navus
Revista de Gestão e Tecnologia

Recebido em 31/10/2016. Aprovado em 17/02/2017. Avaliado pelo sistema *double blind peer review*. Publicado conforme normas da ABNT.
http://dx.doi.org/10.22279/navus.2017.v7n2.p49-65.482

Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação

Orlivaldo Kléber Lima Rios Mestrando em Ciência da Computação. Universidade Federal de Pernambuco (UFPE) – Brasil. oklr@cin.ufpe.br
José Gilson de Almeida Teixeira Filho Doutor em Ciência da Computação. Universidade Federal de Pernambuco (UFPE) – Brail. jgatf@cin.ufpe.br
Vânia Patrícia da Silva Rios Licencianda em Ciência da Computação. Instituto Federal Baiano (IFB) – Brasil. vanipaty@yahoo.com.br

RESUMO

Instituições Federais do Ensino Superior desenvolvem suas atividades acadêmicas e administrativas com base em seus Planejamentos. Cada instituição desenvolve suas regras de conduta que devem estar asseguradas por suas políticas de segurança da informação e comunicação. Entretanto, no último Levantamento de Governança de TI em 2014, elaborado pelo Tribunal de Contas da União, foi divulgado que apenas 51% dos órgãos da Administração Pública Federal adotaram integralmente a política de segurança da informação e comunicação. Considerando que há recomendações e orientações do Governo Federal para a institucionalização dessa política em todos os órgãos da Administração Pública Federal, direta e indireta, essa pesquisa teve como objetivo identificar o cenário em que se encontram as Instituições Federais do Ensino Superior na área de gestão de segurança da informação, quanto a existência e as práticas utilizadas para elaboração e implantação da política de segurança da informação e comunicação. Foi utilizado o método indutivo de natureza aplicada com uma abordagem quantitativa e procedimento documental. Teve como instrumento de coleta de dados a aplicação de um questionário em estudo de campo envolvendo todas as instituições federais de ensino superior do Brasil. Ao final da pesquisa percebeu-se que o fator humano é a maior criticidade para o sucesso no planejamento da PoSIC, principalmente a participação da Alta Gestão. A pesquisa mostrou a necessidade de promover ações estratégicas dos processos de segurança da informação, nas organizações governamentais, em especial as IFES, quanto à implantação da PoSIC.

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

Information security management: practices used by federal higher education institutions for deployment of information security policy

ABSTRACT

Federal Institutions of Higher Education develop their academic and administrative activities based on their Planning. Each institution develops its rules of conduct that must be carried out by its information and communication security policies. However, in the last Survey of IT Governance in 2014, prepared by the Federal Audit Court, it was reported that only 51% of the Federal Public Administration fully adopted the security policy of information and communication. Considering that there are recommendations and guidelines of the Federal Government to institutionalize this policy in all organs of the Federal Public Administration, both direct and indirectly, this research aimed to identify the scenario where the Federal Higher Education Institutions regarding the existence and practices used to the design and implementation of information and communication security policy. The inductive method with a quantitative approach and documentary procedure was used, and a field study survey as data collection tool involving all federal institutions of higher education in Brazil was applied. At the end of the survey it was realized that the human factor is the most critical factor for success in the planning of Information Security Policy, especially the participation of the High Management. The research has shown the need to promote strategic actions of information security processes in government organizations, especially the Federal Institutions of Higher Education, concerning the implementation of Information Security Policy.

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

1 INTRODUÇÃO

O Tribunal de Contas da União - TCU, por meio da Secretaria de Fiscalização de TI - Sefti, publicou por meio do Acórdão 1.603/2008 – Plenário, um quadro crítico dos processos de segurança da informação dos órgãos da Administração Pública Federal - APF, direta e indireta (BRASIL, 2008). Dados daquele Acórdão demonstraram que dos órgãos pesquisados, 64% não tinham instituído sua Política de Segurança da Informação e Comunicação - PoSIC. Assim, o TCU, entendendo que a constatação dessa fiscalização era preocupante na área de segurança da informação, recomendou ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR, que:

> [...] orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso (BRASIL, 2008, p. 41).

Considerando tal recomendação, o Ministro Chefe do GSI/PR, na condição de Secretário-Executivo do Conselho de Defesa Nacional, através da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 (BRASIL, 2008), designou a Norma Complementar 03/IN01/DSIC/GSIPR (BRASIL, 2009) com o objetivo de estabelecer diretrizes, critérios e procedimentos para a elaboração, institucionalização, divulgação e atualização da PoSIC nos órgãos e entidades da APF, direta e indireta. Nessa norma complementar constam orientações de como pode ser a elaboração da PoSIC, recomendando itens a serem contemplados. Entretanto, apesar de ser uma recomendação, a norma não é específica para ser implementada apenas em um determinado órgão da APF, fato este que pode influenciar na disseminação de diversos modelos de PoSIC, tornando-se necessário uma atenção redobrada na elaboração desse documento para um determinado segmento da APF.

Segundo a Secretaria de Fiscalização de Tecnologia da Informação (BRASIL, 2015), no ano 2014, 51% dos órgãos pesquisados adotaram integralmente a PoSIC. Outros 15% assumiram ter a política, porém só utilizavam parcialmente. Assim, percebe-se que 34% dos órgãos pesquisados não possuíam a PoSIC institucionalizada, ou seja, não havia o documento em que a Alta Administração definisse sua visão sobre o assunto com as diretrizes que direcionassem as ações de segurança da informação em conformidade a legislação do órgão, alinhada ao seu Planejamento Estratégico, bem como as definições de responsabilidades de cada processo ou atividade desenvolvida no órgão.

Apesar de a PoSIC ser o principal instrumento direcionador da gestão da segurança da informação, é preocupante que apenas 66% (15% parcialmente e 51% integralmente) dos órgãos que participaram daquela pesquisa declararam dispor de uma política formalmente instituída como norma de cumprimento obrigatório.

Entretanto, mesmo com ações do governo federal que promovam a implantação de PoSIC, algumas Instituições Federais do Ensino Superior – IFES ainda não disponibilizam esse documento em caráter institucionalizado (Brasil, 2016). Tal informação é exposta pelo Levantamento de Governança de TI, realizado pela Secretaria de Fiscalização de Tecnologia da Informação (BRASIL, 2015). Segundo Brasil (2016), 98 IFES participaram daquele levantamento (BRASIL, 2015), porém, apenas 47 instituições declararam ter a PoSIC em suas instituições. Todavia, apenas 34 instituições declararam utilizar de forma integral, outras 13 instituições ainda estão em fase de finalização, seguindo o documento parcialmente. Outras 51 instituições declararam que ainda não dispõe de uma PoSIC.

Considerando que há recomendações e orientações do governo federal para a institucionalização da PoSIC em todos os órgãos da APF, direta e indireta, e considerando que as IFES estão inseridas nesse panorama de fiscalização do TCU, 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 identificar o cenário das IFES quanto à existência da PoSIC, assim como as práticas em gestão de segurança da informação utilizadas por instituições que já institucionalizaram esse documento.

2 REFERENCIAL TEÓRICO

Discute-se neste capítulo a segurança da informação, política de segurança da informação e PoSIC na administração pública federal.

