DOI: http://dx.doi.org/10.9771/cp.v13i5.33783

Aspectos da Segurança da Informação da Propriedade Intelectual nos Institutos Federais: uma análise por meio dos documentos institucionais

Aspects of Intellectual Property Information Security in Federal Institutes: an analysis through institutional documents

Rodrigo Nogueira Albert Loureiro[1]
Gabriel Francisco da Silva[2]
Márcio Vilar França Lima[1]
Frederico Duarte de Menezes[1]
[1]Instituto Federal de Pernambuco, Recife, PE, Brasil
[2]Universidade Federal de Sergipe, São Cristóvão, SE, Brasil

Resumo

Ao longo da última década, os Institutos Federais (IFs) têm ampliado a proteção da Propriedade Intelectual (PI). Por outro lado, o número de crimes cibernéticos nos órgãos federais vem crescendo, já que, em 2017, foram notificados 28.147 incidentes de segurança da informação. Nesse cenário, ressalta-se as dificuldades e as limitações enfrentadas pelos Núcleos de Inovação Tecnológica (NIT) e pelos Departamentos de Tecnologia da Informação (DTI) dos IFs. Diante do exposto, o presente trabalho tem por objetivo traçar um panorama sobre a gestão da segurança da informação no âmbito dos NITs dos IFs da Região Nordeste do Brasil, por meio de análise de documentos institucionais que permeiam os NITs e DTIs, utilizando como instrumento metodológico uma pesquisa documental. A pesquisa demonstrou que os regulamentos não contemplam mecanismos suficientes para proteger as PIs, além de mostrar falta de convergência entre o NIT e o DTI, propiciando um ambiente mais vulnerável na proteção do conhecimento institucional.

Palavras-chave: Institutos Federais. Propriedade Intelectual. Segurança da Informação.

Abstract

Over the last decade, Federal Institutes (FIs) have expanded the protection of Intellectual Property (IP). On the other hand, the number of cybercrimes in federal agencies has been growing, since in 2017, 28.147 information security incidents were reported. In this scenario, difficulties and limitations faced by the Technological Innovation Nucleus (TIN) and Information Technology Departments (ITD) of the FIs are highlighted. In view of the above, the present work aims to provide an overview of information security management within the scope of the TINs of the IFs in the Northeast of Brazil, through the analysis of institutional documents regarding the TINs and ITDs, using as a methodological instrument a documentary research. The research demonstrated that the regulations do not include sufficient mechanisms to protect IPs, in addition to showing a lack of convergence between the TIN and the ITD, providing a more vulnerable environment in the protection of institutional knowledge

Keywords: Federal Institutes. Intelectual Property. Information Security.

Área Tecnológica: Gestão da Propriedade Intelectual. Gestão da Segurança da Informação.

Artigo recebido em: 03/10/2019
Revisado em: 26/03/2020
Aprovado em: 13/04/2020

1 Introdução

A educação profissional no Brasil passou por uma série de reformulações ao longo de sua história centenária, mas foi a partir de 2008, com a criação dos Institutos Federais de Educação, Ciência e Tecnologia (IFs) e da Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPCT) que esse tipo de educação ganhou novo *status*. Presente em todas as unidades da Federação, a RFEPCT conta com 38 IFs e 644 *campi* nos diversos municípios brasileiros (BRASIL, 2019b). Para Silva (2009), a educação proposta pelos IFs é centrada nos processos formativos e caracterizada pelas dimensões da ciência e da tecnologia e pela indissociabilidade entre a teoria e a prática. O autor ainda destaca a missão dos IFs no que concerne ao fomento da articulação entre o ensino, a pesquisa e a extensão para a consolidação na construção da ciência e do desenvolvimento tecnológico e o respeito à atitude de questionamento do indivíduo frente à realidade (SILVA, 2009).

No que se refere à pesquisa, a Lei n. 11.892, de 2008, que institui a RFEPCT, em seu artigo 6º estabelece que os IFs devem realizar e estimular a pesquisa aplicada, o empreendedorismo, o cooperativismo, além do desenvolvimento científico e tecnológico (BRASIL, 2008). Em consonância a essa legislação, foi celebrado no ano de 2010 o Termo de Acordos e Metas (TAM) entre o Ministério da Educação e a RFEPCT. O TAM estabelece um conjunto de ações para a consolidação da pesquisa no âmbito da rede, entre as quais o desenvolvimento de pelo menos um projeto de pesquisa, inovação, por campus, com a participação de docentes e de discentes, além da ampliação em 10% ao ano desses projetos em parceria com instituições públicas e privadas com viés de aplicação em interesse social (BRASIL, 2010).

O fomento à pesquisa nos IFs também ocorreu por meio da ampliação de bolsas de iniciação científica institucional e do aumento do número de grupos de pesquisa certificados no Diretório de Grupos do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). De acordo com Queiroz Neto, Pereira e Naka (2017), foram disponibilizadas 332 (trezentos e trinta e duas) bolsas no ano de 2008, enquanto em 2015 esse número saltou para 2.697 (dois mil seiscentos e noventa e sete). No que concerne aos grupos de pesquisa, o mesmo autor relata um aumento de 2.703 (dois mil setecentos e três) grupos, entre os anos de 2000 e 2016 foram 46 e 2.749, respectivamente.

Paralelamente à consolidação da pesquisa nos IFs, houve também uma evolução na produção científica e na criação de soluções inovadoras voltadas ao atendimento das demandas da sociedade. Em muitos casos, esse conhecimento produzido é passível de proteção por meio da Propriedade Intelectual (PI), seja por meio de patentes, registros de *software*, desenhos industriais, marcas, entre outras. No âmbito dos IFs, o Núcleo de Inovação Tecnológica (NIT) é o órgão responsável por gerir a política de inovação e a salvaguarda dos ativos intelectuais. Esses núcleos foram instituídos a partir da publicação da Lei n. 10.973, de 2004, conhecida como a Lei da Inovação, que, em seu artigo 16, determina que as Instituições de Ciência e Tecnologia (ICTs) brasileiras devem dispor de um NIT, seja ele próprio ou associado a outra ICT (BRASIL, 2004).

Entre as atribuições mínimas do NIT, destacam-se: a avaliação e classificação dos projetos decorrentes das atividades de pesquisa institucional; o zelo na manutenção das políticas locais de fomento à proteção das criações e Transferência de Tecnologia (TT); emissão de parecer

acerca da conveniência em promover a proteção e divulgação das criações desenvolvidas no âmbito da ICT; e acompanhamento e manutenção dos títulos de PI institucional. Além disso, o NIT deve informar ao Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) sobre a política de PI, as criações desenvolvidas, as proteções requeridas e as TTs realizadas pela instituição (BRASIL, 2004).

De posse das informações repassadas pelas ICTs, o MCTIC divulga todos os anos um relatório intitulado "Política de Propriedade Intelectual das Instituições Científicas e Tecnológicas e de Inovação do Brasil (FORMICT)". O documento contém informações consolidadas sobre o panorama da inovação nessas instituições, como: o número de proteções à PI e o *status* do NIT e da política de inovação institucional. Nesse sentido, o Formict do ano-base de 2011 mostra que dos 28 (vinte e oito) IFs que preencheram o referido relatório, apenas 50% informaram ter realizado algum tipo de proteção (BRASIL, 2012). Em contrapartida, o Formict do ano-base de 2017 apresenta que dos 38 (trinta e oito) IFs que preencheram o referido relatório, 76% informaram ter protegido algum ativo intelectual (BRASIL, 2019a). Esses números demonstram que ao longo dos anos os IFs têm envidado esforços na proteção de seu capital intelectual.

