2743 - ASPECTOS DISTINTOS E CONCOMITANTES DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO NAS INSTITUIÇÕES FEDERAIS DE ENSINO SUPERIOR

AUTORIA

Hudson Augusto Silva de Castro

hud_augusto@yahoo.com.br

Universidade Federal do Pará – UFPA

Wesley Igor Paixão Piedade

profhudsoncastro@gmail.com

Faculdade Paraense de Ensino – FAPEN

Cristiano Descovi Schimith

cristiano.schimith@gmail.com

Universidade Federal do Pará – UFPA

Sabrina Bianca da Silva Alves

brina.biancs@gmail.com

Universidade Federal do Pará – UFPA

RESUMO

A Política de Segurança da Informação e Comunicação (PoSIC) é um sistema de política privativa de instituições públicas e privadas, tem objetivo protetivo em relação aos dados das organizações. Tendo em vista que as universidades são geradoras de informações e são fomentadoras de conhecimento, questiona-se se as Universidades Federais do Estado do Pará possuem uma Política de Segurança da Informação e Comunicação e, sobretudo, quais as similaridades e distinções existentes entre as PoSICs destas instituições. Neste sentido, o objetivo da pesquisa é verificar as características qualitativas das PoSICs nas instituições federais de ensino superior. Como principal resultado observou-se que apesar de todas possuírem uma Política de Segurança da Informação e Comunicação, elas não possuem todos os requisitos básicos apontados pela literatura existente acerca do tema.

Palavras-chave: PoSIC. Segurança da Informação. Segurança de dados. Gestão da informação.

Eixo Temático 1: Inovações e Diversidades na Gestão Pública

1 INTRODUÇÃO

A administração pública rege direitos e prerrogativas no âmbito público, com ações diretas e indiretas.

Conforme previsto no Art. 37 da Constituição Federal de 1988, no que tange e envolve a administração pública sobre o princípio da legalidade, o administrador público, em sua função, só pode fazer algo em virtude da lei, a qual ampara suas decisões e ações, ou a falta delas (BRASIL, 2015).

Documentos e dados legislativos devem ser periodicamente avaliados pela direção e administração em conformidade com as normas vigentes, os manuais que estabelecem procedimentos e de suas legislações de sistema da informação e comunicação, sempre buscando se testificar com relação ao atendimento de segurança e requisitos da comunicação e informação (BRASIL, 2015).

Com o controle de acesso, são elaboradas normas que estabelecem processos, procedimentos e mecanismos que garantem de forma controlável o acesso às informações e instalações de sistemas de informações (BRASIL, 2015).

Essas medidas possuem como objetivo a proteção, segurança e prevenção de dados, para que não ocorram vazamentos de informações sigilosas e não comprometam a administração pública (BRASIL, 2015).

A PoSIC (Política de Segurança da Informação e Comunicação) é um sistema de política privativa de instituições públicas e privadas. Criada para a inclusão de políticas das informações e comunicações que objetivem proteger e assegurar os dados das organizações.

O Tribunal de Contas da União (TCU) e a Secretaria de Fiscalização de TI (SEFIT) realizaram em 2013 e 2016 uma pesquisa auto avaliativa com pouco mais de 500 entidades públicas federais com o objetivo de obter informações sobre governança pública e de gestão de TI (LEAL, 2019). Esse levantamento apontou que cerca de 16% das entidades e órgãos federais não possuem uma PoSIC.

As universidades, de forma geral, são geradoras de informações e são fomentadoras de conhecimento. Nesse cenário, conforme disposto na Lei nº 11.892, criada no dia 29 de dezembro de 2008, os reitores das universidades federais têm como atribuições reduzir as vulnerabilidades das instituições de ensino, estar à frente das ameaças, reduzir a exposição aos riscos e diminuir os impactos associados aos ativos da organização. Além disso, deverão estabelecer um processo que tenha por objetivo identificar, quantificar, priorizar, tratar, comunicar e monitorar os riscos físicos e virtuais.