2.1 Segurança da Informação

Para Fontes (2012, p. 6) "a informação é um recurso essencial para toda e qualquer organização, independentemente do seu porte e do segmento de atuação no mercado". As organizações dependem incessantemente das informações para seus processos decisórios, crescimento corporativo e planejamento das atividades estratégicas e operacionais. Dzazali e Hussein (2012) destacam que, organizações públicas enfrentam o desafio de proteger suas informações, considerando que são ambientes onde há crescente complexidade, interconexões, incertezas e dependência da tecnologia, tendo ainda que realizar suas respectivas missões sem deixar de se submeter às normas e diretrizes provenientes dos órgãos centrais do governo. Contudo, é necessário que algumas medidas sejam tomadas para que tais informações sejam mantidas seguras e invioláveis.

Segundo Quintella e Branco (2013, p. 2), segurança da informação diz respeito à "proteção da informação contra ameaças que possam valer-se das vulnerabilidades dos ativos, preservando suas propriedades fundamentais: disponibilidade, integridade, confidencialidade e autenticidade". Castilho (2013, p. 55) comenta que "a segurança da informação é obtida a partir da implementação de um conjunto de políticas, processos, procedimentos e estruturas organizacionais de *hardware* e *software*".

Nesse processo de segurança da informação, as organizações necessitam ser direcionadas para a elaboração e implantação de uma PoSIC, descrevendo os procedimentos necessários para a proteção de seus recursos de informação contra a divulgação indevida de forma intencional ou não intencional, modificação não autorizada, destruição não desejada ou negação de serviço através da implantação de controles de segurança.

2.2 Política de Segurança da Informação

A política é uma regra universal, dentro de uma organização, que define as ações e limites para alcançar os objetivos e metas organizacionais. É o documento que definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implementados na proteção da informação (ABNT, 2013a; ALBUQUERQUE JUNIOR; SANTOS, 2014).

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). Estabelece quais medidas de segurança uma organização deve proceder para proteger seus bens físicos e os dados armazenados em componentes tecnológicos (ABNT, 2013a), "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; MAZUMDAR; BAGCHI, 2011).

Faz parte das boas práticas da segurança da informação que qualquer organização tenha sua PoSIC para que o processo de segurança da informação possa ser elaborado, implantado e mantido. Essa política dará o direcionamento necessário para que as organizações definam as regras, os procedimentos e os controles que serão implantados na proteção da informação (FONTES, 2012).

Para elaboração e institucionalização da PoSIC, deve ser realizado o levantamento de informações para a obtenção dos padrões, normas e procedimentos de segurança (FERREIRA; ARAÚJO, 2009), tendo o entendimento das necessidades e uso dos recursos da TI. Com esse direcionamento, Monteiro (2009) ressalta que a PoSIC deverá ser um documento simples e de fácil entendimento, pois deverá ser lido por todos na organização.

Além da descrição das etapas, das práticas e ações que envolvem todo processo de implantação da PoSIC nos órgãos da APF, "é importante considerar a legislação local em termos de estatuto, regulamentos e contratos vigentes, além de considerar a legislação específica e vigente no país" (COELHO; ARAÚJO; BEZERRA, 2014, p. 180). Assim, todos os requisitos que estão envolvidos na implantação da PoSIC devem ser definidos, documentados e armazenados nas instituições.

2.3 PoSIC na Administração Pública Federal

O uso da PoSIC em uma instituição da APF se justifica na própria Constituição Federal, artigo 37, caput, que vincula a Administração Pública aos princípios da legalidade. Considerando tal princípio, a própria Constituição Federal institui o uso de Política de Segurança da Informação e Comunicação nos órgãos e entidades da Administração Pública Federal (BRASIL, 2000).

Segundo Araújo (2012, p. 15), "o Brasil não possui uma Lei única para tratar a segurança da informação, mas, no conjunto de sua legislação, várias podem ser aplicadas na tentativa de manter a segurança de seus ativos nos órgãos da APF". Corroborando com o autor, 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". Já o Decreto nº. 4.553/2002 trata da "salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal" (ARAÚJO, 2012, p. 24).

Preocupado em manter propriedade intelectual e a segurança da informação das organizações e instituições vinculadas aos órgãos da APF, o governo federal brasileiro estabeleceu, em 13 de junho de 2000, o Decreto 3.505 (BRASIL, 2000) com a finalidade de instituir a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal.

Atendendo ao referido decreto e tendo o intuito de atingir os objetivos da segurança da informação 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 (BRASIL, 2009; ARAÚJO, 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 (BRASIL, 2009).

Uma PoSIC deverá contemplar princípios, diretrizes e regras gerais. A mesma deverá ser institucionalizada para sua aplicação em todo órgão.

3 METODOLOGIA

A definição do instrumento metodológico em uma pesquisa está diretamente relacionada com o problema a ser estudado. Para Kauark, Manhães 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 do espírito.

Para a realização dessa pesquisa foi utilizado o método indutivo para alcançar o objetivo proposto. Esse método é caracterizado pelo fato de que o pesquisador parte da observação de fatos ou fenômenos cujas causas deseja conhecer, ou seja, parte-se de algo particular para uma questão mais ampla, mais geral (PRODANOV; FREITAS, 2013). A pesquisa seguiu uma abordagem quantitativa, adequada para apurar opiniões e atitudes explícitas e conscientes dos entrevistados, pois utiliza normalmente instrumentos estruturados (questionários). Nesse caso, procurou analisar e discutir os resultados dos questionários aplicados aos profissionais de TI das IFES. Para classificar e analisar as práticas utilizadas no processo de implantação de POSIC requereu-se de técnica estatística, conforme é retratado em Gil (2010).

Segundo Gerhardt e Silveira (2009), para se desenvolver uma pesquisa, é indispensável selecionar o método e seus procedimentos a serem aplicadas, podendo ser escolhidas diferentes modalidades. Nesse trabalho foram utilizados os procedimentos documental - utilizando documentos oficiais do TCU emitidos ao GSI/PR, Instruções Normativas, Norma Complementar, Decretos e Leis que regem a segurança da informação em órgãos da APF. Quanto ao procedimento de levantamento, foi utilizado o questionário *survey*, elaborado e aplicado em todas as IFES dos estados brasileiros.

A aplicação do questionário ocorreu por meio do preenchimento de um formulário web, implementado em *software LimeSurvey*, aplicado diretamente com profissionais de TI, cujas informações a respeito da institucionalização da PoSIC e suas práticas de implantação se desejou conhecer (GIL, 2010). Cada participante respondeu a um total de 29 perguntas, sendo contactados por meio telefônico e envio de *e-mails,* convidando-os a responder ao *survey*. No *e-mail* constavam orientações sobre os procedimentos a serem seguidos para preenchimento do questionário, onde ficou disponível entre 15/05/2016 a 15/07/2016, período em que a amostra selecionada contribuiu para alcançar o objetivo da pesquisa.

3.1 Definição da população e amostra

A população ou universo da pesquisa foi direcionado aos Núcleos de Tecnologias da Informação das IFES. Para a caracterização do perfil das instituições referente às práticas de gestão para implantação de PoSIC, foi necessário utilizar o método de amostragem com uma pequena parte dos elementos que compunham o universo. “Quando essa amostra é rigorosamente selecionada, os resultados obtidos na pesquisa tendem a aproximar-se bastante dos que seriam obtidos caso fosse possível pesquisar todos os elementos do universo” (GIL, 2010, p. 109).

