ANÁLISE DE RISCOS APLICADA AO SISTEMA INTEGRADO DE GESTÃO DE ATIVIDADES ACADÊMICAS - SIGAA: um estudo do módulo *Stricto Sensu*.[1]

Rafaela Romaniuc Batista[2]
Wagner Junqueira de Araújo[3]

RESUMO:
Os sistemas de informação surgem no cerne do problema envolvendo a segurança da informação, os quais acompanham as inovações tecnológicas da atualidade, por meio da automatização de processos com sistemas integrados. Ao se considerar a dimensão das atividades administrativas e acadêmicas da Universidade Federal da Paraíba - UFPB, o sistema integrado possui uma abrangência e uma complexidade que exigem cuidados específicos no que se refere à criação, uso, armazenamento e compartilhamento das informações ao longo de todo o seu ciclo de vida, o que demanda uma preocupação quanto aos padrões de segurança. Cabe à segurança da informação, por meio de seus controles, proteger os sistemas de informação. A análise de riscos de segurança da informação nos sistemas de informação acadêmicos torna-se necessária por ser informação um importante ativo com riscos inerentes em todo o seu ciclo de vida. Perante o exposto, a presente pesquisa tem por objetivo estudar os possíveis riscos de segurança da informação que podem afetar o Sistema Integrado de Gestão de Atividades Acadêmicas – SIGAA - *Stricto Sensu*, da UFPB, de modo a identificar ameaças e vulnerabilidades. Esta pesquisa se caracteriza como uma pesquisa descritiva, com abordagem quanti-qualitativa, tendo como método o estudo de caso. Referente aos métodos de coleta de dados serão utilizados pesquisa documental, desenvolvimento de entrevistas na Superintendência de Tecnologia da Informação da UFPB e utilização de scanner de vulnerabilidades no SIGAA - *Stricto Sensu*. Espera-se com esta pesquisa contribuir na identificação de possíveis ameaças e vulnerabilidades, e propor medidas que possam mitigar os riscos.

Palavras-chave: Segurança da informação. Análise de Risco. Sistema de Informação. Normas de Segurança da Informação. Políticas de Segurança da Informação.

RISK ANALYSIS APPLIED TO ACADEMIC ACTIVITIES MANAGEMENT INTEGRATED SYSTEM - SIGAA: a study of the module Stricto Sensu.

ABSTRACT:
The term "security" refers to the idea that something valuable should be stored or secured. Information systems arise in the heart of the problem involving information security, which accompany the technological innovations of our time, by automating processes with integrated systems. Considering the size of the administrative and academic activities of the Federal University of Paraíba, the integrated system has a scope and complexity that require special care with regard to the creation, use, storage and sharing of information throughout your lifecycle, which demands a concern about safety standards.It is up to information security through its controls to protect information systems. The information security risk analysis on academic information systems becomes necessary because information turns to be an important asset with inherent risks throughout their life cycle. Given the above, this

[1] Pesquisa de mestrado em desenvolvimento no Programa de Pós-Graduação em Ciência da Informação – PPGCI da Universidade Federal da Paraíba – UFPB.
[2] Mestranda do Programa de Pós-graduação em Ciência da Informação pela Universidade Federal da Paraíba, Brasil.
[3] Professor do Departamento de Ciência da Informação da Universidade Federal da Paraíba, Brasil.

research aims to study the possible information security risks that may affect the Academic Activities Management Integrated System, stricto sensu, of UFPB, in order to identify threats and vulnerabilities. This research is characterized as a descriptive research with qualitative and quantitative approach and method as the case study. Regarding methods of data collection will be used documentary research, interviews development and use of vulnerability scanner, at the Information Technology Superintendent of the Federal University of Paraíba. It is hoped that this research help identify potential threats and vulnerabilities, and propose measures that can minimize the risk to an acceptable level.

Keywords: Information Security. Risk Analysis. Information System. Information Security Standards. Information Security Policy.

