VI ENCONTRO NACIONAL DE PROPRIEDADE INTELECTUAL
25 a 28 de agosto de 2020
EVENTO ON-LINE • UFRN

SAFENIT: UM SOFTWARE PARA DIAGNÓSTICO E DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO PARA OS INSTITUTOS FEDERAIS

Rodrigo Nogueira Albert Loureiro[1] Gabriel Francisco da Silva[2] Frederico Duarte de Menezes[3] Marcio Vilar[4]
[1]Programa de Pós-Graduação em Ciência da Propriedade Intelectual- PPGPI
Universidade Federal de Sergipe – UFS – São Cristóvão/SE – Brasil
Instituto Federal de Pernambuco – IFPE – Recife/PE – Brasil
rodrigo.albert@reitoria.ifpe.edu.br
[2]Programa de Pós-Graduação em Ciência da Propriedade Intelectual- PPGPI
Universidade Federal de Sergipe – UFS – São Cristóvão/SE – Brasil
gabriel@ufs.br
[3]Pró-reitoria de Pesquisa, Pós-Graduação e Inovação - PROPESQ
Instituto Federal de Pernambuco – IFPE – Recife/PE – Brasil
frederico.menezes@reitoria.ifpe.edu.br
[4]Departamento de Controle e Processos Industriais, Coordenação do Curso Técnico em Química Industrial
Instituto Federal de Pernambuco – IFPE – Recife/PE – Brasil
marciovilar@recife.ifpe.edu.br

Resumo

A informação desponta como recurso intangível de maior valor para as organizações. Em decorrência disso, muitas são as tentativas de acesso e apropriação desse conhecimento de forma indevida, seja por meio de técnicas para enganar pessoas ou fragilidade na segurança dos artefatos tecnológicos. O Brasil figurou em 2019 como o segundo país do mundo em perdas financeiras por conta de ataques cibernéticos, que por sua vez, atingem pessoas físicas, empresas privadas e órgãos públicos. No contexto desses órgãos estão os Institutos Federais de Educação (IF) que ao longo da última década vem ampliando em quantidade e relevância a sua produção científica. Essa afirmação pode ser ratificada pelo número crescente de Propriedade Intelectual (PI) protegidos nos IF, realizado pelos Núcleos de Inovação Tecnológica (NIT). Diante desse cenário, faz-se necessário encontrar mecanismos que possam auxiliar os gestores desses Núcleos no diagnóstico de fragilidades de segurança da informação na gestão do conhecimento. Neste contexto, o presente trabalho tem por objetivo apresentar a ferramenta SafeNIT, um programa de computador idealizado para realizar o diagnóstico de vulnerabilidades na gestão do NIT, propondo diretrizes para o fomento de um ambiente seguro no âmbito desses Núcleos.

Palavras-chave: núcleo de inovação tecnológica; segurança da informação; vulnerabilidade.

1 Introdução

Atualmente, a informação desponta como recurso estratégico das instituições, conferindo-lhes maior produtividade, redução de custos e competitividade, independentemente do seu porte ou área de atuação (SÊMOLA, 2014). De acordo com Jungmann e Bonetti (2010) o conhecimento e a tecnologia na elaboração de novos produtos, processos e serviços inovadores representam mecanismo fundamental no desenvolvimento econômico, na geração de riquezas e qualidade de vida da população de um país.

Nesse sentido, o Brasil tem ampliado ao longo dos anos os investimentos em Pesquisa e Desenvolvimento (P&D). Como exemplo, no ano 2000 esse fomento representou 1,05% do Produto Interno Bruto (PIB), enquanto em 2017 esse percentual foi de 1,27% (BRASIL, 2018a). Tais investimentos refletiram no aumento da produção científica, considerando que o país ocupou em 2019 a 14º posição em um ranking mundial (SCIMAGO, 2020). Parte desse conhecimento foi passível de registro por meio das várias proteções conferidas pelos direitos da Propriedade Intelectual (PI), abarcado pelas patentes, marcas, desenhos industriais, programas de computador, topografia de circuitos integrados, entre outros.