Ao se observar o desafio em gerir a segurança de suas informações, questiona-se se as Universidades Federais do Estado do Pará possuem uma Política de Segurança da Informação e Comunicação e, sobretudo, quais as similaridades e distinções existentes entre as PoSICs destas instituições.

Assim sendo, o objetivo desta pesquisa é investigar quais as características similares e distintas das Políticas de Segurança da Informação e Comunicação nas instituições federais de ensino superior.

Para o alcance do objetivo foi realizada uma pesquisa exploratória, de cunho qualitativo, em instituições de ensino superior do estado do Pará. Como principal resultado observou-se que apesar de todas possuírem uma Política de Segurança da Informação e Comunicação, elas não possuem todos os requisitos básicos apontados pela literatura existente acerca do tema.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Os órgãos públicos e privados necessitam de uma boa comunicação para andarem lado a lado com a sociedade (AMARAL, 2016). Esse caminhar possibilita melhorias no desempenho das organizações e obtenção estratégica de informações para alcançar os

objetivos traçados (AMARAL, 2016). Contudo, as instituições públicas enfrentam diversos desafios concernentes ao cenário de incertezas, interconexões entre os mais diversos setores, dependência financeira e tecnológica, adaptações e necessidade de inovações, submissões a regramentos governamentais além de realizar planos organizacionais com o intuito do alcance de suas respectivas missões (RIOS, *et al.*, 2017).

Quando tratado o tema segurança da informação e os acontecimentos que afetam tal segurança, surgiu a Norma Complementar 05/IN01/DSIC/GSIPR (Brasil, 2009), promovida pelo órgão responsável por normatizar a segurança da informação no estado brasileiro, onde esta traz a definição para incidente de segurança que em síntese trata de um evento relacionado à segurança dos sistemas de computação, podendo ter sido confirmado ou apenas suspeito.

Segundo TCU (2021) as falhas da gestão da segurança da Informação trazem riscos tais como "a perda da integridade de dados públicos e pessoais, a indisponibilidade de serviços públicos, o vazamento de informações sigilosas, a invasão da privacidade do cidadão e, inclusive, vultosas perdas financeiras".

Com o desenvolvimento tecnológico, as informações têm se espalhado rapidamente e tem ameaçado órgãos públicos e privados, seja espalhando notícias falsas ou vazando dados, contas privadas e informações sigilosas (AMARAL, 2016).

Com as ondas de ataques cibernéticos, os órgãos federais tiveram que se adaptar aos ataques contemporâneos de hackers, que podem destruir todo um sistema de proteção e armazenamento (AMARAL, 2016).

Ao identificar os desafios que são enfrentados no setor público, sobretudo os que dizem respeito à segurança de informações, pode-se dizer que, de forma geral, são os mesmos causados nas empresas de rede privada (CASTRO, 2015). São eles a aceleração da evolução das ameaças tecnológicas, a alta complexidade dos ataques, a dificuldade em detectar esses incidentes de forma mais ágeis e a diminuição do tempo de reação para esses ataques (CASTRO, 2015).

No entanto, os órgãos governamentais têm a facilidade de serem alvos de forma mais frequente (CASTRO, 2015). Assim sendo, vê-se como necessária a presença de uma

segurança efetiva para garantir o cuidado de documentos, senhas e dados pessoais que estejam de posse das instituições, seja de forma física ou virtual (CASTRO, 2015).

A demanda por segurança é cada vez mais alta e a exposição de riscos está em toda parte; esses ataques podem vir tanto de fora, quanto de dentro da própria instituição. Para salvaguardar dados privados de forma segura, as organizações públicas têm buscado melhorias de segurança de dados em nuvens computacionais (CASTRO, 2015).