1 INTRODUÇÃO

Na atual sociedade, informação é um elemento transformador, a partir do qual é possível tomar decisões, sejam estratégicas ou operacionais, ou usar para apoiar as decisões já tomadas. Observa-se que McGee e Prusak (1994, p. 3) já afirmavam que há uma transição da economia industrial para a economia da informação e prediziam que "[...] nas próximas décadas, a informação, mais do que a terra ou o capital, será a força motriz na criação de riquezas e prosperidade". Com a relevância da informação na sociedade contemporânea, aumenta-se a preocupação com sua proteção. Ao refletir sobre a segurança da informação na atual sociedade, os sistemas de informação surgem no cerne desse problema, pois não basta investir em tecnologia e alinhá-la aos objetivos do negócio, é preciso manipular a informação com segurança.

Historicamente, os sistemas de informação das universidades públicas foram alvo de duras críticas, pelos seus sistemas obsoletos ou inexistentes. Porém, a realidade atual abrange universidades informatizadas sendo auxiliadas em suas atividades meio e fim por sistemas integrados. Com isso, as universidades passaram a depender das inovações tecnológicas e quanto mais eficazes e eficientes seus sistemas de informação forem, mais ágil e rápido será o tempo de resposta.

A tecnologia está em constante evolução, seja devido às inovações seja pela necessidade de melhoria contínua. Há várias formas de se contribuir para essa melhoria, uma delas seria uma gestão de segurança da informação eficiente. Sendo assim, considera-se que analisar o risco dos sistemas de informação pode contribuir para a melhoria desses sistemas auxiliando-os na segurança da informação, por meio dos estudos das ameaças e vulnerabilidades a eles inerentes, porém muitas vezes imperceptíveis no dia a dia da instituição.

Mandarino Junior e Canongia (2010, p. 13) destacam a importância da segurança cibernética como função estratégica de Estado, essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, Informação, dentre outras. Observa-se que os países devem defender suas infraestruturas críticas, entre elas a informação, que por ser um importante ativo precisa ser adequadamente protegido.

Ameaças de segurança da informação existem em variadas formas, desde erros humanos e falhas do sistema até espionagem industrial e crimes cibernéticos. Ameaças são os eventos que exploram as vulnerabilidades e resultam em danos para o sistema ou organização, enquanto vulnerabilidades são as fraquezas que podem ser exploradas de modo a comprometer a segurança de sistemas ou informações, por meio da fragilidade de um ativo ou grupo de ativos, sendo que um incidente ocorre quando as vulnerabilidades são efetivamente exploradas (BEZERRA, 2013, p. 3).

No Brasil, o Centro de Tratamento de Incidentes de Segurança de Rede de Computadores da Administração Pública Federal - CTIR Gov registrou recorde histórico envolvendo o registro de incidentes de segurança da informação, o que colocou o país na segunda posição no rol dos demais países destinatários de incidentes (CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDE DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL, 2015, p. 4). Nesse caso, com exceção do quantitativo de incidentes registrados nos Estados Unidos da América, o quantitativo de incidentes no Brasil ultrapassa a soma de incidentes dos demais países, o que alerta para a relevância do tema segurança da informação.

Observa-se que os procedimentos da segurança da informação são caracterizados pela evolução contínua, pois novas formas de proteção surgem sempre que um novo ataque ou vulnerabilidade é identificado, de maneira que um ciclo é formado. Logo, deve se ter em mente que, da mesma maneira que os ataques evoluem ao longo do tempo, a segurança deve ser contínua e evolutiva (NAKAMURA; GEUS, 2007, p. 25).

No âmbito da segurança da informação, a ameaça abrange os eventos indesejados que englobam os aspectos tecnológicos, os processos executados e, principalmente, as pessoas que em algum momento interagem com a tecnologia. Nesse contexto, o risco acaba sendo a probabilidade de a ameaça se concretizar. A gestão de riscos se faz necessária, pois objetiva controlar de forma adequada os riscos organizacionais de modo que o ciclo de vida da

informação seja protegido das ameaças, garantindo a segurança e a correta disponibilidade da informação no ambiente organizacional.