Uma parte significativa dessas proteções ocorre por meio das Instituições Científicas e Tecnológicas (ICT), pois no ano de 2018, correspondeu a 26% do total de depósitos de pedido de patente no Brasil (INPI, 2019). Ao mesmo tempo que essas instituições têm realizado uma maior produção científica e proteção aos seus ativos intelectuais, faz-se necessário avaliar os riscos de vazamentos, de apropriação por terceiros e de ataques cibernéticos. O Brasil ocupa a segunda colocação em perdas financeiras em decorrência desse tipo de ataque, ultrapassando os US$20 (vinte) bilhões de dólares em prejuízos em apenas um ano (BRASIL, 2019a). No tocante aos órgãos públicos brasileiros, foram realizadas no ano de 2019, um total de 23.674 (vinte e três mil, seiscentos e setenta e quatro) notificações de incidentes cibernéticos (BRASIL, 2020). Esse cenário reforça a necessidade de se implementar mecanismos que possam mitigar os riscos de roubo de informações governamentais, em especial nas ICT, considerando as informações científicas estratégicas geridas nesses órgãos.

No âmbito das ICT estão os Institutos Federais de Educação, Ciência e Tecnologia (IF). Essas instituições fazem parte da Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPCT) criada a partir da promulgação da Lei n° 11.892 de 2008. O modelo de educação nos IF é pautado na indissociabilidade entre ensino, pesquisa e extensão, com foco na promoção de soluções técnicas e tecnológicas para atendimento as demandas da sociedade. Os IF possuem grande capilaridade, pois estão presente em todos os Estados do Brasil e no Distrito Federal, por meio de 38 (trinta e oito) instituições e 644 (seiscentos e quarenta e quatro) *campi* (BRASIL, 2019c).

Assim como outras ICT brasileiras, os IF têm desempenhado papel relevante na produção científica ao longo da última década, e por conseguinte, ampliado o número de ativos intelectuais. Essa afirmação pode ser corroborada por meio da posição ocupada pelos IF no ranking de maiores depositantes proteção à PI entre as ICT brasileiras no ano de 2018, pois figurou no segundo lugar em número de pedidos (BRASIL, 2019d). Essa posição pode ser atribuída ao empenho do Núcleo de Inovação Tecnológica (NIT) organizacional, que apesar de recente institucionalização, tem desempenhado papel relevante na salvaguarda do conhecimento nos IF. Entretanto, é preciso considerar algumas limitações desses Núcleos, dentre as quais: alta rotatividade de pessoal; baixa compreensão sobre o conceito de inovação; constituição recente; baixo recurso orçamentário; infraestrutura deficiente; entre outros (DESIDÉRIO E ZILBER, 2014).

Com o objetivo de auxiliar os gestores de inovação dos IF, encontra-se em desenvolvimento um programa de computador que visa mensurar a vulnerabilidade e promover mecanismos de segurança na gestão dos NIT. De acordo com Moreira (2001, p.22): “a vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações etc. Causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar os bem da empresa”.

O programa de computador supracitado, intitulado de *SafeNIT,* está sendo desenvolvido em duas perspectivas, a primeira delas, disponibiliza um questionário com perguntas que abordam os principais aspectos na gestão da informação desses Núcleos, tanto de procedimentos, quanto de infraestrutura, traçando um panorama de vulnerabilidade de acordo com as respostas inseridas. Essa primeira fase do sistema encontra-se registrada no Instituto Nacional da Propriedade Industrial (INPI) por meio da identificação BR512020001352, sendo esta etapa o objeto de apresentação deste artigo. A segunda perspectiva, em fase de desenvolvimento, visa realizar o tratamento de cada uma

dessas repostas, e estabelecer um conjunto de diretrizes para as melhores práticas em segurança da informação na gestão do NIT.

2 Metodologia

Para fins de construção das perguntas dispostas no software, foram utilizadas referências que tratam sobre o tema segurança da informação, por meio de autores especialistas (SÊMOLA,2014; ALEXANDRIA,2009; LYRA, 2015), das legislações vigentes sobre a matéria (BRASIL, 2011; BRASIL, 2018), dos documentos com as recomendações elaborado pelos órgãos públicos de controle (TCU, 2012; CGU, 2016) e principalmente da Norma Brasileira (NBR) 27002 intitulada de "Código de Prática para controles de segurança da informação" (ABNT, 2013). Da mesma forma, a experiência dos autores deste artigo na gestão de um NIT da RFEPCT serviu como base para a construção dos questionamentos.

A técnica de *Delphi* em grupo, uma derivação do método *Delphi* tradicional (WEBLER *et al*, 1991), e a validação de conteúdo por equipe formada por especialistas (MOREIRA, 2003), foram as metodologias utilizadas para avaliar se o questionário consegue medir o que se propõe e atribuir pesos para as perguntas e respostas. Essa equipe foi composta por 4 especialistas, sendo dois na área de pesquisa e inovação e os demais com formação em tecnologia da informação. A referida reunião ocorreu no âmbito do Instituto Federal de Pernambuco (IFPE) e foi autorizada por meio do processo 23294.010836.2019.88.