Através de estudos que envolvem a prevenção de dados e pesquisas de campo e investigações para uma melhor proteção cibernética, o governo brasileiro buscou tomar atitudes para salvaguardar as informações. Deste modo, em 2000, por meio do Decreto 3.505 foi instituída a Política de Segurança da Informação e Comunicação (PoSIC), que possuía com premissa a prevenção de ataques aos bancos de dados dos órgãos públicos federais (BRAGA *et al*., 2014). No decorrer do tempo e a partir dos avanços tecnológicos, o governo necessita realizar constantes adaptações nas regulamentações pertinentes ao assunto. Deste modo, em 2018 o Decreto 9.637 revoga o decreto de 2000 que passa a instituir a Política Nacional de Segurança da Informação (PNSI) que trouxe inovações em relação ao desenvolvimento de estratégias de segurança cibernética. O sucesso da implantação da política de segurança da informação depende da participação de todos aqueles que fazem parte da instituição (BRAGA *et al*., 2014).

Em relação à sua implementação, primeiro deve-se identificar os requisitos corporativos da Política de Segurança da Informação para uma possível definição de padrões para documentação da política (BRAGA *et al*., 2014). Neste momento é realizada a hierarquização de documentos de Segurança da Informação que estão sendo incluídas ou que estão sendo criadas e, logo após, são relacionados conforme o risco da segurança (BRAGA *et al*., 2014).

A hierarquia existente tem como objetivo estabelecer quais documentos e dados estão disponíveis e em quais momentos e casos eles podem ser aplicados e para quem (BRAGA *et al*., 2014).

A administração deve aprovar a PoSIC para a garantia da segurança e do direito individual e coletivo das pessoas. Ademais, com a sua aprovação, o sigilo da

correspondência e também das comunicações que está previsto na Constituição Federal de 1988, passa a ser garantido (BRAGA *et al*., 2014). Esta é a segunda etapa, momento este em que é garantido o provisionamento de recursos para a implementação da PoSIC.

Desenvolvida e aprovada, a terceira etapa é a implementação que tem como objetivo promover comportamentos culturais e avaliações de Segurança da Informação e Comunicação, sensibilizando, conscientizando, capacitando e especializando servidores públicos e colaboradores internos, além de fomentar a divulgação da PoSIC a todos os colaboradores, usuários, prestadores de serviços e terceirizados (BRAGA *et al*., 2014).

Avaliar se a PoSIC possui conformidade e sustentabilidade, bem como realizar ações corretivas no caso de não conformidade, faz parte da quarta etapa. Aqui é dada a devida proteção a assuntos que merecem tratamentos especiais e capacitação dos segmentos de procedimentos autênticos que devem ser estabelecidos, e dessa forma decidir as exigências de determinação de conformidades não potencias, e quais suas causas (BRAGA *et al*., 2014).

A quinta etapa diz respeito à manutenção de mentalidade de Segurança de Informação e Comunicação, sendo esta revista de forma periódica (BRAGA *et al*., 2014).

A divulgação de informação é a última etapa. Nela torna-se público os conhecimentos gerados ou organizados pela instituição (BRAGA *et al*., 2014). A noção de divulgação pode ser comumente interpretada como equivalente à difusão ou mesmo à disseminação de informações (BRAGA *et al*., 2014).

Atualmente, a segurança da informação tem sido debatida constantemente e vem se tornando um motivo de preocupação cada vez maior para as empresas em todos os seguimentos (LEAL, 2019; DANTAS, 2011).

Tal segurança deve envolver não somente as pessoas que estão ligadas à instituição, como também os sistemas e processos, o que faz com que seja necessária a criação de mecanismos normativos cujas diretrizes e regras estejam envolvidas em um único documento, o que auxilia as organizações nas questões relativas à segurança das suas informações (LEAL, 2019; DANTAS, 2011).

Os itens presentes nas PoSICs precisam ser cumpridos de forma íntegra por todos aqueles que estão direta ou indiretamente ligados às instituições (LEAL, 2019). Caso haja transgressões às políticas implantadas, a PoSIC deve prever sanções que podem estar presentes em outros documentos, como leis, regulamentos internos ou em contratos de trabalho (LEAL, 2019).