Observa-se que é impossível projetar e desdobrar um ambiente totalmente livre de riscos. Contudo, a redução significativa do risco é possível, frequentemente com pouco esforço. Os riscos para uma infra-estrutura de TI não são todos baseados em computador e, na verdade, muitos riscos são provenientes de fontes não computacionais. Logo, é importante considerar todos os riscos possíveis durante a execução de analise de risco para uma organização (TITTEL et al., 2006, p. 185). Nesse sentido, a gestão de risco tem como foco a identificação e o tratamento dos riscos. O objetivo é adicionar o máximo de valor sustentável às atividades da organização, o que aumenta a probabilidade de sucesso, reduz a probabilidade de falha e a incerteza de atingir os objetivos globais da organização (AIRMIC; ALARM; IRM, 2002, p. 2).

Com a importância do estudo de riscos nas organizações, considera-se que, no âmbito das universidades brasileiras, ocorre o aumento da preocupação da segurança da informação em seus diversos processos que estão sendo dinamizados com o uso de sistemas de integração, utilizados para possibilitar a interação entre suas atividades acadêmicas. Como um dos sistemas desenvolvidos com essa finalidade, o Sistema Integrado de Gestão de Atividades Acadêmicas - SIGAA permite a integração da atividade meio (área administrativa) com a atividade fim (área acadêmica) de universidades, possibilitando o inter-relacionamento de sistemas e auxiliando na gerência das informações. A Universidade Federal da Paraíba - UFPB implantou esse sistema no intuito de apoiar o desenvolvimento do ensino, pesquisa e extensão, o que exige cuidados específicos no que se refere à criação, uso, armazenamento e compartilhamento das informações, demandando da organização a preocupação quanto aos padrões de segurança que sejam compatíveis com o valor informacional. Diante do exposto, a pesquisa justifica-se pela relevância do estudo dos riscos no SIGAA da UFPB, de modo a contribuir na identificação de possíveis ameaças e vulnerabilidades e, por consequência, propor sugestões para tornar o sistema mais seguro.

A necessidade de segurança aumenta à medida que a rapidez e eficiência nos processos de negócios são ampliadas por meios dos sistemas, porém a ausência de segurança pode vir a resultar em grandes prejuízos e falta de oportunidades de negócios. Há uma variedade de fatores que justificam a preocupação com a segurança contínua: a evolução dos ataques, a emergência de novas vulnerabilidades provenientes das inovações tecnológicas, o aumento da conectividade, além do aumento dos crimes digitais. Quanto à necessidade de

segurança da informação, o Tribunal de Contas da União elaborou o Relatório de Avaliação da Governança de Tecnologia da Informação na Administração Pública Federal, o que resultou no Acórdão do TCU de nº 3117/2014, onde se esclarece que das 355 organizações públicas federais pesquisadas, apenas 38% declararam identificar os riscos de TI dos processos críticos de negócio, sendo que apenas 21% tratam esses riscos, revelando que a maior parte da Administração Pública Federal não compreende os riscos de TI à que estão sujeitas, sua probabilidade e impacto no negócio e, mesmo as que compreendem, não realizam o tratamento dos riscos de modo a mantê-los em níveis e custos aceitáveis. O Tribunal concluiu afirmando que "uma organização que não faz esse mínimo de gestão de risco fica a mercê da sorte para realizar seus objetivos estratégicos", não é aceitável uma organização não conhecer os riscos associados aos processos de negócio mais críticos, tendo em vista seu tratamento (TRIBUNAL DE CONTAS DA UNIÃO, 2014, p. 4-29).

Diante desse cenário, a pesquisa propõe-se a responder ao seguinte questionamento: quais as ameaças e vulnerabilidades que geram riscos para o SIGAA, módulo *Stricto Sensu,* da UFPB?. Para tanto, faz-se necessário estudar os possíveis riscos de segurança da informação que podem afetar o SIGAA - *Stricto Sensu,* da UFPB.

2 PROCEDIMENTOS METODOLÓGICOS

2.1 CARACTERIZAÇÃO DA PESQUISA

Para atender ao objetivo proposto a presente pesquisa será descritiva, de abordagem quanti-qualitativa, optando-se pelo método de investigação de estudo de caso e utilizando para análise uma metodologia de análise de riscos.

