentos externos. Dessa forma, sugere-se que PoSIC faça referência a essas fontes utilizadas, evitando a cópia não autorizada de políticas de outras instituições já institucionalizados e/ou registrados, evitando maiores problemas jurídicos.
D4	Elaborar diretrizes, normas e procedimentos.	Estabelecer se as diretrizes, normas e procedimentos farão parte de um único documento ou serão criados em documentos separados.
D5	Definir arquitetura da PoSIC	Definir a arquitetura da PoSIC atendendo, no mínimo, as orientações da Norma Complementar Nº 03/IN01/DSIC/GSIPR.
D6	Definir conformidade	Definir a periodicidade da fiscalização da PoSIC em áreas da IFES com base nas diretrizes, normas, procedimentos ou outros documentos advindos da PoSIC em uso.
D7	Fundamentar legislação e normativa	Especificar toda a legislação e normativa que rege a instituição já detectada na etapa 01 – LR3.
D8	Descrever processo disciplinar	Descrever as punições disciplinares por violação da PoSIC.
D9	Definir periodicidade da PoSIC	É sugerido que a PoSIC não ultrapasse o período de dois anos para ser revisada ou até que seja solicitado pelo gestor de segurança da informação em consequência a mudanças estratégicas da instituição.

D10	Identificar suporte técnico da PoSIC	Identificar no corpo da PoSIC o contato de suporte para esclarecimentos dos usuários.
D11	Elaborar o Termo de Aprovação	Deve ser lida e aprovada pelo departamento Jurídico e RH, respectivamente. Após ser aprovado pela área jurídica, a PoSIC deverá ser apresentada ao Reitor da instituição para conhecimento, assinatura de aprovação.

Fonte: Estudos identificados na revisão sistemática – elaborada pelos autores (2016).

4.6 Etapa de Execução

Nessa etapa é necessário realizar formalmente a entrega da PoSIC pelo gestor aprovador (Reitor, Colégio Dirigente, CONSUP, etc.), pois para as regras que vão legislar internamente a instituição, é importante a data da publicação de cada um dos regulamentos. A partir dessa prática, a PoSIC passa a valer para todos os usuários da informação da IFES.

Práticas como comunicação e treinamento da política tornam-se necessários para a cobrança de sua utilização. A Tabela 5 apresenta todas as práticas e ações para a implementação dessa etapa.

Tabela 5
Etapa de Execução da PoSIC

ETAPA 04 - EXECUÇÃO		
Objetivo: Publicar a PoSIC para todos os usuários (servidores, prestadores de serviço, estagiários, alunos, etc.) da instituição por meio de técnicas de divulgação e educação funcional.		
Indicador de Desempenho: Utilização da política por todos os servidores da instituição.		
ID	**PRÁTICA**	**DESCRIÇÃO**
E1	Oficializar a PoSIC.	Institucionalizar a PoSIC na instituição utilizando de Resolução Interna.
E2	Publicar a PoSIC.	Divulgar a PoSIC no âmbito geral da instituição tornando conhecida por todos os servidores, prestadores de serviço, estagiários e agentes externos.
E3	Fornecer treinamento aos usuários.	Todos os servidores da instituição, terceirizados e prestadores de serviços, devem ser comunicados e, de alguma forma, receber treinamento apropriado sobre utilização da PoSIC.
E4	Executar a fiscalização de conformidade.	Fiscalizar periodicamente a PoSIC mediante a legislação e a conformidade vigente na instituição.

Fonte: Estudos identificados na revisão sistemática – elaborada pelos autores (2016).

4.7 Etapa de Revisão e Manutenção

Essa etapa define como acontecerá a manutenção e atualização da PoSIC. É sugerida uma política específica para a manutenção e a atualização de regulamentos mais detalhados, indicando, por exemplo, quem é o responsável pela revisão da PoSIC e em que situações deve acontecer uma manutenção.

A revisão deverá acontecer de acordo com a prática já especificada na etapa de planejamento, onde consta a especificação da periodicidade de revisão. A tabela 6 apresenta todas as práticas e ações para implementação dessa etapa.