A PoSIC deve orientar a forma a qual as pessoas que estão envolvidas na organização irão agir, de maneira a assegurar a proteção das informações empresariais frente a todo tipo de ameaça e risco (LEAL, 2019; DANTAS, 2011).

Espera-se que a cobertura das ameaças virtuais, digitais e físicas supram as expectativas das instituições, exigindo um grau elevado de cobertura em plataformas digitais e capacitação física para um suposto sinistro (TCU, 2012).

A confidencialidade é entendida como a proteção das informações contra acessos não autorizados (SPANCESKI, 2004). Deve-se impedir que os dados sejam excluídos e/ou alterados sem que haja a autorização para fazê-lo (SPANCESKI, 2004). Entretanto, deve haver disponibilidade de informações sempre que solicitada (SPANCESKI, 2004). Assim sendo, garantir a integridade de informações alinhada com a sua disponibilidade é uma tarefa árdua, visto que ao passo que as tecnologias se desenvolvem, novos tipos de ameaças surgem (SPANCESKI, 2004).

É importante prevenir com que dados sigilosos sejam expostos, ou seja, deve-se garantir que eles estejam acessíveis somente às pessoas autorizadas (LEAL, 2019; DANTAS, 2011). Um vazamento de informação pode causar a exposição de profissionais, colaboradores externos e estagiários, por exemplo (LEAL, 2019; DANTAS, 2011).

Como forma de prevenir acessos de terceiros não autorizados, empresas públicas e privadas têm adotado mecanismos de controle baseados em sensores de proximidade, leitores de biometria e reconhecimento de face, o que reduzem as vulnerabilidades (LEITE, 2011).

Sobre a divulgação de informações não autorizadas, a engenharia social representa uma das maiores ameaças para as organizações que trabalham para a proteção

das informações (LEAL, 2019; CHIMENDES *et al.*, 2012). Ela é o ato de manipulação de uma possível "vítima", induzindo-a a fornecer as informações acerca da empresa onde trabalha (LEAL, 2019; CHIMENDES *et al.*, 2012).

A engenharia social por muitas vezes passa despercebida por muitas pessoas, deixando-as vulneráveis ao agressor (engenheiro social). Com isso elas acabam adquirindo confiança e se tornando alvo frágil, fácil, vulnerável e manipulável (LEAL, 2019; CHIMENDES *et al.*, 2012).

Ademais, a política de "mesa limpa" contribui para a não divulgação de dados sigilosos, visto que seu principal objetivo é implementar diretrizes que minimizam os riscos de violação de segurança, fraude e roubo de informações que são causadas por documentos que estão sendo esquecidos nas instalações das empresas sem as proteções necessárias (LEAL, 2019).

Apesar dos riscos de acessos, a Política de Segurança da Informação e Comunicação não tem como objetivo conter apenas acessos não autorizados aos dados institucionais, elas se posicionam de forma proativa à prevenção de ameaças virtuais, digitais e físicas, mantendo o caráter e o respeito das instituições (TCU, 2012).

Em relação ao teor das PoSICs, Leal (2019) afirma que devem tratar, dentre outros temas, acerca da utilização de dispositivos móveis para manter as Políticas de Segurança da Informação e Comunicação sempre em alerta, pois os dispositivos móveis podem ser roubados ou furtados acarretando possíveis esquemas fraudulentos de acesso ás informações sigilosas, por exemplo.

Em seu texto, a literatura aponta que tanto as empresas públicas quanto as privadas precisam possuir em suas PoSICs três pilares considerados básicos, que são confidencialidade, integridade e disponibilidade (CAMPOS, 2007).

Vê-se a necessidade de uma revisão periódica da PoSIC, o que garante a segurança das informações nas organizações frente às novas ameaças advindas do frequente desenvolvimento tecnológico (CARDOSO; OLIVEIRA, 2013). O Comitê de Segurança da Informação e Comunicação busca continuamente pela melhoria interna dos atos administrativos, o que inclui a revisão periódica da PoSIC, apontando para importância

da existência do mesmo (INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL - IPHAN, 2013).

