XIV Encontro Nacional de Pesquisa em Ciência da Informação (ENANCIB 2013)
GT 4: Gestão da Informação e do Conhecimento nas Organizações

Comunicação Oral

ANÁLISE DE RISCO NO SISTEMA DE CONCESSÃO DE DIÁRIAS E PASSAGENS (SCDP): ESTUDO DE CASO SOB A ÓTICA DA SEGURANÇA DA INFORMAÇÃO NO DEPARTAMENTO CONTÁBIL DA UFPB

Josivan de Oliveira Ferreira – UFPB
Wagner Junqueira de Araújo - UFPB

Resumo
O poder da tecnologia tem gerado sistemas informatizados para a execução das mais diversas tarefas, com suas bases de dados interligadas por meio de poderosas redes. O governo federal, visando instrumentalizar eficientemente o serviço público, implantou o Sistema de Concessão de Diárias e Passagens (SCDP), que integra as atividades de concessão, registro, acompanhamento, gestão e controle de diárias e passagens, decorrentes de viagens realizadas com o interesse da administração. Esse meio, repleto de conteúdos e de esferas digitais interligados, está sujeito a diversos tipos de ameaças físicas ou virtuais que comprometem a segurança dos seus usuários e das informações processadas. O presente estudo tem como objetivo geral analisar, sob a ótica da gestão da segurança da informação, o SCDP do Departamento Contábil da Universidade Federal da Paraíba. Procura investigar a garantia de confidencialidade, da integridade e da disponibilidade da informação, através de uma análise de risco nos elementos e nos documentos que integram o sistema. No aspecto metodológico, a pesquisa é caracterizada como um estudo de caso, de caráter qualitativo e quantitativo, exploratório e descritivo. Utiliza como instrumentos de coleta de dados a entrevista estruturada, que permitiu reconhecer ações de uma Política de Segurança da Informação (PSI) por meio do *Facilitated Risk Analysis and Assessment Process* (FRAAP), e a técnica de observação direta, realizada por meio de anotações em diário de campo. Para organizar e analisar os dados, recorreu-se à análise de conteúdo. Com os resultados obtidos, foi possível identificar aspectos do SCDP como: a influência na visão dos usuários, os elementos de segurança e o fluxo informacional. Em relação à análise de risco efetuada, concluiu-se que existem ameaças no processo de concessão de diárias e de passagens, mas, com a adoção de controles selecionados, é possível diminuir o risco.
Palavras-chave: Gestão da segurança da informação. Ciência da Informação. Política de segurança da informação. Análise de risco. Sistema de Concessão de Diárias e Passagens-SCDP.

RISK ANALYSIS ON THE SISTEMA DE CONESSÃO DE DIÁRIAS E PASSAGENS (SCDP): CASE STUDY IN THE PERSPECTIVE OF INFORMATION SECURITY MANAGEMENT IN THE UFPB ACCOUNTING DEPARTMENT

Abstract
The power of technology has generated computerized systems for implementation of various tasks with their databases linked through powerful networks. The federal government aimed at equipping public service efficiently deployed Sistema de Concessão de Diárias e Passagens (SCDP) that integrates the activities of grant, registration, monitoring, management and control of daily and passages, resulting from trips taken in the interest of administration. This environment full of content and digital interconnected spheres is subject to various types of

physical or virtual threats that jeopardize the safety of its users and the information processed. The present study aims at analyzing the perspective of the management of information security, the SCDP accounting department at the Universidade Federal da Paraíba. Investigates the assurance of confidentiality, integrity and availability of information through a risk analysis of the evidence and documents that comprise the system. In the methodological aspect, the research is characterized as a case study, set up as a study of qualitative and quantitative, exploratory and descriptive. Used as instruments to collect data to structured interview that recognized actions of a Security Policy Information (PSI) through the Facilitated Risk Analysis and Assessment Process (FRAAP), and direct observation technique, performed by notes in a field journal. For organizing and analyzing the data, we used content analysis. With these results it was possible to identify aspects of SCDP as the influence on the view of users, the security features and information flow. Regarding the risk analysis carried out, it can be concluded that there are threats in the process of granting and daily tickets, but with the adoption of selected controls can mitigate risk.
Keywords: Information security Management. Information Science. information security Policy. Risk analysis. Sistema de Concessão de Diárias e Passagens-SCDP.

1 INTRODUÇÃO

As organizações dependem cada vez mais dos sistemas informatizados para executar as mais diversas tarefas. A integração desses sistemas com as bases de dados acontece por meio de redes.

O grande poder da tecnologia dos computadores tem gerado poderosas redes de comunicação que as organizações podem utilizar para acessar vastos arquivos de informações, no mundo inteiro, e coordenar atividades, independentemente do espaço e do tempo. Essas redes estão transformando o modelo e a forma das empresas. Em relação ao setor público, o uso de sistemas de informação com tecnologia é cada vez mais amplo, pois, devido à diminuição significativa dos custos em equipamentos de informática, é possível direcionar investimentos e instrumentalizar o gestor, fazendo com que os serviços prestados à população sejam mais eficazes e mais bem fiscalizados.

Nesse novo panorama de gestão, o Governo Federal implantou o Sistema de Concessão de Diárias e Passagens (SCDP), que integra as atividades de concessão, registro, acompanhamento, gestão e controle das diárias e das passagens, decorrentes de viagens realizadas por interesse da administração. Esse sistema do Ministério do Planejamento, Orçamento e Gestão permite o acompanhamento sistemático e em tempo real da concessão de passagens e diárias fornecidas a servidor, convidado, colaborador eventual e assessor especial.