O tipo de pesquisa descritiva é útil quando se pretende descrever o tema ou problema de pesquisa por meio da coleta de dados. A ideia é medir, avaliar ou coletar dados sobre variados aspectos do fenômeno a ser pesquisado. Assim, esse tipo de pesquisa visa descrever as características de determinado fenômeno ou o relacionamento entre variáveis, sendo que sua característica mais relevante encontra-se no uso de técnicas padronizadas de coleta de dados (SAMPIERI HERNÁNDEZ; COLLADO FERNÁNDEZ; LUCIO BAPTISTA, 2006, p. 101; GIL, 2012, p. 28). Nesta pesquisa serão descritos aspectos de riscos envolvendo o sistema em questão, tornando possível conhecer melhor a segurança da informação.

No contexto da análise de risco, verifica-se que existem dois prismas de análise: o qualitativo, útil quando falta disponibilidade de dados ou quando são precários, pois essa análise baseia-se em valores referenciais. E a análise quantitativa, útil quando há disponibilidade de dados e esses são confiáveis, sendo a análise feita com base em valores absolutos (DANTAS, 2011, p. 55). Araújo (2009, p. 53) fez uma síntese comparativa das características entre a análise de risco quantitativa e qualitativa identificando que a análise quantitativa é uma análise de custo/benefício, objetiva e de alta comunicação, além de ser mensurável em valores específicos, enquanto a análise qualitativa oferece resultados úteis e significativos, podendo fazer uso de opiniões. Para tanto, a abordagem quanti-qualitativa se faz necessária, o que permitirá atingir os objetivos específicos da pesquisa correspondentes a: identificar os ativos informacionais do SIGAA - *Stricto Sensu*/UFPB, analisar as ameaças, vulnerabilidades e controles; avaliar as consequências dos riscos identificados; e propor medidas para minimizar os riscos identificados e avaliados.

Por sua vez, trata-se de um Estudo de Caso que investiga de forma intensiva um fenômeno ou objeto ao longo do tempo dentro do seu ambiente natural, em um ou poucos locais. Vários métodos de coleta de dados, como entrevistas, observações, documentos pré-gravados e dados secundários, podem ser empregados, sendo que inferências sobre o fenômeno de interesse tendem a ser ricas, detalhadas e contextualizadas (BHATTACHERJEE, 2012, p. 93, tradução nossa). Para Gil (2012, p. 57-58), o estudo de caso é o estudo profundo e exaustivo do objeto de pesquisa, o que, nesse caso, possibilitará à pesquisa um conhecimento mais detalhado do SIGAA - *Stricto Sensu*.

2.2 CONTEXTUALIZAÇÃO DO OBJETO DE PESQUISA

No intuito de automatizar as atividades meio e fim, a Universidade Federal da Paraíba adquiriu o Sistema Integrados de Gestão (SIG), e trabalha atualmente na implantação dos módulos de acordo com sua realidade organizacional. O sistema SIG foi desenvolvido pela Universidade Federal do Rio Grande do Norte (UFRN), lançado em 2004, visando possibilitar a interação entre a área administrativa e acadêmica. Esse sistema visa propiciar a integração das informações organizacionais de modo a auxiliar universidades públicas em seu negócio. Um dos maiores benefícios dos SIG UFRN é a integração entre os sistemas, pois engloba os sistemas desde a área administrativa, atividade meio, até a área acadêmica, atividade fim das universidades.

SIG UFRN abrange os sistemas: administrativo, patrimonial, acadêmico, de gerenciamento eletrônico de documentos e de planejamento de projetos. Cada um desses sistemas existentes no SIG é composto por módulos, portais e pontos de acesso aos demais sistemas. O objeto deste estudo será o módulo SIGAA - *Stricto Sensu*, que congrega operações relativas à gerência de mestrado e de doutorado, tendo sido implantado de modo a auxiliar a Pró-Reitoria de Pós-Graduação da UFPB. As principais funções deste módulo são controlar o processo seletivo, a estrutura curricular, matrículas e emissão de diplomas. O módulo *Stricto Sensu* é composto de 129 operações que auxiliam os perfis em suas funcionalidades (WIKIUFRN, 2014).