Para esse estudo foi utilizado o tipo de amostra Probabilística Casual Simples, onde “cada elemento da população tem oportunidade igual de ser incluído na amostra” (KAUARK; MANHÃES; MEDEIROS, 2010, p. 62). Com o auxílio de procedimentos estatísticos, tornou-se possível calcular a margem de segurança e dos resultados obtidos. O estudo considerou o cálculo da Amostra Finita com uma população da pesquisa inferior a 100.000 IFES, considerando que no MEC existem 63 Universidades, 38 Instituições Federais de Ensino, 02 Centros de Educação Federal de Ensino Tecnológica e 01 Colégio Pedro II, totalizando 104 Instituições de Ensino Superior Federal.

Em termos estatísticos, para uso do cálculo da Amostra Finita, utilizou-se a seguinte fórmula apresentada na Figura 1.

Figura 1 - Fórmula para cálculo de Amostra Finita.

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

Onde:
σ^2 = nível de confiança escolhido;
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.

Fonte: Adaptado de Gil (2008, p. 97).

Substituindo os valores na fórmula apresentada, foi estabelecido que o percentual com o qual o fenômeno se verifica seja por volta de 3,0%, portanto p é igual a 100 – 3, ou seja, 97. Em seguida, adotou-se um nível de confiança de 99,7% (corresponde a três desvios-padrão) e um erro máximo de 5,0%.

Aplicando-se a fórmula encontrou-se o seguinte resultado representado na Figura 2.

Figura 2 - Cálculo de Amostra Finita.

$$\boldsymbol{x} = \frac{3^2 . 3 . 97 . 104}{5^2(104 - 1) + 3^2 . 3 . 97} = \frac{272376}{5194} = \mathbf{52,44}$$

Fonte: Elaborado pelos autores (2016).

Tendo como base na fórmula apresentada, observa-se a necessidade de uma amostra aproximada de **52,44** questionários respondidos, representando uma população de **104** Instituições de Ensino Superior Federal. O número mínimo de amostras foi arredondado para **52** instituições. Essa amostra era necessária para que o presente estudo possuísse significância estatística em um nível de confiança estabelecido e aceitável, entretanto, no período em que o questionário esteve ativo o que se obteve foi um número de respostas acima do resultado apresentado no cálculo de Amostra Finita, totalizando **67** respostas.

3.2 Seleção e Organização dos Dados

Durante o período de recebimento das respostas, por meio do questionário eletrônico, foi possível perceber diversas informações duplicadas e/ou incompletas. Nesse período já foi possível iniciar o processo de seleção das respostas recebidas, o que diminuiu consideravelmente o número de respostas válidas (completas) a serem analisadas. Gil (2010, p. 113) diz que "é necessário também, à medida que os dados sejam agrupados, examiná-los para verificar se estão completos, claros, coerentes e precisos".

Quanto à participação dos institutos no preenchimento do questionário, 151 respostas foram enviadas e agrupadas na base de dados do questionário eletrônico. Entretanto, após finalizar o período de preenchimento do questionário, 84 dessas respostas foram desconsideradas ao analisar inconsistências nas mesmas (incompletas ou duplicadas), sendo selecionadas apenas 67 respostas válidas (completas), permitindo o não comprometimento da etapa posterior de análise e interpretação dos dados conforme apresenta a Tabela 1.

Tabela 1 - Quantidade de respostas na pesquisa de campo.

Instituições Federais de Ensino Superior pesquisadas			
	Respostas		
	Completas e válidas	Incompletas	Duplicadas
Total	**67**	63	21

Fonte: Elaborada pelos autores (2016).

O questionário foi projetado na base *Limesurvey* de uma forma que o próprio sistema pudesse analisar e selecionar todos os campos preenchidos e separasse o questionário com todas as questões completas, correspondendo a 44% de sua totalidade de respostas (67 respostas), das questões incompletas, o que corresponde a um percentual de 56% (84 respostas), permitindo ao analista de dados, no caso o autor do presente estudo, a identificação de respostas inconsistentes e/ou duplicadas sem validade para análise exploratória dos dados.

4 RESULTADOS E DISCUSSÕES

Esta seção apresenta os resultados obtidos no estudo de campo por meio do *survey*. A análise foi realizada com base nas respostas ao questionário, cujo objetivo foi levantar dados quantitativos das instituições que já têm uma PoSIC institucionalizada, assim como tornar conhecidas as práticas utilizadas para sua implantação. Os resultados obtidos contemplam seis áreas levantadas no questionário aplicado: identificação da instituição; planejamento e elaboração da PoSIC; aprovação e institucionalização; conformidade e penalidade; fatores críticos e melhores práticas para implantar PoSIC.

4.1 Identificação das Instituições

A pesquisa foi feita em 104 instituições distribuídas e localizadas nas cinco regiões brasileiras. Conforme se pode observar na Tabela 2, apenas 64% das instituições responderam ao questionário, o equivalente a um total de 67 instituições, sendo 32 Universidades Federais e 35 Institutos Federais de Educação, Ensino e Tecnologia. A região nordeste teve o maior número de respostas com a participação de 20 instituições.

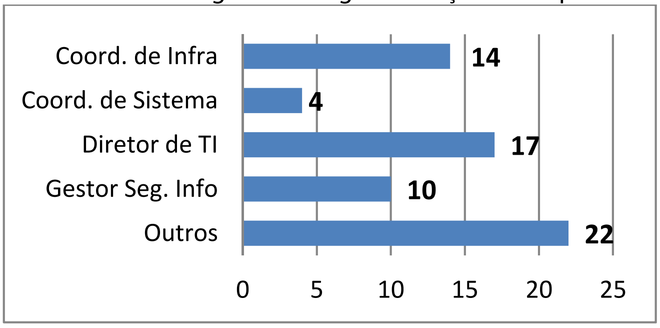
Tabela 2 - Relação de instituições pesquisadas por região.

Região	Pesquisadas	Responderam	%
Norte	15	11	10%
Nordeste	29	20	19%
Centro-Oeste	12	8	8%
Sul	17	10	10%
Sudeste	31	18	17%
TOTAL	**104**	**67**	**64%**

Fonte: Elaborada pelos autores (2016).

O questionário foi destinado aos profissionais da área de Tecnologia da Informação que desempenham alguma atividade de gestão em TI ou que tenham relação direta com as práticas de segurança da informação ou com o gerenciamento da PoSIC. Conforme pode ser visto na Figura 3, é apresentado o quantitativo de 45 respostas para opções de cargos pré-determinadas para coordenador de infraestrutura, coordenador de sistemas, diretor de TI, gestor de segurança da informação e outros cargos ou funções ligadas à segurança da informação.

Figura 3 - Cargo ou função do respondente.

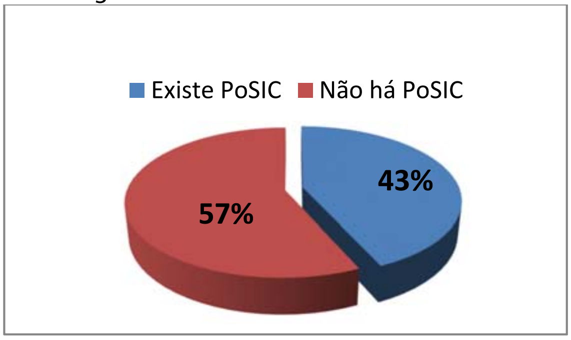


Fonte: Elaborado pelos autores (2016).