Os órgãos da administração pública federal, direta, autárquica e fundacional tiveram que se adaptar ao SCDP até 31 de dezembro de 2008, conforme o artigo 2º do Decreto nº 6.258, de 19/11/2007. A Universidade Federal da Paraíba, em cumprimento a esse disposto,

adotou todos os procedimentos para sua implantação em seus diversos centros de ensino espalhados pelos sete campi. Trata-se de uma organização federalizada há 56 anos, que se expandiu nos últimos anos.

Diante do rápido processo de crescimento da UFPB, local de estudo deste trabalho, acredita-se que a gestão de segurança da informação pode contribuir para o processo de modernização da Instituição, que requer, cada vez mais, priorização de modelos que contemplem a geração de informação com integridade, confidencialidade e disponibilidade. Nessa perspectiva, baseia-se numa visão antecipada de proteção que é exigida, logo após o suprimento das necessidades de aquisição e utilização dos recursos da informação.

O SCDP trouxe recursos inéditos para a UFPB, entre eles, a tramitação eletrônica de documentos e a exigência de um certificado digital vinculado à infraestrutura de chaves públicas - ICP – Brasil, para aprovação de viagens e pagamento de diárias. No entanto, esse meio, repleto de conteúdos digitais interligados, está sujeito a diversos tipos de ataques físicos ou virtuais, razão por que é necessária uma metodologia que oriente ações futuras, empregando-se recursos, técnicas e ferramentas necessárias para a segurança dos usuários e das informações processadas.

Em um setor que desenvolve atividades-meio da Instituição, como a Contabilidade, incorporar uma gestão de segurança da informação aos seus serviços representa uma atuação mais confiável de seu objetivo, que é de prover os interessados com informações sobre aspectos de natureza econômica, financeira e física do patrimônio da empresa e suas mutações.

Laudon (2004) enfatiza que cada empresa tem uma cultura peculiar ou um conjunto fundamental de premissas, valores e modos de fazer as coisas aceitas pela maioria de seus membros. No entanto, os diferentes níveis e as especialidades presentes numa organização criam interesses e pontos de vista que, muitas vezes, são conflitantes. É por isso que a maior parte dos obstáculos que podem surgir no estabelecimento de uma política de segurança está relacionada ao fator humano (ALBERTIN; PINOCHET, 2010, p. 80).

Embora os controles de segurança tecnológica apresentem eficiência no combate aos diferentes tipos de risco advindos da Internet, o elemento humano é sempre um componente sobremaneira importante para solucionar problemas de segurança. É necessário que os usuários cooperem e compreendam que é importante alcançar o nível desejável de segurança, o que exige, nesse caso, um programa de conscientização na organização. Os usuários que desconhecem os controles ou que são resistentes a eles tornam-se pontos fracos que podem resultar em incidentes de segurança (ALBERTIN, 2010, p. 110).

Com o olhar para essa temática, percebeu-se que o universo de Setores de Atividades-meio da UFPB é amplo, composto por diversos centros acadêmicos com distancias físicas consideráveis. Cada setor contábil distribuído no campus tem, pelo menos, um servidor usuário do SCDP que precisa ter um pensamento único em relação ao manuseio da informação para haver segurança do sistema. Assim, o estudo procurou responder ao seguinte questionamento: Como o uso do Sistema de Concessão de Diárias e Passagens por diversos usuários, na contabilidade da Universidade Federal da Paraíba, garante a segurança das informações contidas nos documentos que nele são processados? Portanto, a pesquisa teve como objetivo geral: **Analisar o Sistema de Concessão de Diárias e Passagens, sob a ótica da gestão da segurança da informação, no âmbito do Campus I da Universidade Federal da Paraíba.**

Este estudo se justificou porque ainda são escassas as pesquisas realizadas em Setores de Atividade-meio das Instituições de Ensino Superior no Brasil, notadamente nas IFES e objetiva evidenciar nas atividades do SCDP, como estas estão fazendo uso das políticas de segurança da informação nos seus setores contábeis. Contribuiu para o desenvolvimento esse assunto e gerou a oportunidade de oferecer resultados práticos à universidade para ajudar em seu planejamento estratégico e a continuidade dos seus serviços.

As bases teóricas refletidas nesse estudo tiveram início com os argumentos de Burke (2003), que contribuíram para destacar a importância da informação no decorrer da história, durante a idade média e moderna, enquanto à pós-modernidade, a definição de Hall (2001) para a globalização, indica que este fenômeno trouxe implicações relacionadas ao requisito da segurança. Em seguida, os autores Otlet (1934) e Borko (1968) contribuíram com as colocações relativas às origens da Ciência da Informação, no que diz respeito à documentação e ao fluxo da informação, com os meios de processamento para torná-la acessível e usual. A partir desse ponto, fez-se uso dos conceitos para sistema de informação atribuídos por O'Brien (2004), Turban (2005) e Stair (2006) que provocaram uma necessidade de diferenciar os termos referente a dado e a informação, cuja distinção obteve apoio nos pensamentos de Davenport (1998). Os temas e autores abordados foram referências para abordagem dos tópicos relativos à gestão da segurança da informação e à análise de risco. O primeiro tópico descreveu esse tipo de modelo de gestão na visão de Sêmola (2003) e Beal (2011), onde confirmam o objetivo em garantir a informação dentro dos padrões de sigilo, integridade e disponibilidade. Os autores Albertin (2010) e Araújo (2009) auxiliaram no suporte ao tema gestão da segurança da informação, salientando a importância que as organizações devem atribuir a esse assunto, pois requer o planejamento de uma política cuidadosa e atenta a

detalhes. Em relação à temática de gestão e análise de risco, Peltier (2005) acentua que a análise de risco permite a uma organização assumir o controle de seu próprio destino, onde apenas os métodos e garantias realmente necessárias, serão utilizados para o controle das ameaças e vulnerabilidades à segurança informação.

2 PROCEDIMENTOS METODOLÓGICOS E CARACTERIZAÇÃO DA PESQUISA

Esta pesquisa teve como foco efetuar uma análise sob a ótica da Segurança da Informação, a partir do diagnóstico das ações exercidas pelos usuários do SCDP do departamento contábil da Universidade Federal da Paraíba.