No tocante ao modelo matemático do *SafeNIT*, é composto por uma função logística que permite uma estimativa normalizada da vulnerabilidade em um ou mais NIT estudados, a partir das repostas obtidas no questionário da ferramenta. Para tanto, essas respostas são convertidas em valores numéricos discretos e em seguida aplicados na função mencionada, assim demonstrado pela Eq.1.

$$V = \frac{1}{1+e^{-\left(x-\frac{x_{max}+x_{min}}{2}\right)}} \qquad \text{Eq. 1}$$

Onde:
V = grau de vulnerabilidade do NIT, mediante as questões respondidas;
x = somatório ponderado das respostas dadas ao questionário, representado pela Equação 2;
x_{max} = máximo valor possível para o somatório ponderado;
x_{min} = mínimo valor possível para o somatório ponderado;
e = número de Euler, com valor aproximado de 2,71828.

$$x = \sum_{i=1}^{n} p_i q_i \,. \qquad \text{Eq.2}$$

Onde:
p = peso atribuído a cada pergunta do questionário
q = valor da resposta de cada pergunta

Com a aplicação da Equação 1, os valores possíveis de vulnerabilidade (V) do NIT estudados, limitados em um intervalo de [0,1], poderão ser colocados em uma única curva de vulnerabilidade, permitindo uma comparação mais simples de quais NIT apresentam maior ou menor risco, mediante as respostas dadas ao questionário proposto. Desta forma, todos os NIT terão valores de vulnerabilidade estimada diretamente normalizados, o que garantirá uma análise comparativa mais sistemática, diminuindo o grau de subjetividade na interpretação das respostas aos questionários.

A escolha deste modelo matemático advém da aplicação do mesmo em diversos outros problemas citados na literatura, cujos objetivos são centrados na análise de vulnerabilidade nos mais

diversos contextos como, por exemplo: desastres naturais tais como terremotos (SAPUTRA, 2017); deslizamento de terra (WU e TAKARA, 2008); e incêndios florestais (CHANG, 2013); ataques cibernéticos (LIU, 2017); segurança da informação em ambientes empresariais (LIU et al., 2007); dentre outros. Após a construção da curva de vulnerabilidade com os dados de todos os IF estudados, poderá se identificar grupos de vulnerabilidades com valores muito próximos que venham a indicar fatores em comum que caracterizem situações semelhantes de vulnerabilidade.

3 Resultados e discussões

Antes mesmo de apresentar os gráficos que demonstram a vulnerabilidade de um NIT por meio da simulação de respostas ao *SafeNIT*, convém abordar alguns dos questionamentos que compõe a ferramenta. Nessa apresentação estarão as perguntas, as possibilidades de resposta, os pesos, e as referências que serviram de base, tanto para a elaboração dos questionamentos, quanto as recomendações que serão inseridas na próxima versão do sistema.

A implementação de requisitos e controles de segurança da informação precisam estar em conformidade com o valor do conhecimento, mensurando os transtornos e impactos em caso de apropriação por terceiros dessa informação (ABNT, 2013). Nesse sentido, ressalta-se a necessidade do NIT em dispor de instrumentos mínimos que possam mensurar o valor do conhecimento a ser protegido. Esse requisito pode ser atendido por meio da aplicação de metodologias de valoração disponíveis na literatura, e comumente são incorporadas nas políticas de inovação ou em suas normas complementares. Nessa perspectiva, resta evidente a importância em se instituir documentos que normatizem as regras da gestão da inovação e a salvaguarda das PI nas atividades iniciais desses Núcleos. Dito isto, o primeiro bloco de perguntas da ferramenta versa sobre esses aspectos essenciais na gestão do NIT, e alguns desses questionamentos podem ser vislumbrados por meio Quadro 1.

Quadro 1 – Mecanismos de valoração e documentos que norteiam as atividades do NIT

Perguntas	Pesos	Respostas	Peso	Referências
O NIT dispõe de algum mecanismo de valoração da informação a ser protegida?	2	SIM	1	RAZGAITIS (2003); REITZIG (2005); QUINTELLA et al (2012).
		NÃO	2	
		Em elaboração	3	
As instruções referentes à Proteção da Propriedade Intelectual estão devidamente formalizadas nos documentos Institucionais?	2	Parcialmente	2	BRASIL (2018b); BRASIL (2019b).
		Plenamente	1	

Fonte: Elaborado pelos autores (2020)

Considerando a quantidade de pessoas que podem estar envolvidas no desenvolvimento de um ativo intelectual, incluindo pesquisadores, bolsistas, avaliadores, agentes do NIT, entre outros, torna-se imprescindível o uso de termos de confidencialidade e/ou responsabilidade para todos os envolvidos. Em linhas gerais, o primeiro termo tem por objetivo estabelecer que o usuário deve resguardar o sigilo das informações institucionais, enquanto o segundo esclarece as responsabilidades em caso de má utilização dos dados e recursos da entidade (SÊMOLA, 2014). A utilização desses termos também figura no escopo de ações essenciais em um NIT, e diante de sua importância, foi inserido no *SafeNIT* questionamento sobre a temática, assim exemplificado no Quadro 2.