A opção “Outros” informou a quantidade de profissionais e sua área de atuação nas IFES, tais como: Analista de TI (07), Analista de Segurança da Informação (02), Coordenador de Suporte (01), Coordenador de Redes e Segurança (06), Coordenador de TI (03), Diretoria Adjunto de TI (01) e Técnico de TI (02), totalizando o quantitativo de 22 respondentes.

Considerando a amostra de 67 de IFES que responderam aos questionários, apenas 29 instituições declararam ter a PoSIC, o que corresponde a 43% dos respondentes. 36 instituições declararam não ter implantado ainda sua política, conforme apresenta a Figura 4.

Figura 4 - Existência de PoSIC nas IFES.



Fonte: Elaborado pelos autores (2016).

Apesar de a PoSIC ser o principal instrumento direcionador da gestão da segurança da informação, é preocupante que 57% das IFES que participaram daquela pesquisa declararam não disporem de uma política formalmente instituída como norma de cumprimento obrigatório em atendimento ao Decreto 3.505 e a Norma Complementar nº 03/IN01/DSIC/GSIPR. Alguns fatores de risco podem contribuir para que as IFES não tenham esse documento integralmente instituído, dentre eles podem ser citadas a falta de um comitê de segurança da informação, a falta de apoio da alta gestão e até mesmo a ausência da figura do gestor de segurança da informação que norteará as ações de segurança da informação nas instituições.

Brasil (2000) Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, tendo como objetivo dotá-los de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis. Para Castilho (2013) e Fontes (2012) a PoSIC é fundamental para padronizar a utilização de recursos e minimizar os prejuízos, protegendo adequadamente seus ativos, promovendo as ações necessárias à implementação e manutenção da segurança da informação.

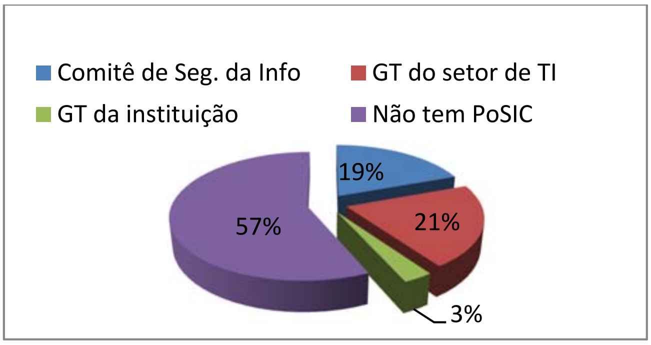
4.2 Planejamento e elaboração

Essa seção tem por objetivo apresentar as informações colhidas apenas nas 29 instituições que utilizam PoSIC de acordo com os números apresentados na Figura 4. Esses dados representam as práticas e os processos de segurança da informação, demonstrando o nível de maturidade ou conhecimento necessário para o planejamento e elaboração.

As instituições foram questionadas quanto a quem elaborou a PoSIC, ficando evidente que não há uma padronização ou prática definida para sua implementação. Segundo Coelho, Araújo e Bezerra (2014), a PoSIC deve ser desenvolvida, normalmente, pelo Comitê de Segurança da Informação. Brasil (2009) orienta que se institua um Grupo de Trabalho formado por pessoas de várias áreas, principalmente a área jurídica, TI e RH. Essa orientação deve-se ao fato de que os profissionais dos diferentes setores da instituição trazem para sua elaboração, informações nas diversas áreas do conhecimento para que o documento tenha sua abrangência além da área de Tecnologia da Informação.

É aconselhável que nesse grupo ou Comitê, estejam presentes pessoas que representem a área jurídica da instituição para o apoio e respaldo legislativo. Entretanto, o que se percebe é que as poucas instituições que possuem a PoSIC já instituída, ainda encontram-se divididas quanto a uma definição dos responsáveis por sua elaboração, ficando a cargo da alta gestão a orientação, aprovação e divulgação desse documento, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes (ABNT, 2013b). A Figura 5 mostra que apenas 19% das instituições tem a PoSIC elaborada pelo Comitê de Segurança da Informação, 3% por Grupo de Trabalho constituído por diversas áreas do instituição e 21% foi elaborado por Grupo de Trabalho composto apenas por profissionais de TI. Outros 57%, o equivalente a 38 instituições, não dispõe ainda de uma PoSIC.

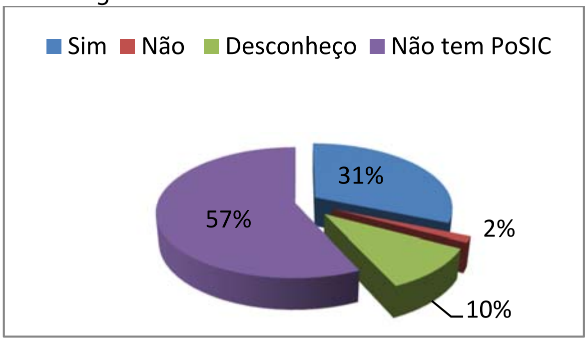
Figura 5 - Quem elaborou a PoSIC



Fonte: Elaborado pelos autores (2016).

Uma prática necessária para a implantação da PoSIC é construí-la alinhada ao Planejamento Estratégico Institucional (PEI). Ferreira e Araújo (2009, p. 36) relatam que ao se elaborar uma política “não podemos esquecer que ela expressa os anseios dos proprietários, responsáveis por decidir o destino de todos os recursos da organização em relação ao uso da informação por todos que tem acesso a este bem”. Entretanto, quando questionados se a PoSIC foi desenvolvida com base na PEI, 31% responderam positivamente, 10% desconhecem o objetivo desse documento e apenas 1% não tem sua PoSIC alinhada ao PEI. Outros 57% não fazem uso da PoSIC, conforme representado pela Figura 6.

Figura 6 - PoSIC alinhado ao PEI da IFES.



Fonte: Elaborado pelos autores (2016).

Um dos fatores de sucesso para a implantação de PoSIC em qualquer organização é obter o apoio da Alta Gestão em todas as etapas do processo. A Norma Internacional ABNT/NBR ISSO/IEC 27002:2013 (ABNT, 2013b), destaca todo um capítulo para tratar da categoria de controle da PoSIC e seu objetivo é prover orientação e apoio da direção para a segurança da informação, através do estabelecimento de uma PoSIC de forma clara e objetiva. Atendendo ao objetivo dessa Norma, foi questionado se a Alta Gestão participou dos processos de elaboração da PoSIC. A tabela 3 apresenta o cenário das instituições quanto ao envolvimento da Gestão máxima no processo de implantação da PoSIC.

Tabela 3 - Participação da Alta Gestão na implantação da PoSIC.

Sim Ativamente	**Sim. Parcial**	**Apenas Aprovou**	**Desconheço**	**Não tem PoSIC**
3%	16%	22%	2%	57%

Fonte: Elaborada pelos autores (2016).

O que se observa, além das poucas instituições que têm uma PoSIC, é que os gestores não participam diretamente das etapas de implantação da política. Apenas 02 (duas) instituições tiveram a participação ativa de seus gestores (3%). Isso equivale à participação nas reuniões, das avaliações e aprovações dos documentos gerados nos processos de implantação. Em 15 instituições, seus gestores não tiveram participação nenhuma (22%), apenas aprovaram o documento final, e outros 2%, equivalente a 01 (uma) instituição desconhecem a participação de seu gestor nesse processo de implantação. Tuyikeze e Pottas (2010) relatam que além do papel integrante da gestão para analisar e aprovar os projetos da política, o seu compromisso expressa apoio necessário para garantir uma comunicação adequada com toda a organização.