O tipo da pesquisa enquadra-se como um estudo de caso, pela análise de um fenômeno contemporâneo, relacionado à segurança da informação em uma organização pública real, objetivando encontrar respostas para um problema existente (YIN, 2005, p. 32).

Uma das vantagens do Estudo de Caso é de que as evidências podem ser coletadas mediante várias técnicas, tais como: observação, observação participante, entrevista, grupo focal, questionários, pesquisa documental e pesquisa etnográfica (MULLER, 2007, p. 49).

Para a coleta de dados desta pesquisa optou-se pela entrevista estruturada como instrumento. Trata-se de uma ferramenta que permite: obter informações em um tempo relativamente curto, proporcionar uma tabulação de dados com maior facilidade e rapidez, diminuir o número de abstinência, esclarecer o significado das perguntas, adaptar-se mais facilmente às circunstancias e analisar o ambiente físico pesquisado (GIL, 1999, p. 118).

Gil (1999, p. 121) afirma que a entrevista estruturada desenvolve-se a partir de uma relação fixa de perguntas, com ordem e redação invariável para todos os participantes. Silva (2010, p. 63) complementa, salientando que o teor e a ordem das questões devem ser mantidos para facilitar a comparação das diferenças entre as repostas dos informantes, o que não seria possível se as perguntas fossem modificadas ou se sua sequência fosse alterada.

Com base na literatura metodológica e técnica, o roteiro da entrevista estruturou-se em um formulário padrão de 29 perguntas, cujas três primeiras serviram para identificar os envolvidos apenas quanto ao sexo, função na organização e sua posição em relação à concessão de autorização no sistema SCDP. As demais questões foram alocadas em três categorias que representam os elementos que foram analisados com foco na segurança da informação: pessoas, processos e tecnologia (ALBERTIN et. al., 2010, p. 8).

O universo da pesquisa, segundo Gil (1999, p. 99), representa “um conjunto definido de elementos que possuem determinadas características”. Esses elementos podem ser compostos por seres animados ou inanimados, conforme salienta Silva (2010, p.73). No caso

desta pesquisa, o universo foi composto pelas sete Pró-reitorias e por 13 centros de ensino do Campus I da UFPB. O estudo teve sua amostragem não probabilística por acessibilidade, comumente aplicada em estudos exploratórios, onde não é requerido um elevando nível de precisão (GIL, 1999, p. 101).

A amostra foi composta pelos servidores que manusearam o SCDP, durante o ano de 2012, evidenciados numa relação de movimentação anual, retirada no módulo gerencial do próprio sistema em 04/01/2013. O demonstrativo é formado pelos usuários do SCDP que participaram ativamente de sua movimentação, seja alimentando as informações necessárias para realizar as diárias e/ou viagens ou concedendo autorização para executá-las e pagá-las totalizando trinta indivíduos.

2.1 MODELO ADOTADO COMO PARÂMETRO PARA A ANÁLISE DE RISCO

Para tal atividade, utilizou-se como suporte metodológico o FRAAP - *Facilitated Risk Analysis and Assessment Process* (Processo Facilitado da Análise e Avaliação de Risco). A opção por este modelo se deu por causa do uso de especialistas da própria organização, esse método permite que o processo seja conduzido, em questão de dias, com um custo baixo e benefício alto, e proporciona um nível maior de aceitação por não ser estabelecido através de uma consultoria externa com procedimentos genéricos (PELTIER, 2005, p. 131).

Segundo Peltier (2005, p. 129), o FRAAP é um processo já testado, eficiente e organizado para assegurar que as informações relacionadas à segurança dos riscos nas operações dos negócios sejam detectadas e documentadas, envolvendo a análise do sistema de acordo com a estrutura ou o segmento de atuação de cada organização. O modelo conta com o apoio de pessoas da própria organização, que completam o processo de avaliação de risco. Esses especialistas incluem gestores que estão familiarizados com as necessidades da missão do ativo em análise e com os colaboradores que compreendem detalhadamente as potenciais vulnerabilidades do sistema e controles relacionados (PERLTIER, 2005, p. 130).

Os resultados do FRAAP são um conjunto de documentos que irão identificar as ameaças, priorizá-las em níveis de risco e identificar possíveis controles que ajudarão a reduzir os níveis desse risco. Maiores informações sobre esse método serão abordadas no quinto capítulo desta pesquisa, porquanto ele foi escolhido como parâmetro para a coleta dos dados.

Na realização da avaliação de risco, devem-se considerar as vantagens e as desvantagens dos aspectos qualitativos e quantitativos (PELTIER, 2005, p. 77). Laureno

(2005, p. 74) contribui para a compreensão desses aspectos quando salienta que a análise de risco pode ser

> tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – quanto qualitativa – baseada em know-how, geralmente realizada por especialistas, que têm profundos conhecimentos sobre o assunto.

De acordo com Sêmola (2009, p. 52), o método quantitativo, para fazer análise de risco, é "orientada a mensurar os impactos financeiros provocados por uma situação de quebra de segurança a partir da valoração dos próprios ativos". Araújo (2009, p. 52) salienta que "essa mensuração inclui o valor do recurso, frequência de ameaça, eficácia da proteção, custos da proteção, incerteza e probabilidade, que serão medidos, divididos e atribuídos ao processo".

Quanto à análise qualitativa, Peltier (2005, p. 79) enuncia que há uma priorização dos diferentes elementos de riscos através de uma revisão sistemática das ameaças, que faz com que a equipe estabeleça probabilidades de ocorrência e perdas, em oposição às atitudes que serão concebidas para reduzir esses riscos a um nível aceitável. São muitas as técnicas que poderão ser aplicadas em uma análise qualitativa de risco, entre elas: *brainstorming*; técnica de Delpho; *storyboarding*; grupo focal; *surveys*; questionários; *checklists*; reuniões e entrevistas (ARAÚJO, 2009, p. 52). No quadro 1, abaixo, demonstra-se as semelhanças e as diferenças entre os dois tipos de análise.