É importante a utilização dos correios eletrônicos no sentido de oferecer um meio de transferência e compartilhamento de arquivos remotos, o que possibilita a interatividade entre instituições e servidores (CENTRO DE ESTUDOS DE TÉCNICAS DE TECNOLOGIA E SEGURANÇA, 2013). Entretanto, mecanismos devem ser implantados para que essa troca de informações ocorra de forma segura (CENTRO DE ESTUDOS DE TÉCNICAS DE TECNOLOGIA E SEGURANÇA, 2013).

Frente ao volume de informações geradas, faz-se necessário classificá-las de acordo com suas prioridades, importância e nível de proteção (LEAL, 2019). Para as empresas privadas, as informações podem ser classificadas como pública, interna, confidencial e restrita, já para os órgãos públicos devem seguir a Lei de Acesso à Informação (LAI) que classifica as informações como ultrassecretas, secretas, reservadas e públicas (LEAL, 2019).

Ainda em relação ao volume de informações, torna-se necessária a realização de backup, estando a sua periodicidade e procedimentos bem definidos para que seja possível restaurar informações perdidas e recuperar informações empresariais excluídas (LEAL, 2019).

O termo de responsabilidade é um documento que é usado para informar o colaborador de maneira clara e precisa de que ele está sujeito a todas as normas e políticas da empresa (LEAL, 2019). Com a assinatura do mesmo, ele declara ciência da leitura, e que compreendeu e entendeu todos os itens descritos no termo, declarando assim a sua responsabilidade (LEAL, 2019).

2 METODOLOGIA

Com o intuito de investigar quais as características similares e distintas das Políticas de Segurança da Informação e Comunicação nas instituições federais de ensino superior, foi realizada uma pesquisa exploratória nas cinco instituições federais de ensino superior presentes no estado do Pará. O referido estado foi escolhido partindo-se do

pressuposto que o geral é reflexo do local, e o estado do Pará é o local onde a pesquisa foi realizada.

Foram encontradas as PoSICs da Universidade Federal do Pará (UFPA), Universidade Federal do Oeste do Pará (UFOPA), Universidade Federal Rural do Amazônia (UFRA), Universidade Federal do Sul e Sudeste do Pará (UNIFESSPA) e do Instituto Federal de Educação, Ciência e Tecnologia do Pará (IFPA).

A pesquisa, caracterizada como qualitativa, teve sua coleta de dados baseada nos pontos básicos apontados pela literatura acerca da Política de Segurança da Informação e Comunicação.

Os resultados obtidos podem ser observados no Quadro 1 a seguir.

Quadro 1: Características das PoSICs das Instituições Federais de Ensino Superior do Estado do Pará.

	UFPA	**UFOPA**	**UFRA**	**UNIFESSPA**	**IFPA**
Possui os três pilares básicos: confidencialidade, integridade e disponibilidade (CAMPOS, 2007)	Não	Sim	Sim	Sim	Não
Existência de um Comitê de Segurança da Informação (IPHAN, 2013)	Sim	Sim	Sim*	Sim**	Sim
Trata de normas acerca da utilização de correio eletrônico (CENTRO DE ESTUDOS DE TÉCNICAS DE TECNOLOGIA E SEGURANÇA, 2013)	Não	Sim	Não***	Não	Não
Trata sobre a proteção das informações contra acessos não autorizados (SPANCESKI, 2004)	Sim	Sim	Sim	Sim	Sim
Faz a cobertura de qualquer tipo de ameaça, seja ela virtual, digital e/ou física (TCU, 2012)	Sim	Sim	Sim	Sim	Sim
Aponta para a colaboração e participação de todos os funcionários, estagiários e prestadores de serviços externos no que diz respeito à	Sim	Sim	Sim	Sim	Sim