Os entrevistados foram questionados quanto a qual modelo de documentação a IFES seguiu para elaboração da PoSIC. Tuyikeze e Flowerday (2014, p. 12), dizem que, "devido a falta de orientação de desenvolvimento de PoSIC, desenvolvedores de políticas de segurança costumam usar fontes comercialmente disponíveis ou modelos disponíveis na internet, a fim de desenvolverem as suas políticas", fato esse comprovado na Tabela 4, onde 14 (quatorze) instituições (apenas 29 tem PoSIC institucionalizada) basearam a elaboração de sua política em outro modelo já disponibilizado por Brasil (2009) e 10 (dez) instituições copiaram de outras IFES.

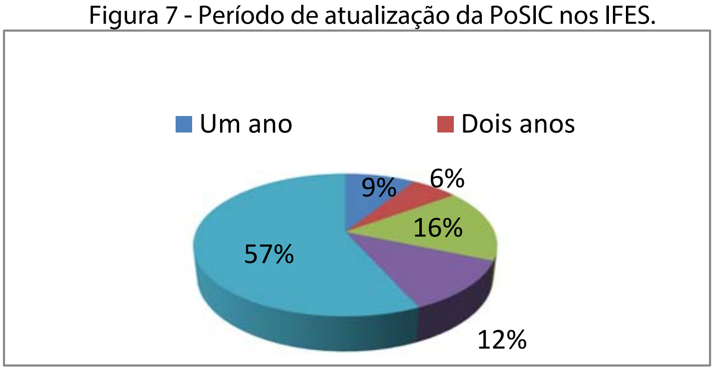
Tabela 5 - Modelo PoSIC utilizado nas instituições.

Modelo	**Quant**	**Percentagem**
Norma Complementar 03/IN01/DSIC/GSIPR	**14**	21%
Modelo de outra IES	**10**	15%
Outro órgão federal, estadual ou municipal	**3**	4%
Desconheço	**2**	3%
Não tem PoSIC	**38**	**57%**

Fonte: Elaborada pelos autores (2016).

Quando questionados quanto à prática e a periodicidade de atualização da PoSIC, a Figura 7 informa que 12% (08 instituições) desconhecem ou não atualizam a política no instituto, 16% (11 instituições) revisam o documento com período superior a 03 anos, apenas 6% (04 instituições) o fazem a cada 02 anos e 9% (06 instituições) o fazem anualmente. Das instituições que não sabiam o tempo de atualização da PoSIC somam 12% (08 instituições).

Figura 7 - Período de atualização da PoSIC nos IFES.



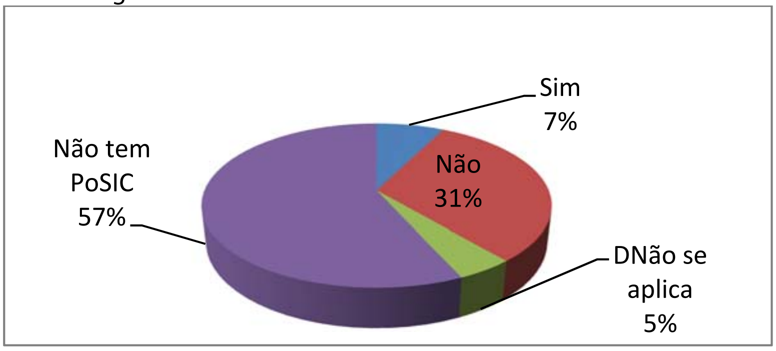
Fonte. Elaborada pelos autores (2016).

Ferreira e Araújo (2009), sugerem que a PoSIC seja atualizada no período de 06 meses a 02 anos. ISACA (2012) recomenda a atualização anualmente. Brasil (2009), diz que não pode exceder o prazo máximo de 03 anos. Essas atualizações são necessárias por que mudanças tecnológicas e humanas acontecem constantemente nos locais de trabalho e com isso as vulnerabilidades se tornam mais constantes.

4.3 Aprovação e Institucionalização

As instituições que afirmaram terem suas políticas já instituídas foram questionadas se foi criado, pelo Comitê de Segurança da Informação ou pelo Grupo de Trabalho, o Termo de Compromisso (ou TR – Termo de Responsabilidade) de uso da PoSIC. Esse documento apresenta a todos os servidores e usuários da instituição o apoio da Alta Gestão quanto ao cumprimento da PoSIC. A Figura 8 representa a situação das instituições com relação a esse documento. Apenas 05 instituições (7%) responderam ter esse documento assinado por sua gestão, 21 instituições (31%) não fazem uso do documento e outras 03 (5%) desconhecem a existência desse documento.

Figura 8 - Existência do Termo de uso da PoSIC da IFES.



Fonte: Elaborado pelos autores (2016).

Coelho, Araújo e Bezerra (2014) recomendam que a divulgação da PoSIC faça parte de programas de formação de funcionários novatos e de reciclagem dos antigos, além de ser divulgada periodicamente. Essa divulgação deve ser formal e efetiva, informando a todos, os detalhes de seu cumprimento e as penalidades, se for o caso, da sua não observância. A Tabela 6 mostra os meios de comunicação mais utilizados pelas IFES para divulgar a PoSIC. Para essa questão o respondente poderia utilizar mais de uma opção.

Tabela 6 - Meios de divulgação da PoSIC nas IFES

E-mail	Site da IFES	Quadro Aviso	Fórum	Outros	Não tem PoSIC
14	**27**	**0**	**1**	**1**	**38**

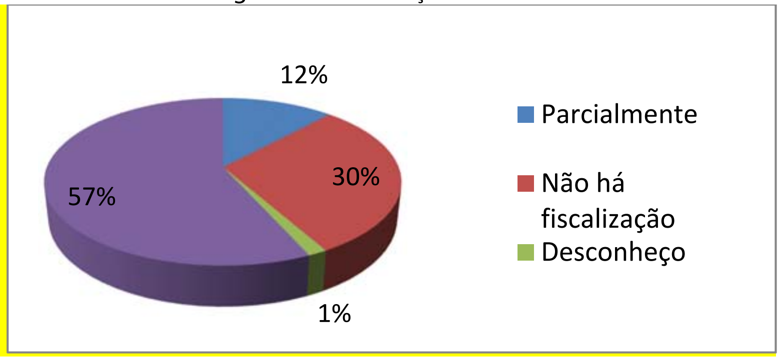
Fonte. Elaborada pelos autores (2016).

4.4 Conformidade e Penalidade

Todo processo de implantação de uma PoSIC, se bem elaborado, gera um documento que possibilita manter a segurança dos ativos e a continuidade do negócio, mantendo a disponibilidade, integridade, confiabilidade e autenticidade da informação. Entretanto, faz-se necessário exercer um processo de fiscalização, ou acompanhamento contínuo, de execução da PoSIC. Nesse quesito, as instituições foram questionadas quanto à sua realização, em periodicidade mínima de dois anos de fiscalização das práticas de segurança da informação em conformidade com o que determina a política.

Das instituições que têm sua PoSIC, apenas 08 instituições responderam que é realizado uma fiscalização periódica, porém o fazem de forma parcial. Esse acompanhamento parcial é realizado nas revisões das políticas, no momento das análises de risco em que os dados de criticidades e vulnerabilidades são apresentados pelas diversas áreas da instituição. A maioria das instituições afirmou não fazer nenhum tipo de acompanhamento. Apenas 01 (uma) instituição desconhece tal procedimento. A Figura 9 apresenta o cenário de cada instituição em relação a fiscalização para o cumprimento desse documento.