Quadro 1 – Análise de risco quantitativa e qualitativa

Propriedade	**Quantitativa**	**Qualitativa**
Análise custo/benefício	sim	não
Cálculos complexos	sim	não
Custos financeiros	sim	não
É objetiva	sim	não
Envolve suposições	baixa	alta
Envolve tempo/trabalho	alta	baixa
Fácil comunicação	alta	baixa
Oferece resultados úteis e significativos	sim	sim
Pode ser automatizada	sim	não
Requer grande volume de informações	alta	baixa
Resulta em valores específicos	sim	não
Usa opiniões	não	sim

Fonte: Adaptado de Araújo (2009, p. 53.)

A principal vantagem do modelo qualitativo é de que sua avaliação prioriza os riscos e identifica as áreas de ação imediata e as melhorias. A desvantagem é que não proporciona medições específicas quantificáveis da magnitude dos impactos, e nesse caso, não recomendado

para uma análise de custo-benefício. Mesmo assim, o aspecto qualitativo é mais ágil, pois não requer cálculos complexos para sua realização e, por causa disso, as organizações tendem a aceitá-lo com mais facilidade.

Independentemente do método adotado, uma análise de risco requer atividades como: levantamento dos ativos, definição da lista de ameaças e identificação das vulnerabilidades para, em seguida, sugerir os controles necessários (LAUREANO, 2005, p. 75).

A estrutura da análise de risco desta pesquisa, com base no FRAAP, foi divida em três etapas: identificação das ameaças, estabelecimento do nível de risco e seleção dos controles. A identificação das ameaças efetuou-se após preenchimento do formulário, de forma individual, com os entrevistados que usam o SCDP, para depois serem alocadas nos seguintes grupos: intrusão física, falha de energia elétrica, insuficiência na classificação e no tratamento da informação, fraqueza no uso da senha, pessoas disfarçadas de clientes, preocupações de firewall, vírus de computador, estações de trabalho sem vigilância, falta de treinamento em servidores e ameaças individuais.

Depois da fase da identificação, fez-se uma classificação das ameaças (alta, média ou baixa), de acordo com sua probabilidade de ocorrência, conforme demonstra o quadro 02 empregado como parâmetro.

Quadro 2 – Definições de probabilidades no FRAAP

Termo	Definição
Probabilidade	Chance de que um evento irá ocorrer ou que um valor de perda específica pode ser atingido se o evento ocorrer.
Alta	Muito provável que a ameaça ocorra no próximo ano (acima de 50%).
Média	Possível que a ameaça ocorra no próximo ano (acima de 30% até 50%)
Baixa	Altamente improvável que a ameaça ocorra no próximo ano (até 30%)

Fonte: Peltier (2005, p. 173, tradução nossa, com adaptações)

Em seguida, de acordo com o quadro 03 seguinte, efetua-se uma segunda classificação (alto, médio ou baixo), de acordo com o impacto causado na instituição.

Quadro 3– Definições para impacto no FRAAP

Termo	Definição
Impacto	Uma medida da magnitude da perda ou dano no valor de um ativo da informação
Alta	Missão inteira ou negócio impactado
Média	Perda limitada à única unidade de negócio ou objetivo
Baixa	Negócio como de costume

Fonte: Peltier (2005, p. 173, tradução nossa).

De posse das classificações, preenche-se a tabela "Análise de Risco", que atribui valores de 01 a 03, sendo 1, para baixo, 2 refere-se a médio, e 3 corresponde ao nível alto, tanto para a probabilidade quanto para o impacto.

A coluna referente ao "Nível de risco" da tabela "Análise de Risco" representa a soma dos valores atribuídos às classificações de cada ameaça, feitas de acordo com a probabilidade e o impacto. O total apurado nessa coluna foi aplicado no quadro 04 com os resultados para se achar a matriz do nível de risco que cada ameaça representa para a instituição.

Quadro 4 – Matriz de nível de risco no FRAAP

PROBABILIDADE	IMPACTO			
	Alto	Medio	Baixo	
Alto	A (6)	B (5)	C (4)	
Médio	B (5)	B (4)	C (3)	
Baixo	C (4)	C (3)	D (2)	
A - Ação corretiva tem de ser implementada; B - Ação corretiva deve ser implementada; C – Requer monitoramento; D - Nenhuma ação necessária no momento.				

Fonte: Peltier (2005, p. 174, tradução nossa)

3 COLETA E ANÁLISE DOS DADOS

A coleta de dados começou pela análise das fontes secundárias, como regulamentos, formulários e manuais, a fim de obter mais informações sobre a pesquisa em questão, na perspectiva de ratificar e complementar os dados obtidos por intermédio das fontes primárias. Esses dados foram obtidos mediante o primeiro contato com alguns servidores da instituição, logo após a autorização da Pró-reitoria Administrativa e do coordenador de Contabilidade e Finanças, a partir de 16 de abril de 2012.

A entrevista iniciou-se em 23 de janeiro de 2013, depois que a pesquisa foi aprovada pelo Comitê de Ética do Hospital Universitário Lauro Wanderley. Em relação ao total dos 30 usuários selecionados mediante o uso frequente do sistema em 2012, 66,67 % foi o percentual de participação, ou seja, 20 servidores do Campus I foram entrevistados. Alguns fatores contribuíram para esse percentual, entre eles, a falta de tempo dos escolhidos para o diálogo e o período do ano que correspondeu as férias e provocou a ausência de alguns servidores na instituição.