O Formict não disponibiliza de forma regionalizada o panorama de proteção da PI por parte dos IFs. Contudo, essas informações podem ser observadas a partir do levantamento realizado pelo Fórum de Dirigentes de Pesquisa, Pós-Graduação e Inovação dos IFs (FORPOG). Esse levantamento mostrou que no ano de 2015 os IFs da Região Nordeste apresentaram os maiores índices de proteção às produções tecnológicas, com 62 (sessenta e dois) depósitos de patentes, 15 (quinze) registros de marca e 17 (dezessete) registros de *software*, seguidos pelos IFs da Região Sudeste com 25 (vinte e cinco), 9 (nove) e 20 (vinte) proteções, respectivamente (LIMA JÚNIOR, 2017). Nessa mesma pesquisa, o autor apresenta os indicadores atualizados apenas de patentes, informando que, entre os anos de 2008 e 2016, os IFs nordestinos realizaram o depósito de 159 (cento e cinquenta e nove) patentes. Não há dúvidas de que os IFs da Região Nordeste têm envidado esforços para a proteção do conhecimento institucional, pois mais que dobrou o número de depósitos de patentes entre os anos de 2015 e 2016.

Diante do exposto, deve-se considerar a importância e o valor das informações gerenciadas pelos NITs, pois torna-se premente a necessidade de proteção desses ativos intelectuais, resguardando a autoria e o direito à exploração do invento em caso de transferência de conhecimento para o setor produtivo. Segundo Oliveira (2012), a salvaguarda do conhecimento tem impacto direto no desenvolvimento de um país, promovendo aos países detentores dessas PIs uma soberania econômica, gerando riquezas e melhoria na vida da população. Nesse sentido, é evidente o papel estratégico associado às diversas proteções conferidas pela PI, sendo necessária a compreensão dos riscos e da vulnerabilidade pelas quais essas proteções estão suscetíveis a ataques cibernéticos. Não é incomum esse tipo de ataque aos diversos órgãos vinculados ao poder público, pois, de acordo com Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal (CTIR), foram realizadas 28.147 (vinte e oito mil e cento e quarenta e sete) notificações de incidentes de segurança da informação no ano 2017 por parte dos diferentes órgãos da esfera Federal (BRASIL, 2017).

Sêmola (2014) enfatiza o valor da informação, despontando como recurso-chave de uma instituição, a partir do desenvolvimento de experimentos, conceitos, métodos, modelos, e descobertas oriundas de pesquisadores, estudantes e executivos. Nessa perspectiva, é preciso estabelecer mecanismos que possam assegurar a proteção desse bem intangível, garantindo

a confidencialidade, a integridade e a disponibilidade a partir de uma gestão de segurança da informação. Entre os preceitos básicos desse tipo de gestão, destaca-se a classificação dos ativos de informação. Segundo Lyra (2008), a definição desses ativos abarca a informação e os recursos que subsidiam ou se utilizam dela, a exemplo da tecnologia utilizada, das pessoas que manipulam essas informações e do seu ambiente. Por meio da Figura 1 é possível avaliar a classificação dos grupos pertencentes aos ativos da informação.

A identificação dos diversos ativos informacionais e as responsabilidades apropriadas para a sua proteção representam mecanismos importantes na mitigação de riscos na gestão da segurança da informação. Dessa forma, é preciso que a organização realize o inventário desses ativos de forma completa e consistente, designando um responsável para o gerenciamento do ativo ao longo do seu ciclo de vida. Entre as atribuições do responsável pelo ativo (gestor), encontram-se as de: assegurar que os ativos sejam inventariados, classificados e protegidos; avaliar de as classificações e restrições de acesso aos ativos considerados importantes, de acordo com as políticas, de controle de acesso, aplicáveis; e assegurar o tratamento adequado na exclusão ou destruição do ativo (ABNT, 2013).

Figura 1 – Classificação dos grupos dos Ativos da Informação

Fonte: Lyra (2008)

De acordo com Silva e Stein (2007, p. 46), "O problema da segurança da informação tem sempre duas faces, que são representadas pelas características inerentes de dois mundos diferentes e por vezes conflitantes: o mundo da tecnologia e o mundo dos seres humanos". Para as autoras, o comportamento humano abarca grande complexidade, com variáveis de difícil controle, situação que, muitas vezes, é negligenciada pelos profissionais de tecnologia da informação, que, comumente, se concentram nas variáveis de *hardware* e *software* (SILVA; STEIN, 2007). Da mesma forma, os gestores de tecnologia precisam considerar o arcabouço legal na elaboração de um sistema eficaz de gestão em segurança da informação. Nessa perspectiva, o poder legislativo tem envidado esforços na elaboração de um conjunto de atos normativos, com o intuito de reduzir os diversos problemas relacionados ao vazamento de informações e

à quebra de sigilos nos órgãos do Governo Federal. Atualmente, os gestores de tecnologia da informação dispõem de um cabedal de normas, decretos e legislações desenvolvido em conformidade com as políticas e diretrizes de segurança em âmbito internacional.

Entre esses atos normativos, encontra-se a Lei n. 12.527, de 2011, conhecida como Lei de Acesso à Informação (LAI). Em linhas gerais, a LAI determina que os diversos órgãos ou entidades públicas devem garantir o direito de acesso à informação por qualquer pessoa, de forma objetiva, transparente, ágil e com linguagem clara e de fácil compreensão. Contudo, a Lei instrui os órgãos e as entidades do poder púbico a observar as normas e os procedimentos específicos que garantam a proteção da informação de caráter sigiloso, respeitando a tríade da disponibilidade-autenticidade-integridade (BRASIL, 2011). Em seu artigo 23, a LAI trata sobre o processo de classificação das informações de interesse consideradas imprescindíveis para a segurança da sociedade e da nação ou que tenha caráter estratégico, a exemplo daquela que possa "[...] prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico". Tal classificação é normatizada por meio do seu artigo 24, que instrui os órgãos e as entidades públicas acerca da categorização das informações como: ultrassecreta, secreta e reservada.

Em uma perspectiva mais singular, destaca-se o Decreto n. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal (BRASIL, 2000). O referido decreto determina que os órgãos vinculados ao poder público federal disponham de uma Política de Segurança da Informação e Comunicação (POSIC). Em linhas gerais, a Posic deve ter como pressuposto básico: a proteção aos assuntos que merecem atenção especial; a capacitação dos segmentos das tecnologias sensíveis; a capacitação científica e tecnológica do Brasil para uso da criptografia na segurança e defesa do País; o uso soberano de mecanismos de segurança da informação; e a conscientização dos órgãos públicos Federais no que diz respeito à importância das informações processadas e sua vulnerabilidade (BRASIL, 2000).

Entretanto, ainda que exista uma legislação determinando que os órgãos Federais devam instituir uma Posic, algumas Instituições Federais de Ensino Superior (IFES) não dispõem desse documento. Segundo Rios, Rios e Teixeira (2017), em pesquisa realizada junto à Secretaria de Fiscalização de Tecnologia da Informação, de 98 (noventa e oito) das IFES que participaram do levantamento, apenas 47,9% informaram ter uma política instituída.

Além da Posic, outros fatores impactam nas atividades do Departamento de Tecnologia da Informação (DTI) dos órgãos públicos, tanto do ponto de vista de infraestrutura tecnológica quanto de capital humano. A pesquisa realizada por Sousa (2015) demonstrou uma dependência considerável dos IFs aos diversos recursos de Tecnologia da Informação (TI) no cumprimento dos vários macroprocessos institucionais. Ao mesmo tempo, o autor constata uma série de dificuldades enfrentadas na governança de TI por parte do DTI, incluindo a infraestrutura de *hardware* e *software*, muitas vezes, deficitária, há, ainda, a falta de apoio das instâncias superiores, as limitações orçamentárias e os problemas relacionados aos recursos humanos, principalmente pela alta rotatividade dos servidores.

Conforme relatado, os DTIs vivenciam uma série de carências, que vai desde questões de infraestrutura até os aspectos humanos. Essa situação traz impactos aos diversos setores dos IFs, incluindo o NIT. Em decorrência da responsabilidade e dos diversos riscos (roubo ou vazamento) relativos às informações das PIs geridas por esses núcleos, se faz necessário que haja a

compreensão de alguns aspectos que impactam diretamente a segurança da informação desses órgãos. Uma forma de balizar tais especificidades está relacionada aos aspectos descritos em alguns dos atos normativos e de relatórios institucionais.