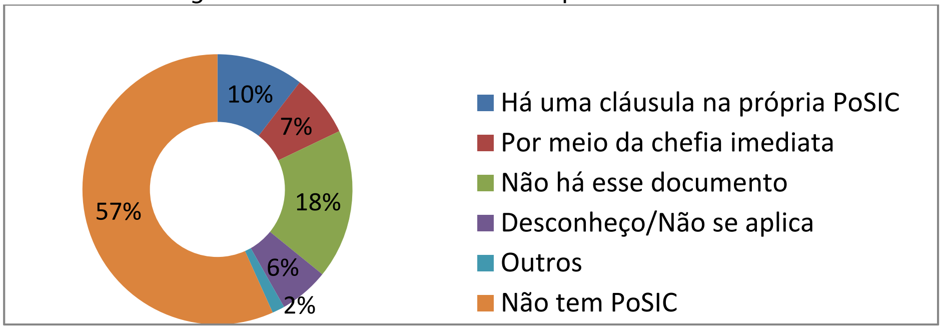
Figura 9 - Fiscalização da PoSIC.



Fonte: Elaborado pelos autores (2016).

É recomendado que tenha na própria PoSIC uma cláusula de aplicação de penalidades e, se for necessário, sanções previstas em lei quando da ocorrência de uma quebra de segurança ou da violação de alguma de suas diretrizes. Dessa forma, o usuário ao tomar conhecimento dessa cláusula, tornar-se-á inteiramente responsável pelo não cumprimento do documento. Contudo, ao questionar a forma como todos os usuários da instituição (servidores, terceirizados, alunos e prestadores de serviço) são comunicados sobre as penalidades em não cumprir com a PoSIC, a Figura 10 mostra uma realidade totalmente diferente do recomendado.

Figura 10 - Penalidade em não cumprimento da PoSCI.



Fonte: Elaborado pelos autores (2016).

Nessa questão, percebe-se que 07 instituições (10%) informaram que há uma cláusula na própria PoSIC que trata sobre as penalidades. Tais ações deverão ser devidamente apuradas e aos responsáveis serão aplicadas as sanções penais administrativas e civis em vigor. Outras 05 instituições (7%) declararam que o usuário é informado quanto às penalidades por meio de seu chefe imediato, 04 instituições (6%) desconhecem essa cláusula em sua política, 01 instituição (2%) informou, no campo "outro", que essa cláusula ainda está em fase de estudo, mas que será inclusa no próprio documento. A maioria dos institutos (18%) informou que não existe nenhum documento que trata de assuntos concernentes a penalidades ou de qualquer outra natureza que deixe os usuários cientes de seu cumprimento e penalidade legal. Esse item é composto por 12 instituições.

4.5 Fatores Críticos

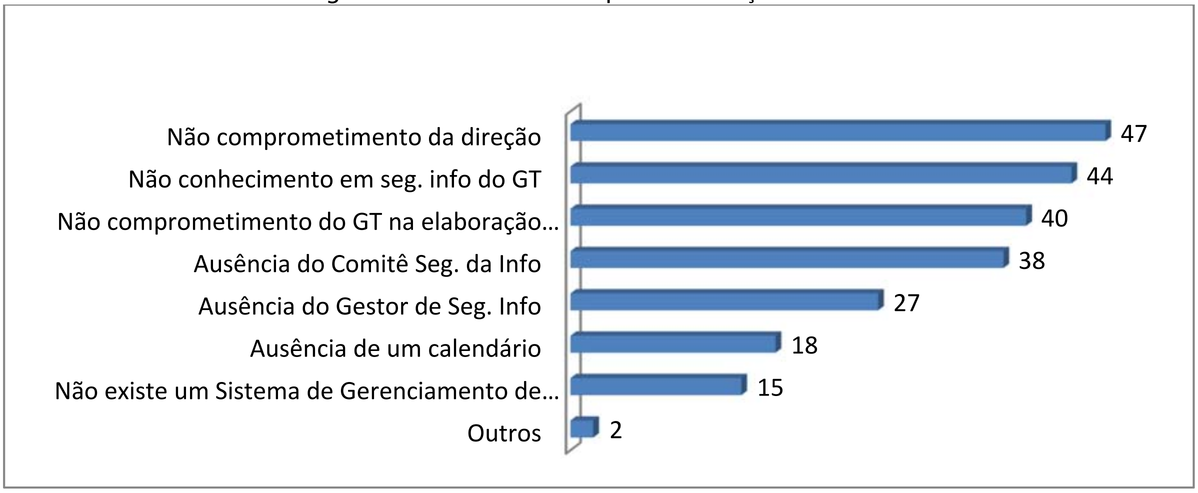
De acordo com o presente estudo, foram identificadas e propostas pelo pesquisador algumas práticas que podem ser consideradas como fatores críticos que prejudicam a implantação de PoSIC. Tais práticas forneceram subsídios importantes que permitiram identificar e elencar alguns fatores negativos que impedem o desenvolvimento, aprovação e institucionalização da política nos institutos.

Nessas três questões foi permitida aos respondentes a opção de múltipla escolha, identificando as práticas já realizadas na instituição. Para essas questões não foram utilizadas o método de porcentagem, pois as múltiplas escolhas ultrapassariam o quantitativo dos 100%, considerando as 67 instituições pesquisadas.

Analisando a Figura 11, fica claro que na opinião dos respondentes, o maior fator crítico para implantação de uma PoSIC nas IFES, com um total de 47 indicações, é a falta de comprometimento da sua Alta Gestão. Um estudo feito por Quintella e Branco (2013), mostra que o apoio da alta gestão está entre os 05 (cinco) maiores fatores críticos de sucesso para implantação de uma PoSIC. Instituições que não têm apoio da direção para sua elaboração, dificilmente terão sucesso em sua implantação, considerando que os demais fatores abordados na Figura 11 são altamente influenciados ou prejudicados pelo apoio ou não da Alta Gestão.

O segundo fator crítico identificado pela maioria dos respondentes, com 44 respostas é a falta de capacitação dos membros do Comitê de Segurança da Informação ou Grupo de Trabalho que desenvolvem a PoSIC terem pouco conhecimento em segurança da informação. Fica inviável construir um documento dessa natureza de não promover treinamento para as pessoas que a constroem.

Figura 11 - Fatores Críticos para elaboração de PoSIC nas IFES.



Fonte: Elaborado pelos autores (2016).

Falta comprometimento das pessoas que compõem o Grupo de trabalho - GT que elaboram a PoSIC foi o terceiro fator crítico mais escolhido com 40 indicações. Essa falta de comprometimento implica no desenvolvimento de práticas e ações nas etapas de implantação da PoSIC, o que pode ser mitigado com a definição de um calendário ou cronograma de atividades que viabilize a participação ativa de todos os membros do Comitê (ou GT). Demais fatores também foram selecionados, tais como: ausência de um Comitê de Segurança da Informação com 38 indicações, ausência do gestor de segurança da informação com 27 indicações e ausência de um cronograma para exercer as atividades de elaboração com 18 indicações.

Analisando os critérios selecionados pelos respondentes, o que se percebe é que o fator humano é a maior criticidade para o sucesso no planejamento da PoSIC, quer seja gerencial ou grupo de trabalho, quer seja capacitação técnica ou comprometimento no cronograma. Ferreira e Araújo (2009), dizem que mesmo existindo diversas tecnologias para a elaboração de uma PoSIC, o elemento humano é o fator fundamental para que a PoSIC seja implementada de forma eficaz.