No processo de apuração dos dados, houve dificuldades para tabular as respostas de múltipla escolha do formulário, porquanto, em pesquisas que envolvem análise de risco são necessárias respostas dicotômicas. As questões dicotômicas são as que proporcionam apenas duas opções de resposta, do tipo: sim/não; concordo/não concordo. Na visão de Cooper et. al

(2001, p. 286), a dicotomia de respostas é apropriada para perguntas que se referem a questões de fato, ou seja, "quando alguma coisa é um fato ou não". No entanto, a falta de alternativas pode provocar dificuldades para algumas pessoas, pois, estando obrigadas a responder duas opções, acabam dando respostas não realísticas. Por isso, com o objetivo de adquirir dados com maior grau de certeza, optou-se por aplicar um formulário que proporcionasse aos entrevistados questões com respostas de múltiplas escolhas. Nesse caso, considerou-se como resposta "Sim", as alternativas "Às vezes" e "Raramente" das questões 9, 10, 12, 18, 19, 21, 22, 23, 24 e 25. Em relação às alternativas "Raramente", "Às vezes", "Às vezes sinto dificuldade", "Não tenho conhecimento" e "Não lembro", das perguntas 11, 13, 14, 15, 16, 20, 25, 27, 28 e 29, corresponderam a "Não" como resposta. Os dados apurados foram organizados em um quadro que possibilitou o tratamento com as alternativas de respostas, cujos dados foram aplicados para a obtenção de informações sobre os níveis de risco no FRAAP.

3.1 ANÁLISE DE RISCO

Para efetuar a análise de risco com foco na segurança da informação nos processos do SCDP, utilizou-se o FRAAP, adaptando-o à realidade da instituição pública pesquisada, o que corrobora o pensamento do próprio autor, que sugere que se aplique um processo de acordo com o negócio da instituição para garantir que os gastos estejam entre aqueles que realmente são necessários (PELTIER, 2005, p. 190).

Encontrados os percentuais para as prováveis ameaças, a etapa seguinte foi detectar a probabilidade de ocorrência de cada ameaça apontada, atribuindo nível alto, para o percentual acima de 50%, nível médio, para aqueles que se enquadraram no intervalo entre 30% e 50%, e baixo, para os resultados que ficaram abaixo de 30%. Quanto ao impacto, atributo necessário para o prosseguimento da análise, tomou-se como base o quadro 3, que define os níveis da magnitude da perda, como baixo, médio e alto. O nível que melhor se adaptou à realidade do SCDP foi o médio, pois, de acordo com Peltier (2005, p. 173), sua perda se limita a uma única unidade de negócio ou objetivo.

Conhecidos os níveis de probabilidade e de impacto das ameaças diagnosticadas nos processos de concessão de diárias e de passagens da UFPB, o próximo passo foi efetuar a soma desses valores, a fim de detectar o estado dos riscos. Nesse caso, os níveis que estiveram na escala 6-5 foram altos, os que deram o valor 4 (quatro), uma média estrutura, e entre 3-2, ficaram os classificados como de nível baixo. Apresentam-se, na tabela 1, os seguintes resultados da análise de risco efetuada.

Tabela 1 – Análise de risco

Grupo de ameaças	Perguntas correspondentes	Aplicação Sim/Não	Probabilidade	Impacto	Nível de risco
			1 = Baixa 2 = Média 3 = Alta	1 = Baixo 2 = Médio 3 = Alto	6 -5 (Alto) 4 (Médio) 3-2 (Baixo)
1. Intrusão física	O setor exige autorização de acesso ao ambiente por pessoas que não sejam servidores da instituição?	Sim	3	2	5 (Alto)
	O setor utiliza-se de identificação pessoal pelo uso de crachás nos servidores?	Sim	3	2	5 (Alto)
2. Falha de energia elétrica	Não aplicado na pesquisa	Não			
3. Classificação e tratamento da informação	Você classifica as informações do SCDP como confidenciais?	Sim	2	2	4 (Médio)
	É preciso armazenar a documentação de forma impressa?	Sim	3	2	5 (Alto)
	As informações físicas podem ser recuperadas em lixeiras ou em outros depósitos?	Sim	2	2	4 (Médio)
	Documentações para diferentes interessados são enviadas num único envelope?	Sim	2	2	4 (Médio)
4. Fraqueza no uso de senha ou sua partilha	As solicitações para novas identificações de usuários e alteração de privilégios são feitas por escrito e aprovadas pela chefia imediata do usuário?	Sim	1	2	3 (Baixo)
	Todos os usuários que desejam usar o SCDP assinam o Termo de Responsabilização e Sigilo por meio do qual concordam com as políticas, os padrões, as normas e os procedimentos do Órgão Público relacionado ao ambiente de TI?	Sim	2	2	4 (Médio)
	Você guarda em local seguro o token que dá acesso ao SCDP?	Sim	1	2	3 (Baixo)
	Você permite que terceiros saibam sua senha de acesso?	Sim	1	2	3 (Baixo)
5. Pessoas disfarçadas de propostos	Em algumas situações, as informações enviadas a terceiros podem ser mal utilizadas?	Sim	2	2	4 (Médio)
6. Preocupações de firewall	Usa outros programas a fim de controlar as informações que são processadas no SCDP?	Sim	2	2	4 (Médio)
	Armazena ou usa programas que não sejam destinados ao objetivo de sua função na instituição?	Sim	2	2	4 (Médio)