A Superintendência de Tecnologia da Informação (STI) da UFPB, órgão suplementar e auxiliar de direção superior da Reitoria da UFPB, instituída por meio de Resolução nº 40 de 2013 do CONSUNI de 16 de dezembro de 2013, tem como objetivo prover serviços, acadêmicos e institucionais, de tecnologia da informação e comunicação. Além disso, a STI deve apoiar o desenvolvimento do ensino, pesquisa, extensão, gestão e serviços à comunidade, sendo o órgão responsável pela implantação e manutenção dos SIG na UFPB (UNIVERSIDADE FEDERAL DA PARAÍBA, 2013, 2015).

Nesse contexto, entende-se que analisar os riscos de segurança da informação do sistema acadêmico da UFPB, módulo *Stricto Sensu*, poderá contribuir para a melhoria da segurança da informação, no sentido de ampliar a visão para os riscos concernentes ao sistema, mitigando assim as vulnerabilidades e ameaças.

2.3 UNIVERSO E AMOSTRA DA PESQUISA

Para esta pesquisa, considera-se como universo os 19 gestores lotados na STI e responsáveis por manter o SIGAA – *Stricto Sensu*, bem como o ambiente de produção do sistema, composto por: instalações, recursos humanos, organização, software e hardware/rede.

No que tange a amostra, foi utilizada a amostragem intencional ou de seleção racional. A amostragem intencional "constitui um tipo de amostragem não probabilística e consiste em selecionar um subgrupo da população que, com base nas informações disponíveis, possa ser considerado representativo de toda a população." (PRODANOV, FREITAS, 2013, p. 98-99). A amostra consiste dos cinco gestores do STI que possuem atribuições diretas ligadas ao sistema, à rede em que o sistema se encontra e aos recursos humanos, os quais, segundo o organograma da STI, correspondem a: Gerente de Sistema de Informação, Gerente de

Segurança da Informação e Gerente de Base de Dados, os quais se encontram dentro da Coordenação de Gestão da Informação - CGI; Coordenador da Rede da UFPB; e Secretaria Executiva, por sua responsabilidade direta na contratação de pessoas que irão trabalhar naquela unidade.

Considerando que a CGI tem como atribuição "coordenar toda execução de planejamento, desenvolvimento e implantação dos serviços relacionados aos sistemas administrativos e acadêmicos" (UFPB, 2013, p. 5), escolhemos os gestores ligados à Coordenação de Gestão da Informação pela necessidade de obter informações detalhadas ligadas ao sistema SIGAA-*Stricto Sensu*. A coordenação de Rede tem como atribuição administrar a rede corporativa de computadores da UFPB, garantindo sua segurança, eficiência e disponibilidade (UFPB, 2013, p. 7), sendo responsável pela infraestrutura e operação da rede. Considerando que sua atribuição abrange todo o suporte à rede, inclusive a rede que disponibiliza o sistema SIGAA – *Stricto Sensu*. A secretaria executiva responsável pela gestão de pessoas e controle de patrimônio inclui-se na pesquisa para responder aos questionamentos relativos à contratação de pessoas que irão trabalhar diretamente com o sistema em questão. Logo, observa-se que a base para a escolha da amostra teve como variáveis o fato de serem gestores inerentes ao sistema acadêmico objeto de estudo, portanto de importância para as atividades fim da instituição, o que evidencia a representatividade da amostra para o universo em questão.

2.4 TÉCNICAS DE COLETA DE DADOS

Para o procedimento de coleta de dados, será adotado um conjunto de instrumentos que permitirá a obtenção de dados em três momentos específicos: pesquisa documental, desenvolvimento de entrevista e utilização de scanner de vulnerabilidades.

No intuito de auxiliar a atingir os objetivos específicos, será utilizada a pesquisa documental como técnica de coleta de dados. No que concerne a essa técnica, Carvalho (1989, p. 154) afirma que a pesquisa documental é aquela que se vale de documentos cientificamente autênticos, isto é não fraudados, sendo considerada de amplo uso nas ciências sociais. Assim, a presente pesquisa pretende fazer uso de normas da Associação Brasileira de Normas Técnicas (ABNT); apostila de gestão de riscos da Rede Nacional de Ensino e Pesquisa (RNP); leis, decretos, instruções normativas vigentes no âmbito da Administração Pública Federal;

além de resoluções e relatórios internos da UFPB, *frameworks*, relatórios de pesquisa e normas internacionais.