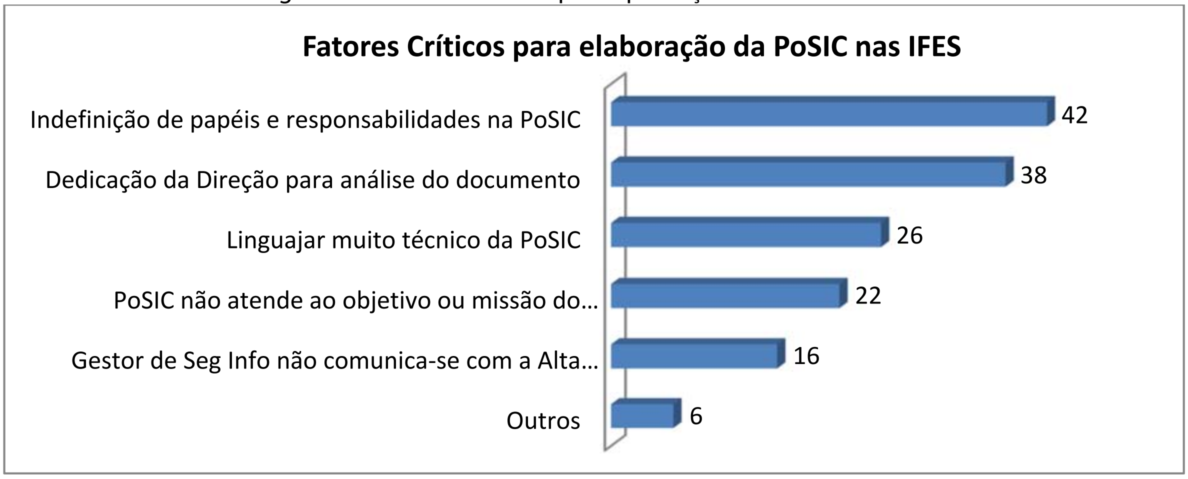
A fase de aprovação da PoSIC corresponde ao resultado positivo conseguido após a análise da proposta elaborada e apresentada à organização. Em particular exige-se o apoio por parte dos dirigentes da instituição como uma forma de garantir os primeiros passos para a implementação da PoSIC e as condições adequadas à sua manutenção (COELHO; ARAÚJO; BEZERRA, 2014).

Conforme é apresentado na Figura 12 o fator crítico de maior relevância para aprovação da PoSIC é a indefinição de papéis e responsabilidades. ABNT (2013b) orienta que esse documento tenha uma declaração relativa à atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação dos papéis definidos em cada ação especificada. O segundo maior fator crítico para aprovação está na dedicação da Alta Gestão para aprovação do documento com 38 indicações. Geralmente, nas Instituições de Ensino Federal, o órgão máximo superior que aprova a PoSIC é o CONSUP (Conselho Superior) da instituição, composto por servidores de diversas áreas da instituição. Solicitado pelo Gestor máximo da IFES, o CONSUP precisará compreender o conteúdo de todo o documento para sua aprovação. Vários critérios são analisados, tais como: simplicidade, objetividade e linguajar acessível a todo o público (interno e externo) a que se destina a política.

O terceiro maior fator crítico apontado pelos respondentes, com 26 indicações, está o linguajar muito técnico da PoSIC. O Grupo de Trabalho que elabora a PoSIC é composto, em sua maioria, por profissionais de TI, entretanto esses deverão entender que uma das práticas para a escrita da política está na clareza do texto para a fácil compreensão dos seus leitores, os quais abrangem pessoas dos mais diversos níveis de escolaridade dentro instituição e que - na maioria dos casos - não compreendem o linguajar técnico utilizado por seus desenvolvedores.

Outro fator apontado pelos respondentes foi a informação de que a PoSIC não atende ao Planejamento Estratégico Institucional. Esse critério recebeu 22 votos. O último fator crítico para aprovação da PoSIC foi a ausência de comunicação entre o gestor de segurança da informação com a Alta Gestão (podendo ser o Reitor ou seu designado para essa atribuição) com 16 votos. Todavia, independentemente do tamanho da instituição, a Alta Gestão deverá manter ampla comunicação com o gestor de segurança da informação durante as etapas de implantação da PoSIC. Outros fatores, não citados pelos respondentes, tiveram um indicativo de 6 votos.

Figura 12 - Fatores Críticos para aprovação de PoSIC nas IFES.



Fonte. Elaborado pelos autores (2016).

Organizações atuais precisam cumprir com as melhores práticas, detalhadas nos padrões de segurança da informação (SENGUPTA; MAZUMDAR; BAGCHI, 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 (ISACA, 2012). Agindo dessa forma, IFES podem implementar suas PoSIC de forma atender as práticas de gestão de segurança da informação no processo de implantação desse documento.

5 MELHORES PRÁTICAS

Muitas instituições de ensino têm adotado melhores práticas para implementar a segurança da informação em seus *campi*; outros tem adotado padrões internacionais como a ISO e outras instituições tem adotado padrões de órgãos nacionais. Algumas outras começam a implantar PoSIC porque as práticas de segurança da informação orientadas pelo COBIT, ITIL e a família ISO/IEC 27000 exigem a existência desse documento, uma vez que sigam esses modelos de gestão (FONTES, 2012).

Com isso, o uso de padrões e melhores práticas, como ITIL, COBIT e ISO/IEC 27002, estão sendo impulsionados por requisitos de negócios para melhorar o desempenho, a transparência e maior controle sobre as atividades de TI (IT GOVERNANCE INSTITUTE, 2008). 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 (ISACA, 2012).

Considerando as práticas apresentadas no estudo de campo apresentado nessa pesquisa e em conformidade com as práticas de gestão em segurança da informação para implantação de PoSIC recomendadas pelo *COBIT 5 for Information Security*, ITIL v3 e ISO/IEC 27002:2013, o quadro 1 apresenta a relação de algumas dessas práticas.

Quadro 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 estar 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 Seg. Info ou GT composto por pessoas de diversas áreas e setores da organização	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 segura e correta dos recursos e processamento da informação			X
32	Deve descrever as consequências do não cumprimento da PoSIC	X	X	X
33	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	Deverá ser aprovada pela Alta Direção	X	X	X

Fonte. Elaborado pelos autores e adaptado por ABNT (2013b), ISACA (2012), Tylor (2011).

6 CONCLUSÃO

Se em empresas privadas é um desafio fundamental para os lucros e para a sobrevivência do negócio resguardar as suas informações, a Administração Pública deve considerar a segurança da informação como um direito dos cidadãos, mantendo as informações íntegras e disponibilizando-as apenas àqueles que podem acessá-las no momento em que delas precisarem.

Considerando que há recomendações e orientações do Governo Federal para a institucionalização da PoSIC em todos os órgãos da APF, direta e indireta, compreendeu-se a necessidade de identificar o cenário em que também se encontram as IFES quanto à existência e as práticas que são utilizadas para implantação desse documento.

As IFES são organizações públicas que enfrentam o desafio de proteger suas informações, considerando que são ambientes onde há crescente complexidade, interconexões, incertezas e dependência da tecnologia, tendo ainda que realizar suas respectivas missões sem deixar de se submeter às normas e diretrizes provenientes dos órgãos centrais do governo federal. Dessa forma, precisam atender ao desafio da proteção tecnológica da informação, assim como atender aos anseios da educação quanto ao ensino, pesquisa e extensão.