Quadro2 – Utilização de documentos que exijam confidencialidade das informações

Pergunta	Peso	Respostas	Peso	Referências
O NIT da sua Instituição utiliza documentos que exijam a confidencialidade das informações em seu processo de gestão?	3	SIM	1	ABNT (2013); TCU (2012).
		NÃO	3	

Fonte: Elaborado pelos autores (2020)

Mitnick & William (2003) afirmam que a classificação da informação é um item essencial na salvaguarda dos dados em uma entidade, pois define orientações de como resguardar esse conhecimento em vários níveis, de forma alinhada ao seu valor. O Brasil dispõe da Lei 12.527 de 2011, conhecida como Lei de Acesso à Informação (LAI), preconizando a publicidade de informações de entidades públicas e permitindo restrições de acesso aos dados sensíveis. Contemplada nessas restrições enquadra-se: "prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico" (BRASIL, 2011). Contudo, para que seja possível classificar uma informação usando as diretrizes da LAI em um órgão público, faz-se necessário uma série recursos e infraestrutura, incluindo a criação de uma Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS), inviabilizando a implementação desse tipo de classificação em muitas instituições.

Nos casos em que o IF não disponha do mecanismo de classificação seguindo as orientações da referida lei, poderão ser utilizadas outras referências na implementação desse processo, a exemplo das recomendações da NBR 27002 e dos guias disponibilizados por alguns órgãos do governo federal como ABIN e TCU. Em decorrência disso, a ferramenta abarca questões que tratam sobre a proteção do conhecimento antes e depois do seu registro, conforme disposto no Quadro 3.

Quadro 3 – Classificação da informação e restrição de acesso

Perguntas	Pesos	Respostas	Pesos	Referências
De acordo com a Lei 12.527/2011 (Lei de Acesso à Informação), o NIT da sua Instituição classifica a informação em grau de sigilo?	2	SIM	1	BRASIL (2011); CGU (2016).
		NÃO	2	
Na sua Instituição, quem possui acesso às patentes no processo de gestão do NIT?	2	Apenas o(a) gestor(a) do NIT.	1	ABNT (2013); TCU (2012); LYRA (2015).
		Somente as pessoas classificadas pelo(a) gestor(a) do NIT.	2	
		Toda a equipe do NIT.	3	

Fonte: Elaborado pelos autores (2020)

A implementação de normas em segurança da informação dos órgãos públicos é realizada pelo Departamento de Tecnologia da Informação (DTI), que comumente conta com o suporte de um comitê de especialistas no assunto. Por força de lei, essas organizações devem dispor de um Política de Segurança da Informação e Comunicação (POSIC) alémde normas internas complementares, consonante com as atividades da instituição (BRASIL, 2018b). É fundamental que todos os atores de uma organização tenham conhecimento acerca desse documento, em especial os gestores do NIT, considerando o nível de sensibilidade das informações geridas por estes órgãos. Nessa perspectiva, o software traz questionamentos sobre o conhecimento e execução das normas da POSIC institucional por parte dos agentes desses Núcleos, e se possuem algum regulamento sobre segurança da informação que atenda as especificidades do setor, assim apresentado no quadro 4.

Quadro 4 – Aplicação da POSIC e documentos específicos do NIT sobre segurança da informação

Perguntas	Pesos	Respostas	Pesos	Referências
Sobre a POSIC (Política de Segurança da Informação Institucional), o NIT de sua Instituição:	3	Aplica	1	BRASIL (2018b); ABNT (2013); TCU (2012).
		Conhece	2	
		Não Conhece	3	
O NIT do qual você é gestor(a) dispõe de algum ato normativo específico que trate de procedimentos de segurança da informação?	3	SIM	1	SÊMOLA (2014); ABNT (2013); TCU (2012).
		NÃO	3	
		Em elaboração	2	

Fonte: Elaborado pelos autores (2020)