segurança de informações (LEAL, 2019; DANTAS, 2011)					
Há uma revisão periódica da PoSIC (CARDOSO; OLIVEIRA, 2013)	Sim	Sim	Sim	Sim	Sim
Tem definida uma rotina de backup (LEAL, 2019)	Não	Sim	Não	Não	Não
Orienta os colaboradores acerca da "mesa limpa" (LEAL, 2019)	Não	Sim	Não	Não	Não
Estabelece sanções em caso de transgressão às normas e condutas praticadas pelos colaboradores (LEAL, 2019)	Sim	Sim	Sim	Sim	Sim
Cita o termo de responsabilidade (LEAL, 2019)	Sim	Sim	Não	Sim	Sim
Classifica a informação como ultrassecreta, secreta, reservada e pública (LEAL, 2019)	Não	Não	Não	Não	Não
Estabelece normas acerca da utilização de dispositivos móveis (LEAL, 2019)	Sim	Sim****	Não	Não	Não
Orienta acerca da Engenharia Social (LEAL, 2019; CHIMENDES *et al.*, 2012)	Não	Sim	Não	Não	Não

Fonte: Dados da pesquisa.

*É constituído pelo Comitê Executivo de TI. **Chamado de Comitê de Governança Digital. ***Apenas cita que devem ser criadas normas. ****De forma parcial, visto que aborda apenas dispositivos móveis tombados.

ANÁLISE DE DADOS

Percebeu-se que apenas três das instituições analisadas possuem os pilares apontados pela literatura (CAMPOS, 2007). O que demonstra que 60% das instituições pesquisadas possuem preocupações em relação à presença de princípios em suas Políticas de Segurança de Informação e Comunicação.

Foi verificada a presença de outros pilares. O pilar que se mostrou comum em todas as PoSICs foi o da autenticidade, que é o pilar que está ligado à informação não

adaptada e divulgada sem mudanças, o que contribui para uma maior credibilidade da informação divulgada.

Nas instituições pesquisadas observou-se que todas possuem um comitê que tem como objetivo apontar o que é necessário para as melhorias em relação às PoSICs. Isso pode significar que todas têm a preocupação de manter seus comitês de segurança sempre atentos e seguros (IPHAN, 2013).

Em algumas instituições os comitês são conhecidos como Comitê Executivo de TI e Comitê de Governança Digital.

Foi identificado que apenas uma das instituições cita em sua PoSIC a utilização de correios eletrônicos. O que aponta para uma preocupação, por parte desta instituição, em salvaguardar seus dados (CENTRO DE ESTUDOS DE TÉCNICAS DE TECNOLOGIA E SEGURANÇA, 2013). Contudo, questiona-se o motivo do tema não ser citado nas outras PoSICs.

Foi encontrado que as instituições de ensino possuem controles específicos como a biometria e a utilização de senhas, o que diminuem a vulnerabilidade dos dados dos profissionais, de terceiros e também de visitantes (LEAL, 2019; DANTAS, 2011; LEITE, 2011). Desta forma, os comitês de segurança de informação conseguem trabalhar de maneira segura, obtendo informações corretas e alcançando o objetivo de prevenção contra os ataques e sequestro de dados (LEAL, 2019; DANTAS, 2011; LEITE, 2011).

Foi observado, também, que as instituições presentes nesta pesquisa utilizam de nuvens computacionais e antivírus com o intuito de proteger seus dados, dificultando acessos não autorizados aos mesmos (SPANCESKI, 2004).

Uma das ameaças virtuais que foram apontadas nas PoSICs pesquisadas e que têm sido utilizadas na tentativa de prejudicar as instituições federais, são as nuvens computacionais chamadas de *Malware* que podem ser usadas para invadir sistemas digitais e computacionais mudando os códigos e senhas de acesso, dificultando, assim, a recuperação de documentos e dados importantes (LEAL, 2019; DANTAS, 2011).

Foi observado que as PoSICs estabelecem normas, regras e diretrizes para proteger as pessoas e o sistema interno das instituições federais de ensino superior.