Foi constatado nessa pesquisa que apenas 43% das IFES tem a PoSIC institucionalizada. Ficou evidente que tal situação preocupa o cenário de segurança da informação, pois é estrutural que as instituições tenham suas políticas de segurança para que o processo de proteção da informação possa ser elaborado e assegurado. A segurança da informação só poderá ser obtida a partir da implantação de um conjunto de controles adequados, o que inclui a presença de uma PoSIC, estabelecendo, implementando, monitorando e fiscalizando o que for necessário na instituição para que os objetivos e metas institucionais possam ser alcançados.

O reflexo dos dados apresentados por poucas instituições não terem sua PoSIC está relacionado à participação da alta gestão no processo de segurança da informação. Esse quadro reflete no principal fator crítico para elaboração de uma PoSIC, na visão dos respondentes.

Esse estudo buscou, por meio dessa pesquisa, compreender o nível de maturidade dos profissionais de segurança da informação na utilização de metodologias e práticas em segurança da informação e governança para o ambiente de tecnologia na elaboração de uma PoSIC clara e consistente. Esta necessidade deve-se a busca por padrões de mercado de TI em manter seus próprios modelos e estruturas de controle, uma vez que a evolução tecnológica e de governança criam constantes necessidades de atualizações e padrões internacionais que fornecem informações precisas para o planejamento e elaboração da PoSIC, integrada à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da instituição concernentes à segurança em geral.

Diante de todas as informações coletadas no estudo de campo, acredita-se que a elaboração de um documento padrão possa auxiliar as instituições de ensino a promoverem as etapas de levantamento, planejamento, desenvolvimento, execução e revisão da PoSIC 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 necessite utilizá-lo nas práticas e processos de sua manutenção e revisão.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**:2013. Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão da segurança da informação. Rio de Janeiro: ABNT, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **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, 2013b.

ALBUQUERQUE JUNIOR, Antonio Eduardo de; SANTOS, Ernani Marques dos. Adoção de medidas de Segurança da Informação: um modelo de análise para institutos de pesquisa públicos. **Revista Brasileira de Administração Científica**, v. 5, n. 2, p. 46-59, 2014.

ARAÚJO, Wagner Junqueira de. Leis, decretos e normas sobre Gestão da Segurança da Informação nos órgãos da Administração Pública Federal. **Informação & Sociedade: Estudos,** v. 22, Número Especial, p.13-24, 2012.

BRASIL. **Decreto nº 3.505 de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Casa Civil, Subchefia para Assuntos Jurídicos, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acessado em 11 dez. 2015.

BRASIL. Tribunal de Contas da União. **Levantamento acerca da Governança de Tecnologia da Informação na Administração Pública Federal**. Brasília: TCU, Secretaria de Fiscalização e Tecnologia da Informação. Sumário Executivo, 2008. 48 p. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2515176.PDF>. Acessado em: 14 dez. 2015.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **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. Brasília, DF, GSI/PR, 2009. 5 p. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf >. Acessado em: 11 dez. 2015.

BRASIL. Tribunal de Contas da União. **Levantamento de Governança de TI 2014**. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2015. 94 p. Disponível em: <http://portal3.tcu.gov.br/portal/pls/portal/docs/2705176.PDF>. Acessado em: 16 dez. 2015.

BRASIL. **Demanda TCU nº 265-54** [mensagem pessoal]. Mensagem recebida por no-replay@tcu.gov.br em 30 maio 2016.

CASTILHO, Sérgio Duque. Política de segurança da informação aplicada em uma instituição de ensino mediante análise de risco. **RETEC-Revista de Tecnologias**, v. 5, n. 2, p. 51-66, 2013.

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação NBR 27001 e NBR 27002**. Rio de Janeiro-RJ: RNP/ESR, 2014.

DZAZALI, Suhazimah; HUSSEIN Zolait, Ali. Assessment of information security maturity: an exploration study of Malaysian public service organizations. **Journal of Systems and Information Technology**, v. 14, n. 1, p. 23-57, 2012.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio T. **Política de segurança da informação**: guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2009.

FONTES, Edison. **Políticas e normas para segurança da informação.** Rio de janeiro: Brasport, 2012.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de Pesquisa**. Porto Alegre: UFRGS, 2009.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GIL, A. C. **Como Elaborar Projetos de Pesquisa.** 5. ed. São Paulo: Atlas, 2010.

ISACA. **COBIT 5 for Information Security**. (2012). Disponível em: www.isaca.org/cobit. Acesso em: 7 abr. 2017.

IT GOVERNANCE INSTITUTE. **COBIT, Aligning. 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit.** USA: IT Governance Institute, 2008.

KAUARK, Fabiana; MANHÃES, Fernanda Castro; MEDEIROS, Carlos Henrique. **Metodologia da pesquisa:** guia prático. Itabuna: Via Litterarum, 2010.

MONTEIRO, Iná Lúcia Cipriano de Oliveira. **Proposta de um Guia para elaboração de políticas de segurança da informação e comunicação em órgãos da APF**. Dissertação (Mestrado) - Universidade de Brasília. Brasília-DF, 2009.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do Trabalho Científico:** Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

QUINTELLA, Heitor Luiz Murat de Meirelles; BRANCO, Marcelo Pereira de Oliveira. Fatores Críticos de Sucesso em Segurança da Informação em Um Órgão da Administração Pública Federal. In: SIMPÓSIO NACIONAL DE INOVAÇÃO E SUSTENTABILIDADE (SINGEP), 2., 2013, São Paulo. **Anais do II SINGEP e I S2IS**. São Paulo: Uninove, 2013. p. 1-16.

SENGUPTA, Anirban; MAZUMDAR, Chandan; BAGCHI, Aditya. A Methodology for Conversion of Enterprise-Level Information Security Policies to Implementation-Level Policies/Rule. In: INTERNATIONAL CONFERENCE ON EMERGING APPLICATIONS OF INFORMATION TECHNOLOGY, 2., 2011, Kolkata. **Proceedings…** Kolkata, India: IEEE, 2011. p. 280-283.

TUYIKEZE, Tite.; POTTAS, Dalenca. An Information Security Policy Development Life Cycle. In: MULTI-CONFERENCE SEISMC, 2010, Port Elizabeth. **Proceedings of the South African Information Security**. Port Elizabeth: ISSA, 2010. p. 165-176.

TUYIKEZE, Tite; FLOWERDAY, Stephen. Information Security Policy Development and Implementation: A Content Analysis Approach. In: INTERNATIONAL SYMPOSIUM ON HUMAN ASPECTS OF INFORMATION SECURITY & ASSURANCE, 8., 2014. **Proceedings…** East London, South Africa: Nelson Mandela Metropolitan University, 2014. p. 11-20.

TAYLOR, Sharon. **ITIL:** Service Design. Best management Pratice. London: TSO The Stationary, 2011.

VEIGA, Adele Da. The Influence of Information Security Policies on Information Security Culture: Illustrated through a Case Study. In: INTERNATIONAL SYMPOSIUM ON HUMAN ASPECTS OF INFORMATION SECURITY & ASSURANCE, 9., 2015. **Proceedings**… Lesvos, Greece: University of Plymouth, 2015. p. 11-20.