Diante do exposto, o presente trabalho se propõe a traçar um panorama acerca da gestão da segurança da informação no âmbito dos NITs dos IFs da Região Nordeste do Brasil, por meio de uma análise dos documentos institucionais que permeiam esses núcleos e o DTI. Essa temática se mostra relevante, considerando que não há trabalhos na literatura que abordem aspectos relacionados à segurança da informação de forma direcionada aos NITs, e, em uma perspectiva mais singular, aos IFs da Região Nordeste.

2 Metodologia

Do ponto de vista metodológico, inicialmente, foi utilizada a técnica de pesquisa documental. Segundo Sá-Silva, De Almeida e Guindani (2015), a análise de documentos auxilia na compreensão de objetos que necessitam de contexto histórico, possibilitando novas formas de compreensão de um fenômeno. Para isso, foram analisados os principais regulamentos e relatórios que subsidiam as atividades do NIT e do DTI dos IFs situados na Região Nordeste do Brasil. A escolha dos IFs nordestinos para a pesquisa em tela se justifica pelos indicadores de proteção à PI, pois, de acordo com a pesquisa de Lima Júnior (2017), essas instituições apresentaram os maiores índices de proteção aos ativos intelectuais, mais especificamente das patentes, entre os anos de 2008 e 2016 na RFEPCT.

Os documentos selecionados para essa etapa da pesquisa foram: a Política de Inovação, a Posic e o Plano Diretor de Tecnologia da Inovação (PDTI) dos IFs delimitados para este trabalho. Preliminarmente, foi realizado um recorte dos principais aspectos sobre a segurança da informação na Política de Inovação. Tal avaliação consiste em compreender como e se ocorrem abordagens que permeiam especificamente a segurança da informação na gestão da PI.

No segundo estágio da pesquisa, foram analisados os documentos que orientam as atividades do DTI que tratam do tema segurança da informação, em específico, a Posic e o PDTI. Essa avaliação tem o objetivo de verificar a existência de mecanismos direcionados à salvaguarda da PI e/ou apoio ao NIT. Ainda no escopo dessa análise, encontra-se uma síntese das principais ações do DTI, inclusive apontando suas dificuldades e limitações, que, por conseguinte, impactam nas ações de segurança da informação institucional. Tanto a Política de Inovação quanto o PDTI e a Posic analisados estão em suas versões mais recentes, assim disponibilizadas pelos *sites* institucionais dos IFs e contempladas nesta pesquisa.

3 Resultados e Discussões

A análise documental dos regulamentos e dos relatórios associados ao NIT e ao DTI dos IFs nordestinos estão apresentadas em duas seções. Incialmente, foi realizada uma avaliação da Política de Inovação dos NITs, no que tange aos procedimentos relacionados à segurança da informação. Enquanto, na segunda etapa, foram analisados os principais documentos associados aos DTIs, objetivando avaliar se existe e qual é a abordagem sobre a proteção das PIs, além de apresentar um panorama sobre a realidade desses setores, que, de alguma forma,

refletem na salvaguarda do conhecimento institucional. Os IFs contemplados nessa pesquisa são: Instituto Federal de Alagoas (IFAL); Instituto Federal da Bahia (IFBA); Instituto Federal Baiano (IF-Baiano); Instituto Federal do Ceará (IFCE); Instituto Federal do Maranhão (IFMA); Instituto Federal da Paraíba (IFPB); Instituto Federal de Pernambuco (IFPE); Instituto Federal do Sertão Pernambucano (IF-Sertão-PE); Instituto Federal do Piauí (IFPI); Instituto Federal do Rio Grande do Norte (IFRN); e Instituto Federal de Sergipe (IFS).

3.1 A Política de Inovação e a Segurança da Informação

Conforme citado, Lima Júnior (2017) apresenta nos dados de sua pesquisa que os IFs nordestinos têm envidado esforços na proteção do conhecimento ao longo da última década, pela salvaguarda conferida por diversas PIs, sejam por meio de patentes, marcas, desenhos industriais ou registros de *softwares*. Contudo, apesar da melhoria dos indicadores de proteção ao conhecimento gerados nessas instituições, é preciso destacar que as políticas de inovação ainda não contemplam questões específicas sobre a gestão da segurança da informação na administração dos ativos intelectuais pelos NITs.

De forma quase totalitária, as políticas de inovação dos IFs tratam essa temática de forma superficial, limitando-se a exigir dos atores envolvidos o sigilo das informações sobre a criação intelectual com a assinatura de um termo de confidencialidade. Para corroborar essa informação, foi realizado um recorte dos principais pontos que permeiam a segurança da informação nas políticas de inovação dos IFs da Região Nordeste, assim apresentados no Quadro 1.

Quadro1 – Abordagem sobre sigilo das informações nas políticas de inovação dos IFs Nordeste

Instituto	Documento	Abordagem
IFAL	Resolução n. 6 do Conselho Superior, de 12 de junho de 2017	O capítulo XI trata das responsabilidades e da confidencialidade. O tema em questão é tratado do artigo 20 até o artigo 23, e em linhas gerais aborda a obrigatoriedade no sigilo das criações intelectuais desenvolvidas no âmbito do IFAL passíveis de comercialização, celebrado por meio de termos de compromissos e afins. Esse sigilo inclusive se aplica a todos os agentes que atuam no NIT ou que dele sejam usuários.
IFBA	Resolução n. 39 do Conselho Superior, de 29 de julho 2013	O sigilo das informações é abordado por meio do Capítulo III, que em seu artigo 4° diz: "As pessoas ou entidades co-participantes obrigam-se a celebrar um termo de confidencialidade sobre a criação intelectual objeto da co-participação". **Parágrafo único.** A obrigação de confidencialidade estende-se a todo o pessoal envolvido no processo de formalização, encaminhamento e acompanhamento do pedido de patente ou registro até a data da sua concessão".
IF-Baiano	Resolução n. 35 do Conselho Superior de, 1º de setembro de 2016	As diretrizes sobre o sigilo da informação são definidas por meio do Capítulo V, nos artigos 6º, 7° e 8° do referido documento, determinando que todas as criações intelectuais em âmbito institucional devam ser comunicadas ao NIT e que pesquisadores, professores, funcionários, alunos, estagiários e bolsistas devem manter segredo sobre essas criações. Este sigilo se estende a todos os envolvidos no processo de formalização, encaminhamento e acompanhamento do pedido de PI até da data de sua concessão. As pessoas envolvidas neste processo são obrigadas a celebrar um termo de confidencialidade sobre a criação intelectual.