Para além da necessidade de se instituir uma POSIC no âmbito dos IF, o DTI deve promover sua divulgação para a comunidade acadêmica. Da mesma forma, o departamento mencionado deve realizar capacitações sobre práticas em segurança da informação, a partir de formações

customizadas considerando as singularidades do setor (SÊMOLA, 2014). Esses treinamentos devem ser teóricos e práticos, podendo ser ministrados em diversos meios, tais como palestras, mini cursos, distribuição de folhetos, simulações, baseado em web, e disponibilizados tanto de forma presencial, quanto à distância (TCU, 2012; ABNT, 2013). Nesse contexto, a ferramenta dispõe em seu questionário, perguntas que versam sobre a temática, conforme mostra o Quadro 5.

Quadro 5 – Treinamentos em práticas sobre segurança da informação ao gestor do NIT

Perguntas	Peso	Respostas	Pesos	Referências
Como gestor(a) do NIT, você recebe treinamento ou é capacitado(a) nos assuntos relativos às práticas de segurança da informação promovidas pelo Departamento de Tecnologia da Informação e Comunicação do seu Instituto?	3	SIM	1	SÊMOLA (2014); ABNT (2013); MITNICK & WILLIAM (2003).
		NÃO	2	

Fonte: Elaborado pelos autores (2020)

As informações passíveis de geração de uma PI nos IF podem ter sua origem por meio de fontes diversas. Todavia, comumente são oriundas de projetos de pesquisa ou Trabalhos de Conclusão de Curso (TCC). Dito isto, o *SafeNIT* busca avaliar a susceptibilidade das informações na ausência da interação entre o gestor do NIT e os departamentos de pesquisa e pós-graduação institucional. Essa avaliação ocorre a partir de indagações sobre procedimentos adotados por esses setores na busca de proteção das informações sensíveis, assim elencados no Quadro 6.

Algumas ações de fácil implementação podem ser adotadas a fim de evitar que o conhecimento passível de conversão em um ativo intelectual seja disponibilizado ao público antes de sua proteção. De forma sintética, tais ações passam pela atualização e alinhamento do arcabouço normativo institucional, incluindo a política de inovação, o regulamento dos projetos de pesquisa e dos programas de iniciação científica, bem como o regulamento de cursos lato sensu e stricto sensu. Algumas dessas abordagens podem ser visualizadas através do Quadro 6, porém a operacionalização desses processos será contemplada na segunda versão do programa.

Quadro 6 – Acompanhamento do NIT aos projetos de pesquisa e TCCs da pós-graduação

Perguntas	Pesos	Respostas	Pesos	Referências
O NIT é demandado pela Pró-Reitoria de Pesquisa para emitir pareceres acerca do potencial de inovação dos Projetos de Pesquisa desenvolvidos na Instituição?	2	SIM	1	ABNT (2013)
		NÃO	2	
Como gestor(a) do NIT, você atua em conjunto com o Departamento de Pesquisa Institucional nos procedimentos relativos ao sigilo e à confidencialidade das informações dos Projetos de Pesquisa, desde o seu cadastro até a sua execução, na Instituição?	3	SIM	1	ALEXANDRIA (2009); ABNT (2013).
		NÃO	2	
Existe alguma forma de acompanhamento, por parte do NIT, das pesquisas com potencial de inovação, desenvolvidas na Pós-Graduação (stricto e/ou lato sensu), com o intuito de garantir o sigilo das informações?	2	SIM	1	ABNT (2013)
		NÃO	2	

Fonte: Elaborado pelos autores (2020)

Na pesquisa realizada por Loureiro et. al, (2019) sobre a gestão da inovação nos IF, apresentou que os NIT das instituições avaliadas eram vinculados a Pró-Reitoria de Pesquisa, que por sua vez, agrega outros setores, a exemplo da pós-graduação e extensão. Esse compartilhamento de espaço enseja em uma situação de risco aos dados geridos pelo NIT, em decorrência do volume de pessoas que transitam nessa Pró-Reitoria, e por consequência, o difícil controle de acesso. Diante dessa afirmação, um dos itens que possui grande relevância em um processo de análise de vulnerabilidade está relacionado ao espaço físico disponível ao NIT, presente nas indagações (Quadro 7) do *SafeNIT*.