Tabela 6
Etapa de Revisão e Manutenção da PoSIC

ETAPA 05 - REVISÃO E MANUTENÇÃO		
Objetivo: Promover ações que orientem o CGSI na execução das práticas para revisão da PoSIC. **Indicador de Desempenho:** Manter a PoSIC atualizada constantemente.		
ID	**PRÁTICA**	**DESCRIÇÃO**
RM1	Estabelecer periodicidade para Revisão.	É sugerido que a PoSIC não seja revisada fora do período estipulado na etapa 03 – D9. É necessário identificar a data de aprovação e divulgação apresentada na etapa 04 – E2. O Gestor de segurança da informação deverá solicitar ao Comitê de TI a sua revisão, sempre que o período for finalizado.
RM2	Analisar relatórios de incidentes.	Os relatórios de incidentes de segurança da informação devem ser analisados sob responsabilidade da equipe de Tratamento de Incidentes, dentro do período de vigência da PoSIC.
RM3	Rever Planejamento Estratégico Institucional – PEI.	Verificar se houve alteração no PEI. Essa ação é necessária para não alterar a PoSIC em desacordo com o PEI. Ver etapa 01 – LR6.
RM4	Elaborar planejamento de revisão.	Atender todas as práticas da etapa 02, considerando as ações necessárias para as alterações que se fizerem necessário para a revisão.
RM5	Alterar Diretrizes, Normas e Procedimentos.	Identificar em qual etapa e ações a PoSIC sofrerá alterações (diretrizes, normas ou procedimentos) para não demandar tempo desnecessário analisando a PoSIC como um todo. Ver etapa 03 – D4.
RM6	Verificar legislação vigente.	Verificar alterações na legislação vigente da instituição e atualizar se necessário. Ver etapa 01 – LR3 e etapa 03 – D7.
RM7	Atender à mudança institucional	Analisar os incidentes de segurança da informação e/ou mudança institucional e/ou novas recomendações que se fazem necessárias.
RM8	Aprovar alterações na PoSIC	Apresentar para a alta gestão, as alterações necessárias para atualização da PoSIC e solicitar aprovação da mesma.
RM9	Executar alterações da PoSIC	Publicar as alterações aprovadas pelo gestor máximo da instituição. Ver etapa 04 – E2.

Fonte: Estudos identificados na revisão sistemática – elaborada pelos autores (2016).

4.8 Avaliação do Guia

Para assegurar que o Guia alcance seu propósito, foi elaborado um questionário de avaliação com gestores de segurança da informação que já implantaram a PoSIC em suas instituições, de forma a complementar os resultados obtidos com a elaboração do documento. A avaliação foi fundamentada no Modelo de Aceitação de Tecnologia (*Technology Acceptance Model* - TAM) de Davis (1989). O modelo TAM sugere que fatores como facilidade de uso percebida e utilidade percebida influenciam na intenção de uso de um novo sistema ou abordagem teórica e metodológica. Para Davis (1989), as pessoas tendem a usar ou não uma tecnologia com o objetivo de melhorar seu desempenho no trabalho (utilidade percebida). Porém, mesmo que essa pessoa entenda que uma determinada tecnologia é útil, sua utilização poderá ser prejudicada se o uso for muito complicado, de modo que o esforço não compense o uso (facilidade percebida).

O questionário elaborado foi composto por uma lista de afirmações relacionadas à utilidade e facilidade de uso do guia, utilizando a escala Likert para medir a opinião dos respondentes (ver Tabela 1). Uma outra questão, não obrigatória, solicitou que os gestores de segurança da informação relatassem os benefícios e as limitações que encontraram ao avaliar o Guia.

A avaliação procurou obter um número expressivo de participantes com base nas IFES que utilizam a PoSIC, de forma integral, apresentado em TCU (2016). Como critério para determinar o número adequado de amostra para a avaliação do Guia, foi utilizado o cálculo de Amostra Finita, conforme disposto na Figura 2,

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

Figura 2
Fórmula para cálculo de Amostra Finita.
Nota. Fonte: GIL, A. C. (2008). Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas.

onde: σ^2 = nível de confiança escolhido, expresso em número de desvios-padrão; p = percentual com o qual o fenômeno se verifica; q = percentual complementar (100 – p); N = tamanho da população; e^2 = erro máximo permitido; n = tamanho da amostra.

Substituindo-se os valores na fórmula apresentada, foi estabelecido que o percentual com o qual o fenômeno se verifica seja por volta de 2,0%; portanto p é igual a 100 – 2, ou seja, 98. Em seguida, adotou-se um nível de confiança de 95,5% (corresponde a dois desvios-padrão) e um erro máximo de 5,0%. Aplicando-se a fórmula encontrou-se o seguinte resultado apresentado na Figura 3.

$$x = \frac{2^2 . 2 . 98 . 34}{5^2(34-1) + 2^2 . 2 . 98} = \frac{26656}{1609} = \mathbf{16,56}$$

Figura 3
Cálculo da Amostra Finita.
Nota. Fonte: GIL, A. C. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008.