A técnica de coleta de dados entrevista consiste no encontro entre duas pessoas onde, mediante conversa formal, pretende-se obter informação sobre determinado assunto (RAMPAZZO, 2005, p. 110). Quanto à forma, considera-se que a entrevista semi-estruturada - definida por Minayo (2009, p, 64) combina perguntas fechadas e abertas oferecendo possibilidades de o entrevistado discorrer sobre o tema – será útil na coleta de dados para identificar ameaças, controles, vulnerabilidade e consequências. A entrevista se dará no ambiente da STI, em local e data a serem acordado com os respectivos gestores. O roteiro da entrevista foi desenvolvido com base no Anexo A da ABNT NBR ISO/IEC 27001 (2013), correspondente aos controles e objetivos de controle de um sistema de gestão de segurança da informação. As perguntas foram tiradas da descrição dos controles existentes no anexo citado. Porém, quando permaneciam dúvidas mesmo após a leitura do controle, recorria-se a uma leitura mais aprofundada obtida por meio da norma ABNT NBR ISO/IEC 27002 (2013), que descreve detalhadamente cada um dos controles. O roteiro da entrevista consiste em 91 perguntas estruturadas por área de cada gestor, sendo 32 perguntas gerais a serem respondidas por todos os gestores, além das específicas: 10 perguntas para o Coordenador de Redes, 16 para o Gerente de Sistemas de Informação, 02 para o Gerente de Base de Dados, 25 para o Gerente de Segurança da Informação e 06 para a Secretária Executiva.

Pretende-se também fazer uso do scanner de vulnerabilidades NetSparker[4], versão 3.1.6.0 da edição comunitária, que consiste em um scanner de segurança em aplicações web, que pode rastrear, atacar e identificar vulnerabilidades em variadas plataformas de aplicações web. Essa ferramenta propõe-se a identificar variadas vulnerabilidades de segurança da Web a partir da varredura do sistema. A abordagem quantitativa da pesquisa abrange a análise numérica dos dados coletados pelo scanner por meio de procedimentos estatísticos, representados graficamente em tabelas e ilustrações. Serão analisados a quantidade e os tipos de vulnerabilidades web encontradas, sendo divididos em cinco níveis de criticidade: crítico, alto, médio, baixo e alerta. Os testes de invasão (*Penetration Tests*) serão realizados em três locais diferentes, fora do estado, no mesmo município e dentro da universidade proprietária do sistema SIGAA - *StrictoSensu*, de modo a analisar eventuais divergências de acesso ao sistema considerando o acesso remoto por localidade.

[4] NetSparker é um scanner de vulnerabilidades em aplicações web. Mais detalhes em: https://www.netsparker.com/web-vulnerability-scanner/

2.5 ANÁLISE DOS DADOS

A análise de dados consiste na análise de riscos propriamente dita. Para analisar os dados que serão obtidos nos três momentos do procedimento de coleta, serão utilizados como método os procedimentos indicados pela ABNT NBR ISO/IEC 27005 (2008), tendo como suporte metodológico a ferramenta de gestão de riscos da RNP, construída com base nesse método. A ferramenta de gestão de riscos da RNP consiste em uma planilha que auxiliará na estimativa qualitativa dos riscos do sistema SIGAA - *Stricto Sensu*. A partir da pesquisa documental, mais especificamente das normas da ABNT NBR ISO/IEC 27001 (2013) e ABNT NBR ISO/IEC 27002 (2013), em conjunto com os dados obtidos com as entrevistas, pretende-se fazer uso dessa planilha de modo a calcular os riscos existentes no sistema, para tanto a análise de risco foi divida em etapas. Considerando que as perguntas objetivam identificar as implementações dos controles de segurança da informação existentes para os ativos correspondentes, a partir das respostas poderá ser possível realizar a análise qualitativa de riscos. A análise de risco consistirá nas seguintes etapas:

Na primeira etapa, identificar os ativos ligados ao sistema, será feito um levantamento dos ativos relacionados ao sistema. Na planilha, os ativos identificados serão relacionados com seus respectivos objetivos de controle, de modo que a análise de risco terá como base a relação Ativo/Objetivo de Controle.