Tabela 1 – Análise de risco

Grupo de ameaças	Perguntas correspondentes	Aplicação Sim/Não	Probabilidade	Impacto	Nível de risco
			1 = Baixa 2 = Média 3 = Alta	1 = Baixo 2 = Médio 3 = Alto	6 -5 (Alto) 4 (Médio) 3-2 (Baixo)
7. Vírus de computador	Qual a frequência de atualização do seu antivírus?	Sim	1	2	3 (Baixo)
	O antivírus tem algum custo financeiro?	Sim	3	2	5 (Alto)
	Certifica-se de que o endereço apresentado no navegador corresponde ao sítio que realmente se quer acessar, antes de realizar qualquer ação ou transação?	Sim	1	2	3 (Baixo)
8. Estações de trabalho deixadas sem vigilância	Os papéis de trabalho frequentemente são deixados à vista na mesa de trabalho?	Sim	3	2	5 (Alto)
	É costume, no ambiente de trabalho, deixar o computador ligado com as janelas abertas?	Sim	1	2	3 (Baixo)
	Os equipamentos do setor são suficientes para executar seu trabalho no SCDP?	Sim	2	2	4 (Médio)
9. Treinamento de funcionários	Recebeu orientação sobre a manutenção sigilosa de sua senha de acesso e a responsabilidade envolvida pelo mau uso dela?	Sim	2	2	4 (Médio)
	A alta administração está ciente de que a instituição precisa de um programa eficaz de segurança da informação?	Sim	2	2	4 (Médio)

	Os gestores do centro incentivam uma política de segurança da informação?	Sim	1	2	3 (Baixo)
	Expresse sua opinião sobre a importância de haver na instituição uma ação efetiva dos usuários do SCDP sobre a Política de Segurança da Informação.	Sim	1	2	3 (Baixo)
10. Ameaças individuais identificadas	Procura discutir assuntos de trabalho em ambientes que não sejam da instituição?	Sim	2	2	4 (Médio)

Fonte: Pesquisa direta (2013)

A primeira coluna da tabela sinaliza para 10 grupos que, conforme sugeridos pelo autor, condensam por similaridade o elenco de ameaças encontradas através das questões do formulário aplicado na entrevista (PELTIER, 2005, 195). Esses grupos foram classificados de acordo com a ameaça que, no conjunto, apresentou o maior nível de risco.

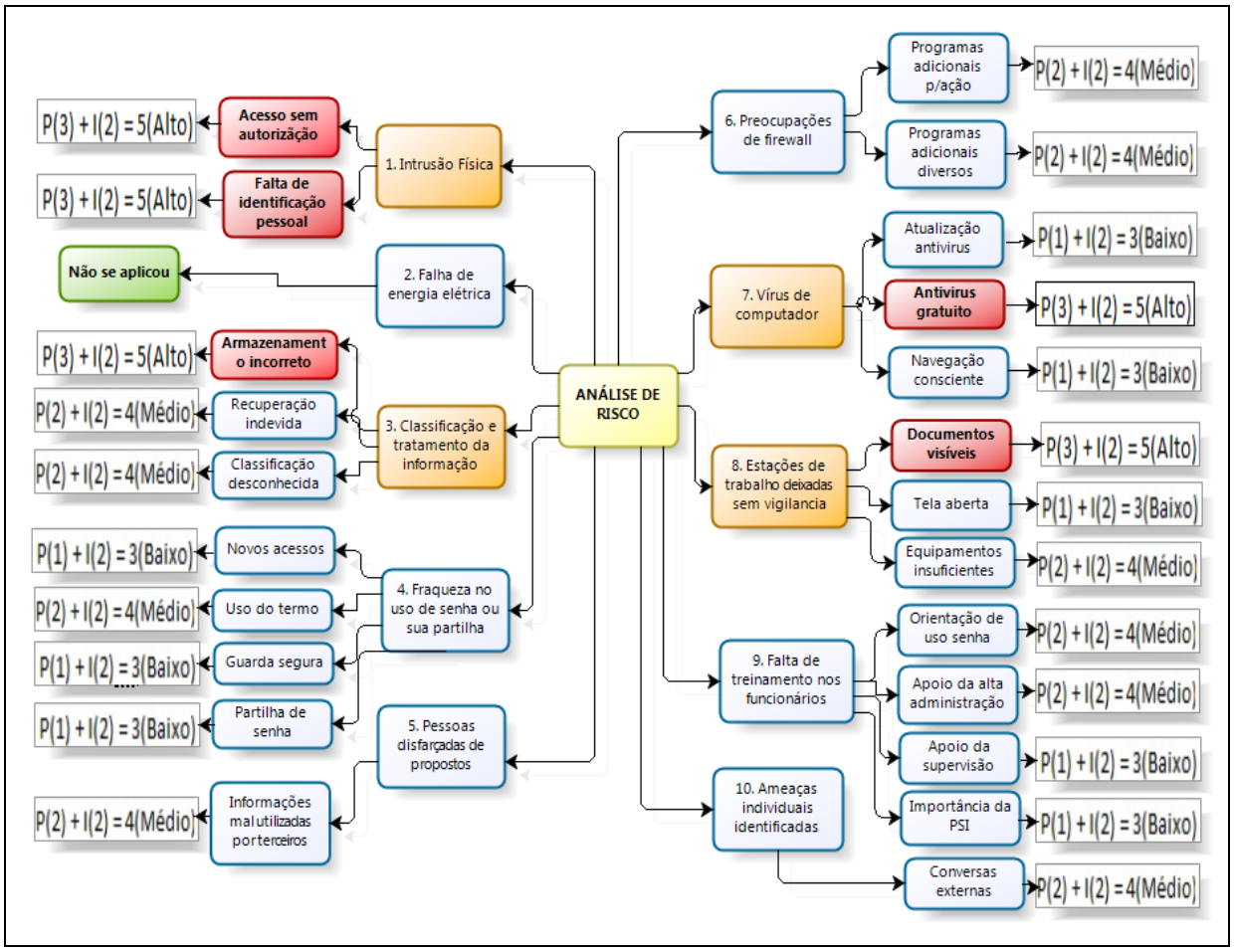
Com base nas informações da última coluna da tabela 1, identificou-se a matriz de risco através do quadro 4, onde: A – a ação tem que ser implementada; B – a ação deverá ser implementada; C – requer monitoramento e D – nenhuma ação é necessária no momento.