Instituto	Documento	Abordagem
IFCE	Resolução n. 5 do Conselho Superior, de 4 de fevereiro de 2011	De forma similar aos outros IFs, o IFCE aborda o sigilo em sua política instituindo que os envolvidos na criação intelectual da organização celebrem um termo de confidencialidade, desde a formalização até o pedido de proteção à PI (Capítulo V). Além disso, faz parte da política instruir os servidores que os resultados de pesquisas, estudos e projetos institucionais de interesse do setor produtivo sejam apenas divulgados e publicados depois de tomadas as medidas de proteção cabíveis.
IFMA	Resolução n. 111 do Conselho Superior, de 24 de abril de 2017	A política de inovação do IFMA dispõe, em seu Capítulo V, das diretrizes para o sigilo das informações. Em linhas gerais, o referido capítulo determina que em uma criação intelectual, as pessoas ou entidades participantes do invento, deverão celebrar um termo de confidencialidade. Além disso, estabelece que os diversos agentes de sua comunidade acadêmica, incluindo servidores, bolsistas, estudantes, visitantes, entre outros, que realizem o desenvolvimento de pesquisa nas dependências do IFMA, deverão manter em sigilo qualquer informação confidencial oriunda dos projetos de pesquisa institucional, acordado por meio do termo de sigilo e confidencialidade.
IFPB	Resolução n. 116 do Conselho Superior, de 10 de abril de 2017	O artigo 4º desta Resolução versa sobre as criações desenvolvidas no âmbito do IFPB devem ser comunicadas ao NIT e os criadores devem ser comprometer na defesa dos interesses da Instituição, em termos da proteção intelectual, garantindo confidencialidade e sigilo sobre as invenções correspondentes. O artigo 5º determina que os diversos contratos e convênios de P&D passíveis de geração de PI do IFPB com terceiros, deverão ter cláusulas reguladoras de confidencialidade. Já em seu artigo 10, a Resolução informa que as documentações que tratam de PI direcionadas para o NIT deverão ser protocoladas em envelope lacrado e assinado pelo responsável pelo pedido, para fins de garantia do sigilo do documento protocolado.
IFPE	Resolução n. 31 do Conselho Superior, de 2 de julho de 2015	No artigo 10 é esclarecido que os projetos de pesquisa científica e tecnológica submetidos a PROPESQ com potencial de geração de PIs passarão por um processo de avaliação. Caso seja verificado o potencial de geração de PIs, todos os envolvidos na criação deverão manter sigilo sobre o invento, através de um termo de confidencialidade. O mesmo artigo também determina que a publicação de uma invenção só poderá ser realizada após autorização do NIT com respaldo do seu Comitê de PI e TT.
IF-Sertão-PE	Resolução n. 34 do Conselho Superior, de 26 de outubro de 2017; Resolução n. 36 do Conselho Superior, de 27 de outubro de 2017	A temática da segurança da informação é abordada por meio de duas resoluções no IF-Sertão-PE. A primeira resolução trata da política de inovação, enquanto a segunda normatiza as ações do NIT. O Capítulo IV da n. 34 aborda o sigilo e a confidencialidade da informação, determinando que as pessoas ou entidades envolvidas sobre uma criação intelectual passível de proteção, obrigam-se a celebrar um termo de confidencialidade. Já a Resolução n. 36 trata do mesmo assunto em seu Capítulo VI e elucida que todas as informações de PIs ou qualquer ação decorrente do NIT serão objetos de sigilo. O capítulo ainda informa que para os contratos, acordos, convênios, ajustes, termos de compromissos e instrumentos afins, os partícipes deverão prever cláusula de sigilo e confidencialidade para fins de preservação e apropriação do conhecimento por pessoas não autorizadas.
IFPI	Resolução n. 28 do Conselho Superior, de 29 de dezembro de 2015	No Capítulo I da norma referida é esclarecido que as informações técnicas e confidenciais oriundas dos projetos de pesquisa entre o IFPI, pesquisadores, colaboradores e empresas com potencial de comercialização, deverão ser mantidas em segredo e objeto de termo de sigilo. No Capítulo III, essa questão do termo é ratificada e exigido que todos os envolvidos no processo de formalização, encaminhamento e acompanhamento do pedido de proteção à PI garantam a confidencialidade. Além disso, determina que toda a sua comunidade acadêmica que esteja envolvida com trabalho de pesquisa em suas dependências, não revele qualquer informação confidencial que possa ter obtido sobre linhas e assuntos destes projetos.

Instituto	Documento	Abordagem
IFRN	Deliberação n. 9 do Conselho Superior de Pesquisa, de 1º de junho de 2017	Por meio do seu artigo 28, enfatiza a proibição da comunidade acadêmica do IFRN de "divulgar, noticiar ou publicar qualquer aspecto de criações ou tecnologias de cujo projeto de desenvolvimento de pesquisa tenha participado diretamente ou tomado conhecimento por força de suas atividades" sem anuência do NIT. Em caso de descumprimento, estará sujeito a penalidades civil e criminal. O artigo 30 estabelece que todos os que tiveram acesso a informação confidencial, sejam institucionais ou não, deverão guardar o sigilo, formalizado por meio de um termo de confidencialidade. Destaca-se a recomendação deste artigo ao esclarecer quer também é dever do pesquisador restringir o acesso somente para pessoas imprescindíveis aos projetos sob sua responsabilidade.
IFS	Resolução n.19 do Conselho Superior, de 24 de outubro de 2007	Em seu artigo 14 institui que as informações e os direitos relativos à PI decorrentes das ações do NIT serão objetos de sigilo. Tais informações sigilosas só poderão ser divulgadas mediante chancela do referido núcleo e aprovação expressa por parte dos envolvidos no objeto. No que concerne aos contratos, acordos, convênios, ajustes, termos de compromissos e instrumentos afins, todos os atores envolvidos deverão aderir a uma cláusula de sigilo e confidencialidade para fins de preservar os resultados passíveis de proteção.

Fonte: Elaborado pelos autores deste artigo (2019)

Para Leite e Ikegaki (2012), a confidencialidade nas ICTs pode ser implementada por meio de alguns instrumentos jurídicos, a exemplo da "cláusula de sigilo e confidencialidade", determinando que as partes envolvidas em parcerias de pesquisa, prestação de serviço, TT, entre outros, não divulguem para terceiros os dados e as informações sobre o conhecimento desenvolvido. Dados do Formict do ano-base de 2017 mostram que 74,9% das ICTs brasileiras já dispõem de uma política de confidencialidade (BRASIL, 2019a). Entretanto, é preciso que outras medidas sejam adotadas no intuito de garantir proteção do conhecimento, pois a política de confidencialidade, apesar de fundamental, não contempla todas as esferas que permeiam a segurança da informação.

3.2 A Posic, o PDTI e as Limitações do DTI

Outra forma de regimentar a gestão da segurança da informação está relacionada à instituição da Posic. De acordo com Ferreira e Araujo (2008), no desenvolvimento de uma Posic, é preciso considerar algo além de *hardware* e *software*, e que abarque as pessoas, os dados, as documentações, os processos do negócio e a PI. No caso dos ativos intelectuais, os autores ainda reforçam que devem existir controles específicos e que a Posic contemple a implementação de procedimentos apropriados no intuito de assegurar a conformidade, em consonância com as legislações dos direitos autorais, das marcas, das patentes, do registro de *softwares* e de outros tipos de proteção.

Além da Posic, outros documentos normatizam as ações do departamento de tecnologia da informação no que tange à segurança da informação. Entre esses documentos, encontra-se o Plano Diretor de Tecnologia da Informação (PDTI) que possui o objetivo de realizar diagnósticos e planejamento na gestão de processos e recursos de tecnologia da informação alinhados as necessidades da organização. Nesse sentido, com o intuito de compreender as atividades realizadas pelos DTIs e qual é a abordagem dos documentos institucionais em relação à proteção da PI por parte dos IFs da Região NE, foi realizado um levantamento dos principais documentos norteadores que estão apresentados no Quadro 2.

Quadro 2 – Documentos que norteiam as atividades de tecnologia da informação dos IFs Região NE