A segunda etapa consiste na identificação das ameaças, a partir das respostas da entrevista e tendo como referência o anexo C da ABNT NBR ISO/IEC 27005 (2008) que traz 43 exemplos de tipos de ameaças, que abrangem danos físicos, eventos naturais, paralisação de serviços essenciais, distúrbio causado por radiação, comprometimento da informação, falhas técnicas, ações não autorizadas e comprometimento de funções. Ao fim dessa etapa, se identificará as ameaças as quais cada um dos ativos levantados está sujeito, porém observa-se que é comum as ameaças afetarem mais de um ativo (BEZERRA, 2013, p. 47-54)

Na terceira etapa, identificação dos controles, considerando-se que as perguntas foram categorizadas por controle e objetivo de controle e que os ativos foram identificados por objetivo de controle, a partir das respostas poderá se identificar os controles existentes ou planejados. Ao fim dessa etapa os controles de cada ativo terão sido identificados e analisados, a partir das respostas da entrevista, quanto a sua existência.

A quarta etapa, identificação das vulnerabilidades, pretende-se levantar as vulnerabilidades, não atendidas pelos controles existentes e que podem vir a comprometer a segurança do sistema, através de dois olhares: visão interna, onde se pretende identificar como o pessoal interno poderia comprometer o sistema; e visão externa, de modo a identificar o que pode ser explorado de modo a conferir privilégios não permitidos. O Netsparker irá contribuir na identificação das possíveis vulnerabilidades técnicas do sistema. Ao final desta atividade pretende-se ter uma lista de vulnerabilidades associadas aos ativos, ameaças e controles.

Na quinta etapa, identificação das consequências, para cada vulnerabilidade será identificada uma consequência de uma lista predefinida composta por: perda da confidencialidade; perda da integridade; perda da disponibilidade; perda da autenticidade; prejuízo financeiro por retrabalho; e afeta a imagem e reputação.

A sexta etapa, avaliação das consequências, pretende avaliar os impactos sobre os ativos do sistema, considerando as consequências de uma violação à segurança da informação. Desse modo, deve ser identificada, nesta etapa, a relevância do ativo para determinar o impacto em um cenário de incidente, de acordo com a perda das propriedades de segurança da informação (confidencialidade, integridade, disponibilidade e autenticidade), prejuízo financeiro ou conseqüência na imagem da organização. Se houver perda de pelo menos quatro tipos de consequências, considera-se o ativo crítico, caso seja de três tipos de consequências, o ativo é importante, quando houver perca dois tipos, o ativo será significante, caso se perca apenas um tipo de consequência, o ativo será considerado de baixa relevância, e se o prejuízo for apenas na imagem da organização, a relevância do ativo será considerada insignificante. A severidade das consequências demonstra o grau das consequências sofridas por um ativo, em relação aos serviços, ao ser atacado ou parar de funcionar. Logo, nesta etapa também será identificada a severidade de cada consequência anteriormente levantada sobre determinado ativo e sua relevância para o sistema em estudo. A resposta será dada de acordo com os critérios de consequência: insignificante (peso 1), baixa (peso 2), média (peso 3), alta (peso 4) e elevada (peso 5).

Na sétima etapa, avaliação qualitativa das probabilidades, para a estimativa da probabilidade de ocorrência de incidentes, as vulnerabilidades serão levadas em conta, individualmente e em conjunto, e os controles existentes considerando a eficiência e eficácia com que reduzem as vulnerabilidades. Os critérios de probabilidade representam o percentual de chance de um evento ocorrer, para a presente pesquisa se adotará os critérios de improvável, remoto, ocasional e provável.

Na oitava etapa, resultado das estimativas, será calculado o impacto, o qual consiste no índice para mensurar o montante dos danos, ou custos à organização, causado pela ocorrência de um evento de segurança da informação. A ferramenta irá calcular o impacto baseada na fórmula: Impacto = Relevância do Ativo X Severidade das Consequências.

A ferramenta faz uso da inserção de pesos em cada critério visando facilitar o cálculo dos riscos permitindo que sejam ordenados por criticidade (Quadro 1).