Tendo como base a fórmula apresentada, observa-se a necessidade de uma amostra de aproximada de 16 questionários respondidos. Para alcançar o número de amostra necessário, foi enviado, para e-mails dos gestores de segurança da informação das IFES, um link no qual o Guia e o questionário de avaliação ficaram disponíveis eletronicamente por um período de 15 (quinze dias). O questionário foi elaborado e disponibilizado na plataforma *LimeSurvey (software* livre para aplicação de questionários online) para que as instituições pudessem participar da avaliação.

Após o período de avaliação, apenas 13 (treze) gestores de segurança da informação de instituições que já tem sua PoSIC responderam ao questionário. A Tabela 7 apresenta o resultado da avaliação do Guia de melhores práticas para implantar e revisar PoSIC nas IFES.

Tabela 7
Utilidade e facilidade de uso percebida do Guia.

ID	Afirmações	Concordo plenamente	Concordo parcialmente	Nem concordo nem discordo	Discordo parcialmente	Discordo plenamente
1	A estrutura apresentada pelo Guia facilita a implantação ou revisão da PoSIC sem maiores dificuldades.	54% (7)	46% (6)	0	0	0
2	A descrição de cada etapa está clara e compreensível.	77% (10)	23% (3)	0	0	0
3	O Guia torna fácil a tomada de decisão dos responsáveis envolvidos na implantação.	54% (7)	38% (5)	8% (1)	0	0
4	**As etapas de implantação**	77% (10)	15% (2)	8% (1)	0	0

	otimizam o tempo de planejamento e elaboração da PoSIC.					
5	**O conteúdo do Guia prepara a IFES para o desenvolvimento de uma PoSIC clara e objetiva**	38% (5)	64% (8)	0	0	0
6	**As práticas e ações apresentadas em cada etapa do Guia favorecem o desenvolvimento de competências e habilidades para o processo de implantação de PoSIC**	62% (8)	23% (3)	8% (1)	7% (1)	0
7	**O Guia pode ser utilizado em qualquer IFES, independente de sua estrutura, sua cultura ou sua missão institucional**	54% (7)	38% (5)	8% (1)	0	0
8	**Utilizaria ou recomendaria o Guia para outras instituições que necessitam implantar ou revisar a PoSIC**	70% (9)	30% (4)	0	0	0

Fonte: Elaborada pelos autores (2016).

Os resultados da avaliação apontam que a percepção dos respondentes em relação à implantação e revisão de PoSIC é positiva e demonstra que o Guia pode ser alinhado com os processos de segurança da informação das instituições mediante ações táticas, estratégicas e operacionais. O que se percebe nessa avaliação é que a maioria dos avaliadores concorda com todas as afirmações apresentadas no questionário, mesmo plenamente ou parcialmente; porém é considerado que as práticas e ações apresentadas pelo Guia permitem que as mais diversas instituições de ensino possam traduzir os procedimentos operacionais de segurança da informação em direcionamentos consistentes, estabelecendo diretrizes, normas e procedimentos com vistas à manutenção do bom uso da informação obedecendo aos fundamentos legais e normativos da instituição, permitindo assim o processo de implantação da PoSIC.

5 Considerações Finais

Esta pesquisa teve como objetivo principal apresentar um Guia de melhores práticas para implantação e revisão de PoSIC IFES de forma objetiva, clara e consistente, em conformidade com a legislação e padrões relacionados à segurança da informação, dada sua importância para as instituições que ainda não dispõem desse documento integralmente instituído ou que necessitem utilizá-lo nas práticas e processos de sua manutenção e revisão.

Dessa forma, instituições públicas ou privadas poderão se utilizar desse documento para planejar a implantação da PoSIC, alinhando os objetivos da segurança da informação com o planejamento estratégico da instituição. Dois fatores importantes são considerados nesse processo de implantação da PoSIC: o apoio da Alta Gestão e o envolvimento do comitê de segurança da informação. Tais papéis, se participativos em todas as etapas, farão com que a PoSIC se torne um documento consolidado e de valor jurídico dentro da instituição, considerando o teor das informações nele contidas.