Instituto Federal	Documento norteador
IFAL	• Política de Segurança da Informação e Comunicação de 27 de março de 2018; • Portaria n. 44/GR, de 8 de janeiro de 2018, que regulamenta o uso de correio eletrônico; • Portaria n. 2.095/GR, de 20 de setembro de 2017, que compõe o Comitê de Governança de TI; • Resolução n. 20/CS, de 12 de novembro de 2018, que aprova o Plano Diretor de Tecnologia da Informação e Comunicação.
IFBA	• Resolução CONSUP n. 9, de 1º de abril de 2013, que aprova a Política de Segurança da Informação do IFBA; • Regulamentação n. 1, de 17 de dezembro de 2014, sobre o uso do correio eletrônico institucional; • Plano Estratégico de Tecnologia da Informação do IFBA Biênio 2017/2018.
IF-Baiano	• Política de Segurança da Informação do IF-Baiano de dezembro de 2011; • Normas de Segurança da Informação de dezembro de 2013; • Resolução n. 1, de 16 de maio de 2016, que aprova o Plano Diretor de Tecnologia da Informação 2016/2019.
IFCE	• Plano Estratégico de Tecnologia da Informação (2014-2018) do IFCE de novembro de 2013; • Plano Diretor de Tecnologia da Informação (2014-2018) do IFCE de fevereiro de 2014; • Resolução n. 23, de 27 de março de 2017, que aprova a Política de Segurança da Informação do IFCE.
IFMA	• Resolução n. 46, de 1º de setembro de 2015, instituindo a Política de Segurança da Informação e Comunicação do IFMA; • Plano Diretor de Tecnologia da Informação e Comunicação (2016-2018) do IFMA.
IFPB	• Plano Diretor de Tecnologia da Informação (2017-2018) do IFPB; • Política de Segurança da Informação do IFPB, de 9 de novembro de 2011.
IFPE	• Resolução n. 60, de 15 de dezembro de 2015, que aprova o Plano Diretor de Tecnologia da Informação do IFPE (2015-2017); • Resolução n. 11, de 6 de fevereiro de 2017, que aprova a Política de Segurança da Informação e Comunicação do IFPE.
IF-Sertão-PE	• Resolução n. 13, de 22 de junho de 2016, que aprova a Política de Segurança da Informação e Comunicação do IF-Sertão PE; • Resolução do Conselho Superior n. 9, de 11 de maio de 2017, que aprova o Planejamento Estratégico de Tecnologia da Informação do IF-Sertão.
IFPI	• Plano Diretor de Tecnologia da Informação e Comunicação (2016-2017) do IFPI; • Resolução n. 85, de 14 de novembro de 2018, que aprova a Política de Segurança da Informação e Comunicação do IFPI.
IFRN	• Resolução n. 99, de 21 de dezembro de 2012, que aprova a Política de Segurança da Informação e Comunicação do IFRN; • Resolução n. 23, de 29 de agosto de 2014, que aprova o Plano Diretor de Tecnologia da Informação e Comunicação (2014-2015) do IFRN.
IFS	• Plano Diretor de Tecnologia da Informação e Comunicação (2014-2019) do IFS; • Deliberação do CGSIC n. 1, de 30 de janeiro de 2018, que aprova a Política de Segurança da Informação e Comunicação do IFS.

Fonte: Elaborado pelos autores deste artigo (2019)

A partir da análise dos dados do Quadro 2, observa-se que essas políticas foram elaboradas tendo como base as diversas legislações sobre a temática e, em uma perspectiva mais técnica, as NBRs da família 27000 (ABNT, 2013). A referida norma técnica tem por objetivo estabelecer, implementar, manter e melhorar de forma contínua os processos de gestão da segurança da informação, para fins de preservar a confidencialidade, a integridade e a disponibilidade

da informação nas organizações. De forma geral, as Posics carregam similaridades e têm como princípio básico os aspectos da confidencialidade, integridade, disponibilidade, autenticidade e não repúdio da informação. Apesar das semelhanças entre essas políticas, algumas foram elaboradas já normatizando o uso e o acesso aos diversos serviços tecnológicos de informação, a exemplo do correio eletrônico, da internet, da segurança física e do ambiente, dos processos de segurança em recursos humanos, da gestão de ativos, entre outros.

O PDTI, por sua vez, trata das ações de segurança da informação, sugerindo a criação de um Comitê de Segurança da Informação e criação/atualização da Posic. Após análise dos documentos supracitados, tem-se a percepção de que não há uma abordagem mais específica sobre a proteção da PI, ou, em alguns casos, o enfoque é bastante superficial. Diante do exposto, serão sumarizadas algumas dessas abordagens e as dificuldades enfrentadas pelos IFs no que se refere à segurança da informação.

3.3 Gestão da Segurança no IFAL

A Posic no IFAL é relativamente recente, foi instituída em março de 2018 e desenvolvida com a finalidade de preservar as informações e seus respectivos ativos no tocante à Disponibilidade, à Integridade, à Confidencialidade e à Autenticidade (DICA), promovendo suporte aos objetivos estratégicos da instituição. Diante do volume crescente de informações no IFAL e da falta de DICA nos sistemas computacionais, a Posic expõe os diversos desafios relacionados à segurança da informação, entre eles: ampla disponibilidade de técnicas e ferramentas de ataque e invasão na rede e no mercado, aliado à facilidade de uso dessas ferramentas; aumento exponencial dos crimes virtuais; leis, regulamentações e normas não unificadas; processos de continuidade dos serviços públicos sem um grau de maturidade adequado; e crescente valorização da informação como principal ativo de gestão do Estado.

No geral, o referido documento trata de conceitos e de definições acerca da segurança da informação, sua abrangência e a delegação ao Comitê de Segurança da Informação o desenvolvimento de políticas temáticas, a exemplo da política de *e-mail*, da internet, da segurança física, da segurança de redes, entre outros. Apesar de abordar os diversos aspectos de proteção à informação no IFAL, a Posic não trata com especificidade assuntos relativos à proteção da PI.

O PDTI do biênio 2018-2019 trata, em linhas gerais, do monitoramento de investimentos e das atividades de Tecnologia da Informação e Comunicação (TIC) em todo o IFAL. O documento em questão também realiza uma análise SWOT. Entre os pontos fracos apontados pela análise SWOT que foram informados, estão: número insuficiente de servidores técnicos; ausência de planejamento para capacitação de equipe de TI; alguns *campi* com infraestrutura de rede lógica deficitária; e burocracia. Já entre as ameaças constam: investimento insuficiente para atender às demandas tecnológicas crescentes da instituição; estrutura física de alguns *campi* necessitando de reformas; e perda de dados, decorrente da intolerância a falhas.

3.4 Gestão da Segurança no IFBA

A Posic do IFBA foi instituída no ano de 2013, tendo por objetivo o estabelecimento de procedimentos, mecanismos, competências, responsabilidades, direcionamentos e valores a serem adotados na gestão da segurança da informação no correto manuseio, tratamento,

proteção e controle dos ativos de informação. Além da conceituação dos temas correlatos, a Posic funciona como documento norteador para elaboração de outros documentos técnicos regulatórios, considerando as especificidades de cada campus. A referida política instrui que os ativos do IFBA devem ser protegidos por meio de normas específicas, e, nesse contexto, estão as PIs. Entretanto, não foram encontrados mecanismos que tratem de forma pontual a proteção desse tipo de conhecimento.

As diretrizes das diversas atividades e recursos de tecnologia da informação do IFBA no biênio 2017-2018 são contempladas por meio do Plano Estratégico de Tecnologia da Informação (PETI). Entre os diversos objetivos elencados no PETI, destaca-se a gestão dos incidentes de segurança da informação relacionados à tecnologia da informação e o intercâmbio com os demais órgãos da administração pública. O referido plano apresenta também uma análise ambiental da TI do IFBA, por meio da aplicação de análise SWOT, apontando como suas ameaças, a desarticulação entre áreas demandantes, a adoção de soluções em TI por parte dos setores sem consulta ao órgão responsável, além da decisão política ter prevalência sobre as técnicas. A análise mencionada também destaca, entre seus pontos fracos, os processos informais de trabalho, o ambiente inadequado para as instalações físicas e a insuficiência de pessoal técnico. Ainda sobre os recursos humanos, o PETI do IFBA aborda a estrutura hierárquica do setor de TI e informa a existência da Coordenação de Segurança da Informação e da Coordenação de Projetos e Inovação em Tecnologia da Informação vinculada ao referido setor. Contudo, essa última coordenação, apesar de possuir nomenclatura similar ao NIT, ao se analisar o detalhamento de suas atribuições, percebe-se que não há relação entre as atividades desses dois setores.