A princípio, não houve grupo cujo resultado apresentou risco alto e risco baixo, relacionado, respectivamente, a uma matriz A e D. Todavia, as ameaças classificadas em uma matriz C, relativas a um nível médio de risco, foram: fraqueza no uso de senha ou sua partilha, pessoas disfarçadas de propostos, preocupações de firewall, falta de treinamento de funcionários e ameaças individuais identificadas.

Os grupos da análise que contiveram, pelo menos, uma ameaça com alto nível de risco, apresentando uma matriz B, foram: intrusão física, classificação e tratamento da informação, vírus de computador e estações de trabalho deixadas sem vigilância.

Através do gráfico mental apresentado na figura 1 abaixo, é possível visualizar todo o processo da análise de risco:

Figura 1 – Diagrama mental da análise de risco



Fonte: Elaboração própria no BizAgi (2013)

De forma sequencial, o gráfico mental da análise de risco destaca, na cor laranja, os grupos com alto nível; sucessivamente, nessa mesma classificação, as ameaças, de vermelho, para, no final, demonstrar a equação dos dados resultante da soma das probabilidades (P) com o impacto (I). Através da análise pelo FRAAP, as ações sugeridas para os grupos de média escala envolvem atividades de monitoração, entre elas:

- Propor mais apoio à alta administração do órgão para assegurar a cooperação e a coordenação por todos os servidores da instituição;
- Aderir a uma gestão destinada a mudanças de processos para facilitar uma estrutura de modificação no órgão;
- Formalizar e implementar um programa de conscientização e apresentar aos servidores pelo menos uma vez ao ano;

- Incluir mecanismos de acompanhamento do tipo avaliações de desempenho, relatórios e reuniões, destinados a incentivar, de forma contínua, a conformidade com as políticas e os procedimentos de segurança da informação, tais como:

a) utilização do Termo de Responsabilização e Sigilo junto com todos os usuários do sistema;

b) criação de procedimentos e normas de segurança da informação para distribuir nos setores;

b) conferência na identificação pessoal antes do fornecimento de informações;

c) instalação de aplicativos no computador desde que homologados pela administração de TI;

d) evitar atividades no SCDP em locais externos à UFPB.

Em relação às medidas de controle apropriadas para os grupos de ameaças que resultaram em riscos de alto nível, elaborou-se o quadro 5 para uma visualização direta:

Quadro 5 – Controles sugeridos dos riscos de nível alto

Grupo de ameaças	Ações
1. Intrusão física	Estabelecer um perímetro de segurança física, ou seja, barreiras tais como portões de entrada controlados por cartão, balcões de recepção com recepcionistas, para proteger as áreas onde estejam as informações e os recursos de seu processamento. (ABNT, 2006)
	Criação de pontos de acesso ao público, tais como áreas de entrega e de carregamento, para haver maior controle das pessoas não autorizadas e que esses sejam isolados dos recursos informacionais. (PELTIER, 2005)
	Restringir o acesso não autorizado aos recursos da informação com ênfase na identificação do usuário. (TURBAN, 2004)
3. Classificação e tratamento da informação	Elaboração, pela equipe gestora, de políticas e procedimentos para o apropriado tratamento e armazenamento das informações sigilosas. (PELTIER, 2005)
	Propiciar um treinamento para os usuários do sistema a fim integrar esses procedimentos nas rotinas dos servidores, para que eles compreendam a manipulação dos dados e aplicações com diferentes níveis de classificação. (PELTIER, 2005)
7. Vírus de computador	Instalação do padrão corporativo de software antiviral em todos os computadores; incorporar nas políticas e normas da empresa técnicas de prevenção de vírus, bem como um programa de conscientização entre os envolvidos; uso de *firewall* bem configurado, que bloqueie as portas de entrada (e, se possível, as de saída) usadas por ele.
8. Estações de trabalho sem vigilância	Adoção de "uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação" (ABNT, 2006, p. 32).
	É importante uma política de conscientização para os padrões de conduta profissional que envolvam a proteção, a privacidade e a confidencialidade de todas as informações confiadas aos usuários do sistema (O'BRIEN, 2004, p.379).

Fonte: Elaboração própria (2013)

4 CONSIDERAÇÕES FINAIS

A vida é intrinsecamente cheia de perigos, reais ou percebidos. Praticamente, tudo o que o homem procura fazer deve ser com base em estudos antecipados, a fim de evitar os ricos que se pode obter com determinada atividade. Em relação à informação, as ameaças são intensas, por compreender um dos principais ativos do patrimônio das organizações. Ela representa a inteligência competitiva dos negócios e o suporte para a continuidade das operações de uma empresa. De acordo com o Centro de Estudos, Reposta e Tratamento de Incidentes de Segurança do Brasil, o ano de 2012 apresentou um total de 466.029 incidentes reportados a esse órgão, que é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet brasileira[1]. Isso representa um aumento de, aproximadamente, 16,65% em relação ao ano anterior. Outros fatores contribuem para o aumento desses riscos, como a concentração de um grande volume de dados num único lugar, a abertura comercial da Internet e o uso disseminado da informática nos diversos setores da sociedade.

Como já referido, o objetivo geral desta dissertação foi analisar o Sistema de Concessão de Diárias e Passagens, sob a ótica da gestão da segurança da informação, no âmbito do Campus I da UFPB. Para se atingir esse objetivo, realizou-se uma pesquisa de campo, através de uma entrevista estruturada com 20 (vinte) usuários do SCDP, em 18 setores do órgão em estudo, bem como uma pesquisa bibliográfica de autores que se utilizam da temática e de fontes secundárias, como documentos oficiais, formulários, relatórios e manuais de sistemas.