Quadro 7 – Instalações físicas do NIT

Perguntas	peso	Respostas	Pesos	
O NIT em que você é gestor(a) possui espaço físico próprio?	2	SIM	1	SÊMOLA (2014); ABNT (2014);
		NÃO	2	

Fonte: Elaborado pelos autores (2020)

Em um processo de implementação de práticas de segurança da informação no âmbito dos NIT é imprescindível que seja analisada a sua infraestrutura. Essa avaliação vai além das instalações físicas, devendo contemplar os artefatos tecnológicos, por meio de sistemas e equipamentos de informática. Para efícácia desse processo é necessáriocompreender o fluxo das informações geridas no setor e a sua armazenagem, que pode ser em meio físico ou digital. No caso deste último, poderá ocorrer de várias formas, a exemplo da utilização de softwares (próprio ou terceiros), servidor de arquivos institucional, e-mail, assim como o uso de dispositivos móveis de armazenamento de dados, a exemplo de pen-drive e disco rígido externo.

Para cada tipo de armazenamento é recomendado uma metodologia específica na inserção de requisitos de proteção, mas em todos os casos, convém a utilização de equipamentos e sistemas que permitam a criptografia dos dados. O uso de recursos criptográficos permite ocultar ou disfarçar uma informação por meio de métodos matemáticos, habilitando apenas aos usuários autorizados o acesso (ALVARENGA, 2010). As indagações apresentadas no Quadro 8 representam alguns dos mecanismos usados no *SafeNIT*para auxiliar na compreensão de como ocorre a gestão e salvaguarda da informação no NIT, bem como a sua infraestrutura.

Quadro 8 – Uso de artefatos tecnológicos na gestão da informação no NIT

Perguntas	Pesos	Respostas	Pesos	Referências
De que maneira as informações relativas às Propriedades Intelectuais da sua Instituição são armazenadas?	2	Meio físico	3	ALEXANDRIA (2009); ABNT (2013); SÊMOLA (2014).
		Meio digital	2	
		Outro	X	
O NIT utiliza algum software de gestão da Propriedade Intelectual?	2	Sim, sistema próprio.	1	MITNICK & WILLIAM (2003); TCU (2012); ABNT (2013);
		Sim, sistema de terceiros.	3	
		Não utiliza.	2	

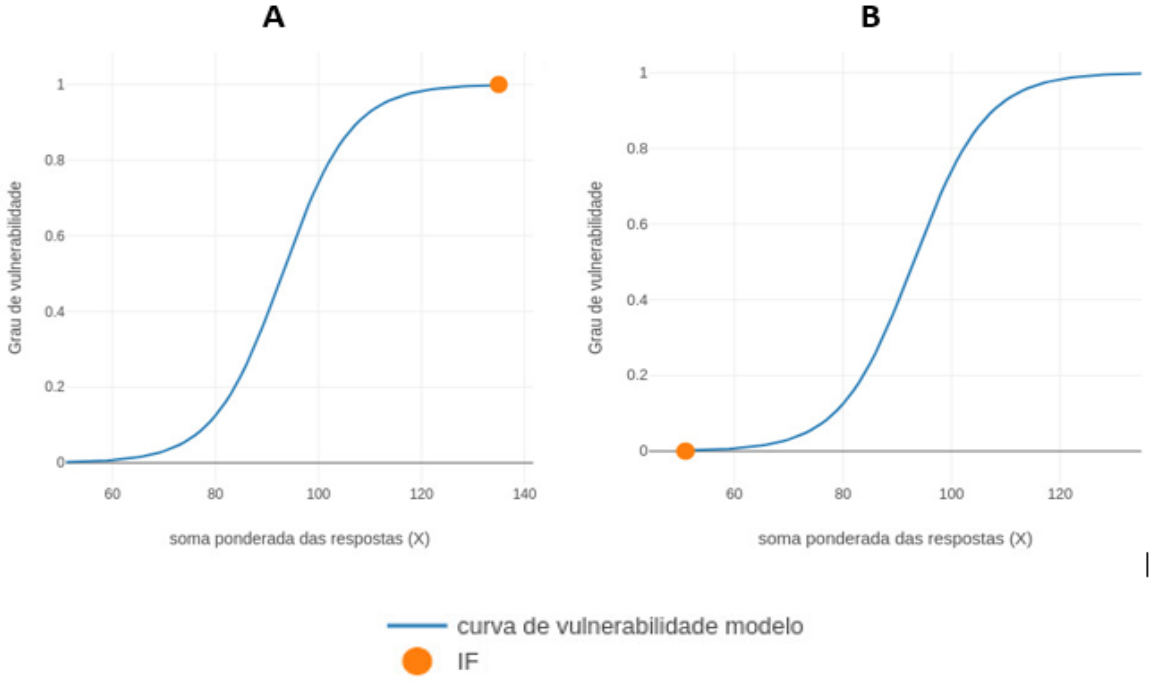
Fonte: Elaborado pelos autores (2020)