3.5 Gestão da Segurança no IF-Baiano

O direcionamento dos diversos recursos de tecnologia da informação no IF-Baiano, incluindo informações, sistemas, serviços, infraestrutura e pessoas, ocorre por meio do PDTI (2016-2019). O referido documento foi desenvolvido pela Diretoria de Gestão de Tecnologia da Informação, tendo o dever de executar a Posic, garantindo a proteção dos dados e a análise do risco do ambiente físico e lógico. Além das diretrizes na gestão da TI, o documento ainda relata algumas dificuldades vivenciadas pela diretoria supracitada, a exemplo do número de servidores não ter acompanhado a expansão ocorrida nos últimos anos no IF-Baiano, bem como o aumento na demanda por serviços tecnológicos. Para tornar mais efetiva as ações do departamento de TI, foram criados eixos temáticos para a capacitação de seus agentes, entre eles, o eixo específico em segurança da informação. Além disso, fica determinada no PDTI a existência de um grupo de trabalho permanente, formado por, pelo menos, um representante de cada campus para tratar a salvaguarda das informações institucionais.

Além da Posic, o IF-Baiano conta com o documento de Normas de Segurança da Informação, estabelecendo que todas as informações, independentemente do seu meio de transmissão, recebam níveis adequados de proteção, indicando a sua classificação, o prazo de sigilo e quem as classificou, em observância ao disposto na LAI. Tanto a Posic quanto a Norma de Segurança da Informação abordam a troca de informações sigilosas entre usuários e devem ser suportadas por acordos formais, a exemplo do termo de responsabilidade, para fins de preservar a privacidade de dados pessoais, direitos autorais e patrimoniais da instituição, sendo essa a abordagem mais próxima sobre segurança da PI tratada nos documentos.

3.6 Gestão da Segurança no IFCE

O Comitê de Tecnologia da Informação do IFCE é o órgão responsável por elaborar o PETI e o PDTI no IFCE. Entre os objetivos estratégicos do PETI está o de promover a gestão da segurança da informação; elaborar regulamentos e normas relativos à Posic; implantar a gestão de riscos; e a criação de banco de dados interno na notificação de incidentes de segurança. O PDTI foi criado com a finalidade de traçar as diretrizes e de orientar o planejamento dos recursos e processos de TI, e um dos seus princípios é garantir a segurança da informação. Considerando as possibilidades e as limitações do ambiente de TI, o PDTI apresenta o resultado da análise SWOT realizada no IFCE, tendo como destaque nos pontos fracos o número insuficiente de procedimentos para tratar a segurança da informação, a vulnerabilidade e a não confiabilidade do serviço de *e-mail*, além de citar a insuficiência de sua equipe. O PDTI também elucida a necessidade de criação de uma Posic em âmbito institucional, sendo esta criada no ano de 2017.

Assim como ocorre com a política em outros Institutos, a Posic do IFCE foi instituída para proteger os diversos ativos de informação, seguindo o princípio da DICA, e a salvaguarda das informações de acordo com o seu valor, sensibilidade e criticidade. A referida política já foi criada em consonância com a LAI e possui um capítulo específico sobre a classificação e o sigilo da informação, além de dispor de um termo de responsabilidade abordando os diversos aspectos da segurança da informação. A segurança dos ativos intelectuais é tratada por meio do artigo 23 da Posic quando estabelece procedimentos apropriados para garantir a conformidade e o respeito às restrições legais quanto ao uso e à disseminação de informações protegidas da PI.

3.7 Gestão da Segurança no IFMA

A PDTI (2016-2018) do IFMA foi baseada na Estratégia de Governança Digital (2016-2019) da Administração Pública Federal, com a finalidade de realizar diagnósticos, planejamentos e gestão de recursos de TI no âmbito do referido Instituto. O documento em questão elenca princípios e diretrizes como ponto de partida para as ações de TI em atendimento aos aspectos legais, entre eles o de garantia em segurança da informação. Entre os objetivos estratégicos desse PDTI, encontra-se o de garantir a infraestrutura de TIC apropriada para a realização das atividades administrativas, de ensino, de pesquisa e de extensão, aqui subentendida com a inclusão de mecanismos de proteção à informação. O documento supracitado também apresenta o resultado da análise SWOT, apontando, entre os seus pontos fortes, a aprovação da Posic do IFMA. Em contrapartida, o documento indica como suas fraquezas e ameaças: a ausência de plano de continuidade de serviços de TIC que requerem alta disponibilidade e confiabilidade; a evasão e a ausência de política de capacitação de servidores; a falta de plano de carreira de cargos específicos para área de TI; e a ausência de política de aquisição e descarte de equipamentos, sendo esse um fator de risco à segurança das informações.

A Posic no IFMA, por sua vez, abrange aspectos básicos da segurança da informação, incluindo, além da DICA, a criticidade, o não repúdio, as responsabilidades, a ciência, a ética, a legalidade e a proporcionalidade. Também compõe essa política um conjunto de normas e de procedimentos sobre a gestão da segurança da informação, a exemplo do uso do correio eletrônico institucional e a gestão de senhas; a gestão de dados corporativos; as hospedagens e as publicações na internet; entre outros. O documento aborda questões relativas à proteção da PI, em específico, aquelas relativas ao direito autoral na gestão dos programas de computadores.

3.8 Gestão da Segurança no IFPB

No ano de 2011 foi instituída a Posic do IFPB, considerada uma declaração formal da organização no compromisso de proteger as informações, propondo diretrizes no manuseio, tratamento e controle para garantir a DICA dos ativos informacionais. A política mencionada carrega uma abordagem conceitual dos principais termos relacionados à segurança da informação e à especificação de duas outras estruturas documentais que dão suporte à Posic, nesse caso, as normas e os procedimentos gerenciados pelo comitê de segurança da informação e comunicação. Fica estabelecida nessa Posic a elaboração de procedimentos para identificação, tratamento e classificação da informação, bem como as normas complementares para a proteção do conhecimento. Entretanto, não foi possível determinar a existência de documentos auxiliares que pudessem promover a segurança da informação de forma direcionada a PI.

A preocupação com a salvaguarda das informações também é abordada por meio do PDTI (2017-2018) do IFPB, pois se destaca na seção planos e metas a necessidade de monitorar e de atualizar periodicamente a Posic. Esse plano diretor também apresenta o resultado da análise SWOT da TI institucional, apontando entre as ameaças a infraestrutura tecnológica suscetível a ataques externos; a falta de plano de contingência; e o investimento insuficiente em TI frente ao aumento das demandas por tecnologia. Entre as fraquezas encontra-se o baixo número de servidores disponíveis para TI; a necessidade de capacitação para os servidores; e a falta de padronização em serviços, infraestrutura e processos de tecnologia no IFPB.

3.9 Gestão da Segurança no IFPE

O PDTI (2015-2017) do IFPE foi instituído com a finalidade de orientar o correto uso dos recursos de TIC, de forma alinhada às prioridades estratégicas do ensino, da pesquisa e da extensão. Esse plano foi elaborado com princípios e diretrizes que norteiam a governança de TI em consonância com o planejamento estratégico da instituição, tendo por objetivo garantir a segurança da informação e os princípios da disponibilidade, integridade e publicidade da informação.

O documento mencionado apresenta o resultado da análise SWOT realizada no âmbito da TI organizacional do IFPE, indicando entre as suas fraquezas a baixa padronização de processos de TI, a quantidade de colaboradores insuficientes para a demanda crescente por recursos tecnológicos; a ausência de normas e processos de governança de TI; e a necessidade constante de capacitação por parte dos servidores de TI. No que tange às ameaças, foram pontuadas a evasão de servidores do setor de TI, a infraestrutura tecnológica vulnerável a ataques externos; e a ausência de uma Posic.

Nesse sentido, a Posic do IFPE é relativamente recente, pois foi criada no ano de 2017, tendo em essência o objetivo de estabelecer mecanismos de proteção dos dados, informações e conhecimentos gerados, bem como a redução dos riscos, preservando a DICA das informações em âmbito institucional. A política foi estruturada em conceituações e na determinação da criação de normas complementares que, por sua vez, disponha de um conjunto de procedimentos com a finalidade de tratar especificidades da gestão dos ativos de informação, tendo como exemplos as normas para uso do *e-mail*, o acesso físico e lógico, o correio eletrônico, a criptografia de dados, entre outros. Como determinações constantes nessa Posic, encontra-se a

de realizar atualização anual ou de acordo com a demanda de novos requisitos institucionais. Os documentos analisados demonstram que não existe uma abordagem direcionada para a segurança da PI, mas há a possibilidade de elaboração de normas específicas que atendam a essas demandas dos setores institucionais.