Também foram implementadas nestes sistemas procedimentos que pudessem penalizar quem tentasse invadir o sistema computacional. Ademais, aponta que o constante envolvimento daqueles que fazem parte da instituição é fator essencial para a implantação de uma Política de Segurança da Informação e Comunicação de forma eficiente, eficaz e sustentável.

Nesse ponto foi observado que existem sanções em casos de contravenções cometidos pelas condutas exercidas pelos trabalhadores em todas as instituições pesquisadas, exceto na UFRA. O que indica uma fragilidade de implantação da PoSIC, visto que a não previsão de sanções pode trazer menor credibilidade à política de segurança, ocasionando em seu não cumprimento (LEAL, 2019).

Observou-se que todas as instituições pesquisadas fazem revisões periódicas das PoSICs, o que prevê situações que podem fugir do controle (CARDOSO; OLIVEIRA, 2013).

Todas as instituições fazem revisões no mínimo uma vez ao ano. Com exceção do IFPA, que realiza sua revisão no mínimo uma vez a cada cinco anos. Trazendo o questionamento se sua PoSIC está atualizada em relação às novas tecnologias e ameaças.

Foram analisados e encontrados que as PoSIcs das Instituições Federais de Ensino Superior do Pará, com exceção da UFOPA, não possuem uma normativa que estabelece normas e diretrizes para a manutenção e restauração de cópias de segurança (backup), o que aponta para uma fragilidade na proteção de seus dados (LEAL, 2019).

Foi identificado que apenas a Universidade Federal do Oeste do Pará orienta, em sua PoSIC, os seus colaboradores acerca da “mesa limpa”, indicando uma preocupação da instituição em preservar seus documentos físicos (LEAL, 2019).

Foi encontrada em todas as PoSICs analisadas citação ao termo de responsabilidade, exceto na UFRA. O que leva ao questionamento de como a PoSIC é vista pelos colaboradores, uma vez que a ausência da previsão de sanções frente a atos transgressores e a não menção ao termo de responsabilidade na Política de Segurança da Informação e Comunicação pode indicar uma não obrigatoriedade à Política (LEAL, 2019).

Em nenhuma PoSIC analisada as informações foram classificadas de acordo com a LAI. O que aponta para o não cumprimento da legislação. Contudo, questiona-se como as informações estão sendo classificadas, se elas são classificadas e, caso haja classificação, o motivo dessa classificação não estar presente em suas PoSICs.

Em relação à citação de normas que tratem acerca de dispositivos móveis, apenas em duas PoSICs encontrou-se citações. Dessas duas, uma aborda de forma direta e total enquanto a outra de forma parcial, visto que aborda apenas dispositivos móveis tombados.

Nas PoSICs analisadas foi identificado que apenas a UFOPA realiza orientações aos seus funcionários e colaboradores internos e externos, no sentido de realizarem comentários e fornecerem informações das instituições para pessoas que não estejam ligadas à instituição. O que indica uma preocupação da Universidade em preservar os dados somente àqueles que deles possuem autorização para a posse (LEAL, 2019; CHIMENDES *et al.*, 2012).

3 CONCLUSÃO

Considerando que existem diversas regras impostas pelo governo brasileiro no que diz respeito a implantação e fiscalização de Políticas de Segurança da Informação no âmbito da administração pública federal, notou-se a necessidade de realizar um estudo dentro das instituições federais de ensino superior com o objetivo de investigar quais as características similares e distintas das Políticas nelas instituídas.

As IFES precisam atender ao desafio da proteção tecnológica da informação, em meio aos mais diversos cenários nos quais estão inseridas, bem como superar desafios da educação pública de qualidade promovendo um ambiente de inovação e tecnologia. Verificou-se que apesar de a literatura existente sobre o tema apontar pontos vistos como básicos para a elaboração de uma PoSIC, as instituições pesquisadas não atendem em sua totalidade, e o principal questionamento é o motivo para o não cumprimento.