Quadro 1 – Nível de Impacto

Nível	Peso	Cálculo
Desprezível	1	5
Baixo	2	10
Significativo	3	15
Importante	4	20
Desastre	5	25

Fonte: Dados da pesquisa (2015)

A última etapa, cálculo do risco, será feito o cálculo do risco de forma automatizada pela ferramenta considerando a probabilidade da vulnerabilidade ser explorada e o impacto anteriormente calculado (Quadro 2). O cálculo do risco se baseia na fórmula: Risco = Probabilidade da Vulnerabilidade ser Explorada X Impacto

Quadro 2 – Nível de Risco

Nível	De	Até	Prioridade
Extremo	81	100	1
Alto	49	80	2
Médio	19	48	3
Baixo	5	18	4
Irrelevante	1	4	5

Fonte: Dados da pesquisa (2015)

Ao fim dessa análise de riscos pretende-se ter uma estimativa dos riscos existentes relacionados ao sistema objeto da pesquisa, possibilitando sugerir melhorias para que o sistema funcione de forma segura e eficiente.

REFERÊNCIAS

AIRMIC; ALARM; IRM. **A Risk Management Standard**. London, United Kingdom: Airmic, Alarm, Irm, 2002.

ARAÚJO, Wagner Junqueira de. **A segurança do conhecimento nas práticas da gestão de segurança da informação e da gestão do conhecimento**. 2009. 280 f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005**: tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

_____. **NBR ISO/IEC 27001**: Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro, 2013.

_____. **NBR ISO/IEC 27002**: . tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

BEZERRA, Edson Kowask. **Gestão de riscos de TI**: NBR 27500. Rio de Janeiro: RNP/ESR, 2013.

BHATTACHERJEE, Anol. Social science research: principles, methods, and practices. **Textbooks Collection**, Florida, v. 3, 2012.

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDE DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL (CTIR Gov). **Estatísticas de incidentes de rede na apf – ano 2014.** Brasil: CTIR/DSIC/GSI/PR, 2015. Disponível em: <http://www.ctir.gov.br/estatisticas.html>.

DANTAS, Marcus Leal. **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

FREIRE, Gustavo Henrique. Ciência da informação: temática, histórias e fundamentos. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 11, n. 1, p. 6-19, 2006.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6 ed. São Paulo: Atlas, 2012.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. **Livro Verde**: Segurança Cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

MCGEE, James V.; PRUSAK, Laurence. **Gerenciamento estratégico da informação.** Elsevier Brasil, 1994.

MINAYO, Maria Cecília de Souza. (Org). **Pesquisa social:** teoria, método e criatividade. 28 ed. Petrópolis: Vozes, 2009.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

RAMPAZZO, Lino. **Metodologia científica**: para alunos de graduação e pós-graduação. Edições Loyola, 2005.

SAMPIERI HERNÁNDEZ, Roberto; COLLADO FERNÁNDEZ, Carlos; LUCIO BAPTISTA, Pilar. **Metodologia de pesquisa**. São Paulo: McGraw-Hill, 2006.

TITTEL, Ed; STEWART, James M.; CHAPPLE, Mike. **CISSP**: certified information systems security professional study guide. New Jersey: John Wiley & Sons, 2006.

TRIBUNAL DE CONTAS DA UNIAO (TCU). **Relatório de avaliação da governança de tecnologia da informação na administração pública federal**. Brasília: TCU, 2014.

UNIVERSIDADE FEDERAL DA PARAÍBA (UFPB). **Resolução n^{O} 32 de 2014**: Institui a política de segurança da informação da UFPB, normatiza procedimentos com esta finalidade e dá outras providências. João Pessoa, 2014. Disponível em: <http://www.ufpb.br/sods/consuni/resolu/2014/Runi32_2014.pdf>. Acesso em: 20 mar. 2015.

_____. Resolução nº 40 de 2013 de 12 de Dezembro de 2013: Cria a Superintendência de Tecnologia de Informação(STI), como órgão auxiliar de Direção Superior da Reitoria da Universidade Federal da Paraíba, e aprova seu Regimento. João Pessoa, 2013. Disponível em: < http://www.ufpb.br/sods/consuni/resolu/2013/Runi40_2013.pdf>. Acesso em: 25 mar. 2015.