3.10 Gestão da Segurança no IF-Sertão-PE

A Posic do IF-Sertão-PE, promulgada no ano de 2016, foi desenvolvida para normatizar os diversos recursos e serviços prestados pelo departamento de TI da instituição, tendo como meta a melhoria da segurança dos usuários *on-line*, dos meios de comunicação de dados e dos sistemas computacionais. A Posic em questão foi criada conceituando os principais termos correlatos, tratando também das responsabilidades e competências dos usuários sobre os ativos da informação, da fundamentação legal e de regulamentos específicos, a exemplo do uso do correio eletrônico, da internet, dos laboratórios de informática e *backups*. Apesar de abrangente, com normas específicas para os diversos ativos de informação institucional, não foi evidenciada nessa política elementos que tratem, de forma direcionada, sobre a segurança da PI no IF-Sertão-PE.

O PDTI do IF-Sertão-PE foi elaborado utilizando como metodologia a preparação, o diagnóstico e o planejamento que reflitam a realidade da TI dos diversos *campi* da instituição para o biênio 2017-2018. Nessa perspectiva, em atendimento à legislação vigente, o referido PDTI apresenta os princípios que norteiam as ações e a gestão de recursos das diversas áreas de TIC em âmbito institucional, como coordenar as ações de proteção da informação e estabelecer um Comitê Gestor de Segurança da Informação e Comunicações, nesse caso, já existente e hierarquicamente ligado ao Gabinete da Reitoria. Ademais, o Comitê supracitado figura como uma "força" na análise SWOT realizada sobre as ações de TI no IF-Sertão-PE, e, entre as fraquezas, estão: o número insuficiente de servidores; a deficiência no mapeamento de processos; as documentações desatualizadas; e a deficiência da estrutura de redes e publicidade ineficiente das ações de TI. Entre as ameaças, encontra-se a perda de servidores para outras instituições; a falta de orçamento próprio; a mudança constante de dirigentes; e a decisão política que prevalece sobre critérios técnicos.

3.11 Gestão da Segurança no IFPI

O PDTI do IFPI, referente ao biênio 2016-2017, foi desenvolvido metodologicamente com base em três fases: preparação, diagnóstico e planejamento. A fase de preparação possui como objetivo a criação do plano de trabalho para elaboração do PDTI, enquanto a fase de diagnóstico tem por finalidade compreender a situação e as demandas de TI que devem ser atendidas, e, no caso da fase de planejamento, o objetivo é o de estabelecer planos e ações para atendimento às necessidades identificadas, contemplando recursos humanos, orçamentários e riscos.

Ainda na fase de diagnóstico, foi realizada a análise SWOT referente à TI da instituição, apresentando como algumas de suas ameaças: o orçamento limitado frente à demanda constante por serviços tecnológicos; os sistemas sem padronização; e a rotatividade constante de recursos humanos. Já relatados em seus pontos fracos encontra-se o baixo número de servidores; a insuficiência no adequado alinhamento entre a TI e os departamentos de ensino, pesquisa e extensão; a hospedagem de alguns serviços de dados e de *e-mail* fora da central de processamento de dados local; e a baixa segurança e integração dos sistemas de informação.

A preocupação com a proteção das informações é algo explicitado no PDTI do IFPI. De fato, tal afirmação se justifica com o disposto na seção princípios e diretrizes, que trata sobre o fomento da proteção do conhecimento, e na seção necessidades identificadas, sugerindo a instituição da gestão de segurança da Informação e comunicação. Nesse diapasão, a Posic do IFPI aborda 14 (quatorze) diretrizes, entre elas: a gestão de riscos, a gestão de ativos de informação, a segurança física e do ambiente, o uso de internet e de *e-mail* e tratamento da informação, com algumas delas já regulamentadas no próprio documento e outras exigindo a criação de normas específicas, garantindo a DICA das informações. A política supracitada determina que as informações com diferentes níveis de confidencialidade devem ser classificadas de acordo a legislação vigente, e, neste caso, incluem-se as PIs. Entretanto, não foi possível identificar normas complementares que pudessem abarcar a segurança dos ativos intelectuais.

3.12 Gestão da Segurança no IFRN

Instituída no ano de 2012, a Posic do IFRN foi elaborada com o propósito de estabelecer diretrizes, normas, procedimentos e responsabilidades para os diversos atores da instituição no correto manuseio, tratamento, controle e proteção da informação organizacional. Além de abordar a conceituação dos diversos termos relacionados à segurança da informação, a política traz como escopo os aspectos estratégicos, estruturais e organizacionais que servirão de base para a elaboração de documentos normativos para atendimento às especificidades institucionais, referindo-se ainda aos requisitos de segurança humana, física e lógica. A Posic também preconiza que as políticas e as normas devem ser amplamente divulgadas a todos os servidores do IFRN e apresenta o termo de responsabilidade.

De acordo com o documento disponível no *site* institucional, a PDTI vigente do IFRN é a do biênio 2014-2015 e tem por finalidade o diagnóstico, o planejamento e a gestão de recursos e de processos de TIC, abarcando todos os *campi* e setores da organização. Figurando como seus princípios e diretrizes está o de garantir a segurança em TIC, cabendo à Coordenação de Infraestrutura e Redes a promoção, a orientação e o acompanhamento da implementação da Posic no IFRN.

Na análise SWOT apresentada no PDTI do IFRN, a Posic figura como um dos pontos fortes, assim como o fato de dispor de um Comitê de Segurança da Informação instituído. Entre as fraquezas mencionadas, encontra-se o quadro de servidores limitado; a ausência de política de capacitação; a falta de um processo formal de segurança de TI; e a ausência de uma política de descarte de equipamentos. No tocante às ameaças, é possível ressaltar: a evasão de servidores de TI; a ausência de plano de carreiras específico para o setor; a ampliação acelerada do Instituto; e a mudança rápida das tecnologias. As limitações apresentadas trazem impacto sobre as ações de segurança, ao mesmo tempo, é preciso elucidar a ausência de mecanismos na Posic que visem à salvaguarda dos ativos intelectuais do IFRN.

3.13 Gestão da Segurança no IFS

O PDTI do IFS (2014-2019) baseia-se em diretrizes de documentos da administração pública federal, ancorado nos macroprocessos de: preparação, diagnóstico e planejamento. Na fase de diagnóstico, com o intuito de avaliar o panorama de TI no IFS, foi realizada uma avaliação por

meio da análise SWOT, na qual, figurando entre as suas ameaças, estão: o corte orçamentário; as mudanças de direcionamento de prioridades; a falta de padronização entre sistemas; e, em destaque, o quadro de servidores insuficientes. Nesse contexto, além do número reduzido de servidores, a análise dos pontos fracos apresenta: a alta rotatividade desses funcionários, assim como a ausência de política de capacitação; a infraestrutura deficiente em novos *campi*; a falha no processo de comunicação; e a ausência de integração entre os setores do IFS. A PDTI, por meio de sua seção princípios e diretrizes, determina a implementação de ações que efetivem a segurança da informação seguindo o que preconiza a DICA.

A preocupação com os ativos de informação institucional figurou como uma das prioridades do IFS, pois a primeira Posic foi promulgada no ano de 2011. A versão mais atual da política é a de janeiro de 2018 e traz atualizações em consonância com a Política de Gestão de Riscos e Controles Internos e a Política de Governança de TIC do IFS dos anos 2017 e 2018, respectivamente. Assim como ocorre na Posic de outros Institutos, essa política foi estruturada em um conjunto de documentos, incluindo as Normas, objetivando o cumprimento de obrigações e de métodos alinhados com as diretrizes da Posic e com os Procedimentos para fins de instrumentalizar o que está disposto nas normas. A referida política é explícita ao determinar que as informações de caráter sensível deverão passar por um processo de classificação e que os servidores públicos serão responsáveis pela segurança das informações que estão sob sua responsabilidade. Essa determinação reafirma o nível de responsabilidade na gestão do conhecimento por parte dos atores do NIT.