Para o alcance do objetivo da pesquisa foi feita uma análise das PoSICs sob a ótica da literatura existente. Entrevistas com os membros das instituições não se mostrou como necessária. Contudo, frente aos resultados obtidos, sugere-se que, em trabalhos futuros,

tais entrevistas ocorram e sejam encontradas significações para as ausências aqui apontadas.

Não obstante, a necessidade de mensurar a eficácia da implantação das PoSICs se mostra como relevante, visto que a falta de determinados pontos, como a previsão de sanções, a referência ao termo de responsabilidade e a ausência de princípios básicos, pode dar às PoSICs um caráter de não obrigatoriedade.

REFERÊNCIAS

AMARAL, F. **Introdução à Ciência de Dados: mineração de dados e big data**. Rio de Janeiro: Alta Books, 2016.

BRAGA, L. V.; ALVES, W. S.; FIGUEIREDO, R. M. da C.; SANTOS, R. R. dos. O papel do Governo Eletrônico no fortalecimento da governança do setor público. **Revista do Serviço Público**, *[S. l.]*, v. 59, n. 1, p. p. 05-21, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Estratégia de Segurança da Informação e Comunicações e de Segurança cibernética da Administração Pública Federal**, 2015.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Norma Complementar nº 05/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.

CAMPOS, A. **Sistemas de Segurança da Informação.** 2. ed. Florianópolis: Visual Books, 2007.

CARDOSO, F. E.; OLIVEIRA, P. C. de. Política de Segurança da Informação nas empresas. [S.l: s.n], 2013. Disponível em: https://s.profissionaisti.com.br/wp-content/uploads/2013/06/Politica-de-Seguran%C3%A7a-nas-Empresas.pdf. Acesso em: 26 de outubro de 2020.

CASTRO, C. S. **Direito da Informática, Privacidade e Dados Pessoais.** Coimbra: Almedina, 2015.

CENTRO DE ESTUDOS DE TÉCNICAS DE TECNOLOGIA E SEGURANÇA - CE. **Tecnologia da Informação: técnicas de segurança: código de prática para controles de segurança da informação**. [S.l: s.n], 2013.

CHIMENDES, V. C. G. *et al*. Engenharia Social: o elo mais frágil da segurança nas empresas. **Revista Eletrônica do Alto Vale do Itajaí**, n. 2, 2012.

DANTAS, M. L. **Segurança da informação: uma abordagem focada em gestão de risco.** Olinda: Livro Rápido, 2011.

INSTITUTO DO PATRIMÔNIO HISTÓRICO E ARTÍSTICO NACIONAL (IPHAN). **Política de Segurança da Informação**. Brasília, 2013.

LEAL, J. C. Identificando pontos em comum entre tipos de políticas de segurança da informação: pontos importantes a serem considerados na implementação de uma política de segurança da informação. **ForScience**, v. 7, n. 1, 2019.

Lei Federal n° 11.892, de dezembro de 2008 – Regula o acesso a divulgação de informação previsto no art.12 da Constituição Federal. Acesso em: 25 de agosto de 2020.

LEITE, C. M. **Políticas de segurança física e lógica em ambientes institucionais que utilizam tecnologia da informação**. 36 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Rede) - Universidade Tecnológica Federal do Paraná, Curitiba, 2011.

Orlivaldo Kléber Lima Rios, José Gilson de Almeida Teixeira Filho, & Vânia Patrícia da Silva Rios. (2017). Gestão de segurança da informação: Práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. Navus, 7(2), 49-65.

SPANCESKI, F. R. **Política de Segurança da Informação: desenvolvimento de um modelo voltado para instituições de ensino**. 2004. 102 f. Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Instituto Superior Tupy, Joinville, 2004.

Tribunal de Contas da União. **Boas Práticas em Segurança da Informação**. 4. ed. Brasília, 2012.

_____. **Estratégia de Fiscalização do TCU em segurança da informação e segurança cibernética 2020-2023**. Brasília, 2021.