5.1 Recomendações

Outras pesquisas relacionadas à política de segurança da informação, em específico nos órgãos da APF, podem ser derivadas deste estudo, utilizando seus aspectos, referenciais bibliográficos, práticas e recomendações. Duas recomendações para trabalhos futuros podem ser consideradas, tais como: a realização de um estudo de caso com aplicação do Guia, de forma integral, em alguma IFES que ainda não tenha institucionalizado sua PoSIC, com o intuito de obter dados sobre a eficiência das práticas proposta e um estudo com levantamento bibliográfico das metodologias utilizadas na implantação de PoSIC, e também selecionar uma ou mais metodologias, identificar demais práticas que ajudarão a fortalecer o documento proposto e aplicá-las em um estudo de caso.

Referências

Araújo, W. J. de (2012). Leis, decretos e normas sobre Gestão da Segurança da Informação nos órgãos da Administração Pública Federal. *Informação & Sociedade*: *Estudos*, v. 22.

Biolchini, J., Mian, P. G., Natali, A. C., & Travassos, G. H. (2005). Systematic Review in Software Engineering: relevance and utility. Relatório Técnico RT-ES-679/05, *Programa de Engenharia de Sistemas e Computação* (PESC), COPPE/UFRJ.

Cardoso, M. de O. (2011). *Propostas de Diretrizes para o Desenvolvimento de uma Política de Segurança da Informação e Comunicações para o Centro de Processamento de Dados Distrito Federal da Dataprev Baseadas na Norma ABNT NBR ISO/IEC 27002:2005.* (Dissertação de Especialização em Ciência da Computação. Universidade de Brasília, Brasília, DF, Brasil).

Cardoso, J. (2013). IT Policy Framework Based on COBIT 5. *ISACA Journal,* (1). Recuperado de http://www.ISACA.org/Journal/archives/2013/Volume-1/Documents/13v1-IT-Policy-Framework-Based.pdf

Decreto nº 3.505 de 13 de junho de 2000 (2000). Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. **Presidência da República. Disponível em** http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm.

Davis F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology**.** *MIS Quarterly*, p.319.

Editora ABNT (2013). NBR ISO/IEC 27001:2013. Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão da segurança da informação. Rio de Janeiro: ABNT. Autor.

Editora ABNT (2013). NBR ISO/IEC 27002:2013. Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT. Autor.

Editora ISACA (2012). COBIT. 5: A Business Framework for the Governance and Management of Enterprise IT. Author.

Editora ISACA (2012). COBIT 5 for Information Security. Author.

Fontes, E. (2012). *Políticas e normas para segurança da informação*. Rio de Janeiro: Brasport.

Gehrmann, M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. Navus-*Revista de Gestão e Tecnologia*, *2(2)*, 66-77.

Kauark, F., Manhaes. F. C., & Medeiros. C. H. (2010). *Metodologia da pesquisa: guia prático.* Itabuna: Via Litterarum.

Lei Nº 8.159, de 8 de janeiro de 1991 (1991, 8 de janeiro). Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L8159.htm.

Monteiro, I. L. C. O. (2009). Proposta de um Guia para elaboração de políticas de segurança da informação e comunicação em órgãos da APF. (Dissertação de mestrado em Ciência da Computação. Universidade de Brasília, Brasília, DF, Brasil).

Presidência da República (2009). *Norma Complementar nº 03/IN01/DSIC/GSI/PR.* Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Disponível em http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

Sengupta, A., Mazumdar, C., & Bagchi, A., (2011). A Methodology for Conversion of Enterprise-Level Information Security Policies to Implementation-Level Policies/Rule. In: Emerging Applications of Information Technology (EAIT), *Second International Conference on IEEE*, pp. 280-283.

Taylor, S. (2011). ITIL: Service Design. Best management Pratice. *TSO The Stationary*, London, edition.

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

Tribunal de Contas da União (2015). *Levantamento de Governança de TI 2014*. Disponível em http://portal3.tcu.gov.br/portal/pls/portal/docs/2705176.pdf.

Tribunal de Contas da União (2016). *Demanda nº 265-54* [mensagem pessoal]. Mensagem recebida por no-replay@tcu.gov.br em 30 maio de 2016.

Tuyikeze, T., & Flowerday, S. (2014). Information Security Policy Development and Implementation: A Content Analysis Approach. In: *HAISA*, 11-20.

Veiga, A. da. (2015). The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. *HAISA*, 22-33.