4 Considerações Finais

Os diversos documentos institucionais analisados demonstram que os DTIs dos IFs vivenciam uma série de dificuldades e limitações, entre as quais destacam-se: o baixo número de servidores e a alta rotatividade; a limitação orçamentária; e a ausência de padronização dos os sistemas; a insuficiência no adequado alinhamento entre o DTI e os departamentos de ensino, pesquisa e extensão da organização. Por conseguinte, esse cenário traz riscos aos diversos setores da instituição no tocante ao vazamento de informações. Em sua grande maioria, as Posics propõem a elaboração de normas específicas sobre segurança da informação para atendimento às particularidades dos setores. Todavia, não foi evidenciada a existência de tal norma direcionada ao NIT.

Ainda no tocante à Posic, nota-se que parte dessas políticas já trata sobre a classificação da informação, assim preconizado pela LAI. Contudo, esse direcionamento não se mostra presente nas Políticas de Inovação. Adicionalmente, não se evidenciou nos documentos institucionais analisados mecanismos que abordem especificamente a segurança da informação na perspectiva da PI e tampouco a relação direta entre as atividades do DTI e do NIT. Da mesma forma, não foi possível identificar na Política de Inovação desses núcleos uma abordagem direcionada para segurança da informação. No geral, essas políticas limitam-se a exigir dos envolvidos o sigilo das informações sobre o invento e a assinatura de um termo de confidencialidade.

Por fim, é preciso destacar que muitas das Posics necessitam ser revisitadas, já que é recomendado pela família da NBR 27000 que ocorram atualizações periódicas a cada 12 meses. Nesse sentido, sugere-se que, nas próximas atualizações, tanto a Posic quanto a Política de

Inovação possam se convergir, elaborando normas e procedimentos que pretendam ampliar a proteção dos ativos intelectuais no âmbito dos Institutos Federais.

Referências

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **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, 2013.

BRASIL. **Decreto n. 3.505, de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF: Casa Civil, 2000.

BRASIL. **Gabinete de Segurança Institucional**. Estatísticas de incidentes computacionais em órgãos de governo e vinculados – dados para diagnóstico, 2017. Brasília, DF, 2017. Disponível em: https://www.ctir.gov.br/estatisticas/. Acesso em: 15 dez. 2018.

BRASIL. **Lei n. 10.973, de 2 de dezembro de 2004.** Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo. Brasília, DF: Presidência da República, Casa Civil, 2004.

BRASIL. **Lei n. 11.892, de 29 de dezembro de 2008**. Dispõe sobre a criação dos Institutos Federais de Educação, Ciência e Tecnologia. Brasília, DF: Presidência da República, Casa Civil, 2008.

BRASIL. **Ministério da Educação**. Termo de Acordo de Metas e Compromissos Ministério da Educação. Institutos Federais. Brasília, DF, 2010.

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal. Brasília, DF: Presidência da República, Casa Civil, 2011.

BRASIL. **Ministério da Ciência, Tecnologia e Inovações e Comunicações**. Política de propriedade intelectual das instituições científicas e tecnológicas do Brasil: relatório FORMICT 2011. Brasília, DF, 2012.

BRASIL. **Ministério da Ciência, Tecnologia e Inovações e Comunicações**. Política de propriedade intelectual das instituições científicas e tecnológicas do Brasil: relatório FORMICT 2017. Brasília, DF, 2019a.

BRASIL. **Ministério da Educação.** Secretaria de educação profissional e tecnológica. 2019b. Disponível em: http://redefederal.mec.gov.br/expansao-da-rede-federal. Acesso em: 20 fev. 2019.

CERVO, Amado Luiz. BERVIAN, Pedro Alcino. SILVA, Roberto da. **Metodologia científica.** 6. ed. São Paulo: Pearson Prentice Hall, 2007.

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política de segurança da informação**. Rio de Janeiro: Ciência Moderna, 2008.

LEITE, Soraya Helena Coelho; IKEGAKI, Luciana Maria Baiocco. Confidencialidade e propriedade intelectual: aspectos gerais. **Publicações da Escola da AGU**, [*S.l.*], v. 2, n. 14, 2012.

LIMA JÚNIOR, G. A. Núcleo de Inovação Tecnológica: da criação ao momento atual. *In*: SOUZA, Ruberley Rodrigues de. (org.). **Pesquisa, Pós-Graduação e Inovação na Rede Federal de**

Educação Profissional, Científica e Tecnológica. 1. ed. Goiânia: Editora IFG, 2017. v. 1. p. 179-188.

LYRA, M. R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

OLIVEIRA, Hércules Rodrigues. Propriedade Intelectual: uma visão de Contrainteligência. **Revista Brasileira de Inteligência**, Brasília, DF, Abin, v. 67, 2012.

QUEIROZ NETO, J. P.; PEREIRA, J. L. A. R.; NAKA, M. H. A Evolução da Pesquisa na Rede Federal. *In*: SOUZA, Ruberley Rodrigues de. (org.). **Pesquisa, Pós-Graduação e Inovação na Rede Federal de Educação Profissional, Científica e Tecnológica**. 1. ed. Goiânia: Editora IFG, 2017. v. 1. p. 35-46.

RIOS, O. K. L.; RIOS, V. P. S.; TEIXEIRA, J. G. A. Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições Federais do Ensino Superior. **Revista Gestão & Tecnologia**, Pedro Leopoldo, v. 17, n. 1, p. 130-153, jan.-abr. 2017.

SÁ-SILVA, Jackson Ronie; DE ALMEIDA, Cristóvão Domingos; GUINDANI, Joel Felipe. Pesquisa documental: pistas teóricas e metodológicas. **Revista Brasileira de História & Ciências Sociais**, [*S.l.*], v. 1, n. 1, 2009.

SÊMOLA, M. **Gestão da Segurança da Informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SILVA, C. J. R. (org.). **Institutos Federais – Lei n. 11.892, de 29/12/2008**: comentários e reflexões. Brasília, DF: Editora do IFRN, 2009.

SILVA, D. R. P.; STEIN, L. M. Segurança da Informação: uma reflexão sobre o componente humano. **Ciências & Cognição**, [*S.l.*], v. 10, 2007.

SOUSA, Edilson Leite de. **Investigação do processo de aplicação das tecnologias da informação e comunicação na gestão dos Institutos Federais de Educação, Ciência e Tecnologia**. 2015. 130 p. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2015.

Sobre os Autores

Rodrigo Nogueira Albert Loureiro

E-mail:rodrigo.albert@reitoria.ifpe.edu.br
Doutor em Ciência da Propriedade Intelectual pela Universidade Federal de Sergipe (UFS) em 2020.
Endereço profissional: IFPE, Av. Prof. Luís Freire, n. 500, Cidade Universitária, Recife, PE. CEP: 50740-545.

Gabriel Francisco da Silva

E-mail: gabriel@ufs.br
Doutor em Engenharia de Alimentos pela Universidade Estadual de Campinas (UNICAMP) em 1999.
Endereço profissional: UFS, Av. Marechal Rondon, s/n, Rosa Elze, São Cristóvão, SE. CEP: 49100-000.

Márcio Vilar França Lima

E-mail: marciovilar@recife.ifpe.edu.br
Doutor em Química pela Universidade Federal de Pernambuco (UFPE) em 2011.
Endereço profissional: IFPE, Av. Prof. Luís Freire, n. 500, Cidade Universitária, Recife, PE. CEP: 50740-545.

Frederico Duarte de Menezes

E-mail: frederico.menezes@reitoria.ifpe.edu.br
Doutorado em Química pela Universidade Federal de Pernambuco (UFPE) em 2011.
Endereço profissional: IFPE, Av. Prof. Luís Freire, n. 500, Cidade Universitária, Recife, PE. CEP: 50740-545.