O desdobramento das perguntas acima elencadas gera uma série de cenários sobre o processo de gestão da informação por parte do NIT, que podem representar um ambiente mais ou menos vulnerável de acordo com os procedimentos adotados. Ainda que teoricamente a salvaguarda dos dados em meio digital possa representar um ambiente mais seguro, comparativamente ao meio físico, deve-se levar em consideração um gama de fatores: “Em qual local está sendo salvo?”; “Se possui criptografia”?; “Quem possui acesso?”; “Possui cópia de segurança”?; entre outros.Independentemente do meio utilizado para armazenamento das informações, deve-se considerar várias situações que ensejam na vulnerabilidade dos dados, conforme pontuado por Sêmola (2003 p.48):

> **Físicas** - Instalações prediais fora do padrão; salas de CPD mal planejadas; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em sala com armários e fichários estratégicos; risco de explosões, vazamento ou incêndio. **Naturais** - Computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento umidade e de temperatura etc. **Hardware** - Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação. **Software** - Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário. **Mídias** - Discos, fitas, relatórios e impressos podem ser perdidos ou danificados (SÊMOLA, 2003 p. 48).

Como visto, diversos fatores devem ser levados em consideração na gestão segura da informação. O olhar sobre tais aspectos, torna-se um desafio para os gestores dos NIT, seja pelo desconhecimento técnico sobre o assunto e/ou a falta de infraestrutura, bem como ausência de apoio do departamento de informática. As perguntas apresentadas ao longo deste artigo pode favorecer a visualização de falhas na segurança na gestão das informações por parte desses gestores. Em uma perspectiva mais prática, é possível avaliar o grau de vulnerabilidade a partir das respostas inseridasno sistema *SafeNIT*, conforme demonstrado na Figura 1.

Figura 1 – Representação gráfica da vulnerabilidade de dois NIT por meio do SafeNIT



Fonte: Elaborado pelos autores (2020)

O resultado acima é reflexo de uma simulação utilizando respostas antagônicas, onde na situação "A" apresenta que o NIT possui um alto grau de vulnerabilidade, enquanto o cenário "B" demonstra que esse órgão adota práticas que minimizam o risco de perda e roubo de informações importantes. Essa fase de dignóstico torna-se fundamental na implementação de uma gestão da segurança da informação, mas é preciso que após essa fase existam diretrizes para auxiliar os gestores na adoção de protocolos que visem salvaguardar o conhecimento sensível. Dito isto, a segunda versão do *SafeNIT*, que encontra-se em desenvolvimento, contemplara uma série de procedimentos baseado nas melhores práticas para promoção de um ambiente seguro, de forma adptada as atividades de um NIT.

3 Conclusões

Na medida em que os IF ampliam sua produção cientifica e tecnológica, há também uma maior responsabilidade na gestão do conhecimento por parte dos NIT, principalmente em decorrência dos diversos riscos de ataques cibernéticos e roubo de informações. Diante dessa realidade, o artigo em tela objetivou apresentar o software SafeNIT, como um instrumento que visa auxiliar os gestores do NIT no diagnóstico de vulnerabilidades concernentes à segurança da informação. Com isto, espera-se contribuir com o fomento de discussões científicas sobre temas relacionados à segurança do conhecimento passível de geração de PI e que a ferramenta possa subsidiar o desenvolvimento de novos trabalhos, principalmente, considerando a ausência de estudos com essa temática. Neste contexto, encontra-se em desenvolvimento a segunda versão do SafeNIT, abarcando além do

diagnóstico, diretrizes e práticas em segurança da informação, para que os NIT possam adotar medidas que tornem o ambiente menos suscetível à apropriação dos dados sensíveis por terceiros.

4 Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

5 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, 2013.

ALEXANDRIA, J. C. S. **Gestão de Segurança da Informação-uma proposta para potencializar a efetividade da Segurança da Informação em ambiente de pesquisa científica**. 2009. Tese de Doutorado. Universidade de São Paulo.

ALVARENGA, L. G. **Criptografia Clássica e Moderna**.2ª Ed. Clube de Autores, 2010.

BRASIL. **Decreto nº. 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, 2018b.

BRASIL. **Gabinete de Segurança Institucional**. Estatísticas de incidentes computacionais em órgãos de governo e vinculados – dados para diagnóstico, 2019c**.** Brasília: 2020. Disponível em: <https://www.ctir.gov.br/estatisticas/>. Acesso em: 30mai 2020.

BRASIL. **Guia de orientação para elaboração da política de inovação nas ICT** /organizadora, Adriana Regina Martin et al. -- Brasília: Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2019b.

BRASIL. **Lei n° 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º... e dá outras providências. Diário Oficial [da] República Federativa do Brasil, 2011.

BRASIL. **Lei n°11.892, de 29 de dezembro de 2008**. Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências. Brasília, DF: Presidência da República, Casa Civil, 2008.

BRASIL. **Ministério da Ciência, Tecnologia e Inovações e Comunicações**. Política de propriedade intelectual das instituições científicas e tecnológicas do Brasil: relatório FORMICT 2018. Brasília. 2019d.

BRASIL. **Ministério da Ciência, Tecnologia e Inovações**. Dispêndio nacional em C&T por valores. 2018a.Disponível em: <https://www.mctic.gov.br/mctic/opencms/indicadores/detalhe/recursos_aplicados/indicadores_consolidados/2.1.1.html>. Acesso em: 02 fev 2020.

BRASIL. **Ministério da Educação.** Secretaria de educação profissional e tecnológica,2018c. Disponível em: <http://redefederal.mec.gov.br/expansao-da-rede-federal>. Acesso em: 20 fev 2019.

BRASIL. Senado Federal. **Brasil é 2º no mundo em perdas por ataques cibernéticos 2019a**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>. Acesso em: 04 dez 2019.

CHANG, Yu et al. **Predicting fire occurrence patterns with logistic regression in Heilongjiang Province**, China. LandscapeEcology, v. 28, n. 10, p. 1989-2004, 2013

CGU - Controladoria Geral da União. **Aplicação da lei de Acesso à Informação na Administração Pública Federal.** 2º Edição, Brasília, 2016.

INPI - Instituto Nacional Da Propriedade Industrial. **Relatório de atividades INPI 2018**. Brasília. 17 de janeiro de 2019. Disponível em: http://www.inpi.gov.br/sobre/relatorios-de-atividades. Acesso em: 20 mar 2020.

LIU, Wei; TANAKA, H.; MATSUURA, K. **Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms**. IPSJ Digital Courier, v. 3, p. 585-599, 2007.

LIU, Enhao. **Logistic Regression Model for Predicting Warning "Incident" Rates and Implications for the Common Vulnerability Scoring System**. 2017. Tese de Doutorado. The Ohio State University.

LOUREIRO, R. N. A.; SILVA, G. F.; GARCEZ JÚNIOR, S.; SANTOS, J. A.; VILAR, M.; MENEZES; F. D. Innovation management in the Federal Institutes of Education, Science and Technology of the Brazilian Northeast: An overview. **International Journal for Innovation Education and Research,** v. 7, n. 7, abr. 2019.

LYRA, M. R. **Governança da Segurança da Informação**. Edição do Autor – Brasília, 2015.

MITNICK, K.; SIMON, D. **A Arte de Enganar–Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson Education, 2003.

QUINTELLA, C. M.; TEODORO, A.F.O. **Desmistificando a estratégia tecnológica: Uma abordagem prática sobre prospecção tecnológica, valoração, vantagens econômicas, ambiente deinovação e jargão técnico**. Valoração de tecnologias. In: Cristina M. Quintella. (Org.) 1ed. Salvador, BA: EDUFBA, 2012.

RAZGAITIS, R. **Valuation and Princing of Technology-Based Intellectual Property**. Hoboken, New Jersey. John Wiley & Sons, 2003.

REITZIG, M. **Methods for patent portfolio valuations: challenges for and responses by academia**. Presentation at OECD/EPO Meeting. Berlin. 2005.

SCIMAGO. **Scimago Institutions Rankings, journal & country rank, 2020**. Disponível em: < https://www.scimagojr.com/countryrank.php?year=2019>. Acesso em: 01 jun 2020.

SAPUTRA, Aditya et al. **Seismic vulnerability assessment of residential building susing logistic regression and geographic information system (GIS) in Pleret Sub District (Yogyakarta, Indonesia)**. Geoenvironmental Disasters, v. 4, n. 1, p. 11, 2017.

SÊMOLA, M. **Gestão da Segurança da Informação. Uma visão executiva**. 2. Ed. Elsevier Brasil, 2014.

SÊMOLA, M. Gestão da Segurança da Informação. 3.ed. Rio de Janeiro: Campus, 2003.

TCU – Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília: TCU, 2012.

WEBLER, T. et al. A novel approach to reducing uncertainty: the group Delphi. Technological forecasting and social change, v. 39, n. 3, p. 253-263, 1991.