Conforme os dados da pesquisa, os entrevistados consideram o SCDP como um sistema de elevada importância para a instituição, cuja informação processada é sigilosa pela maioria. Embora tenham apontado algumas dificuldades de processamento, nada impediu que os resultados fossem satisfatórios quando questionados sobre o atendimento das necessidades da organização pelo sistema. Também houve relatos que apontaram o SCDP como um mecanismo confiável de controle e meio eficiente para a transparência das ações do governo.

Verificou-se a existência da certificação digital que representa um mecanismo capaz de garantir a autenticidade, a confidencialidade e a integridade às informações eletrônicas, incluindo a guarda segura de documentos. Para a instalação desse mecanismo na UFPB, o órgão precisou cumprir vários procedimentos relacionados aos padrões da Infraestrutura de Chaves Públicas Brasileira (IPC-Brasil), o que permitiu a alguns usuários a função de

---

[1] Estatísticas dos Incidentes Reportados ao CERT.br. Núcleo de Informação e Coordenação do Ponto BR. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 25 de fevereiro de 2013.

autorizar no sistema, isto os fazem responsáveis por avaliar e analisar os documentos anexados no SCDP. No âmbito da UFPB, esse grupo é formado pelos seguintes profissionais: Reitor, Pró-reitor, Coordenador de Administração, Coordenador de Contabilidade e Finanças, Coordenador de Orçamento e Diretores de Centros Acadêmicos.

A partir do momento em que se mapeou o fluxo informacional do sistema, foi possível visualizar a existência de vulnerabilidades capazes de acarretar em brechas para um ataque aos documentos impressos, cujas informações serviram de base para formular as questões das abordagens de campo. Contatou-se que, embora o sistema permita a transferência eletrônica de documentos, a documentação impressa ainda é necessária e tramita em oito estações de trabalho diferentes. Porém, devido à estrutura de certificação digital, não há impedimento para que o processo seja ágil.

No que diz respeito à análise de risco, tomou-se como base o modelo FRAAP sugerido por Peltier (2005), direcionando a análise para 10 (dez) grupos de ameaças avaliadas pela aplicação de um formulário com 29 perguntas. Em seguida, classificaram-se as ameaças de acordo com os parâmetros de probabilidade e impacto, cujo resultado possibilitou que fosse encontrada a matriz de risco que determina a exigência de ações de monitoramento e de correção.

Em relação às ações de correção, alguns pontos-chave que devem ser observados com mais atenção e que, com base nesta pesquisa, emergiram como contribuições para a instituição ter sucesso nesse processo foram:

- Estabelecer um perímetro de segurança física através de barreiras às áreas que contêm as informações e o uso de métodos para identificação pessoal nos servidores;
- Implantar políticas e procedimentos para o apropriado tratamento e armazenamento das informações sigilosas, bem como o treinamento dos usuários do sistema para haver uma integração dos novos procedimentos em suas rotinas;
- Estabelecer uma política de conscientização para que os padrões de conduta profissional conduzam a proteção da privacidade e confidencialidade das informações confiadas aos usuários do SCDP.

A segurança da informação nos documentos processados pelo SCDP não é tarefa fácil de ser garantida. É necessário que haja um perfeito funcionamento nos recursos, que envolvam pessoas, processos e sistemas de informação. Sua busca deve ser um ato contínuo no contexto da universidade, sustentando as iniciativas dos dirigentes e responsáveis pela Tecnologia da Informação e buscando conscientizar os usuários para que o ato da segurança se torne um hábito.

Os riscos sempre existirão e, por menores que sejam, procurarão derrubar as medidas de proteção. Uma análise de risco não os elimina totalmente, pois sua utilização serve como ferramenta capaz de reduzir o risco a um nível aceitável. Portanto, para haver garantia da segurança, é imprescindível que os procedimentos para que ela ocorra sejam organizados e melhorados para atuarem com exatidão.

É importante ressaltar que este trabalho não exaure o assunto. Futuras pesquisas poderão explorar outros sistemas críticos da universidade e realizar um estudo sobre a cultura de segurança da informação nas organizações desse segmento. Abre-se, também, a possibilidade de ampliar a amostra deste estudo com base no modelo proposto para outras instituições de ensino superior, públicas ou privadas, independentemente do seu porte.

REFERÊNCIAS

ALBERTIN, A. L. **Pesquisa FGV-EAESP de Comércio Eletrônico no Mercado Brasileiro**. 12. Ed. São Paulo: FGV-EAESP, 2010.

ALBERTIN, Alberto Luiz; PINOCHET, Luis Hernan Contreras. **Política de segurança de informações: uma visão organizacional para sua formulação**. São Paulo: Elsevier, 2010.

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

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 27001**: Tecnologia da informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação - Requisitos. Rio de Janeiro, 2006.

BEAL, Adriana. **Gestão Estratégica da Informação:** como transformar a informação e a tecnologia da informação em fatores de crescimento de alto desempenho nas organizações – 5. reimp. – São Paulo: Atlas, 2011.

BORKO, H. **Information science: what is it?** American Documentation, Jan. 1968.

BURKE, Peter. **A classificação do conhecimento: currículos, bibliotecas e enciclopédias. In: _____ Uma história social do conhecimento**: de Gutember a Diderot. Rio de Janeiro: Jorge Zahar, 2003. Cap. 5, p.78-108.

BURKE, Peter. **O controle do conhecimento: Igrejas e Estados. In: _____ Uma história social do conhecimento**: de Gutemberg a Diderot. Rio de Janeiro: Jorge Zahar, 2003. Cap. 6, p.109-135.

COOPER, Donald R.; SHENDLER, Pamela S. **Métodos de pesquisa em Administração** – 7ª Ed.- São Paulo: Artmed Editora S.A., 2001.

DAVENPORT, T. H. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação**. São Paulo: Futura, 1998.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Editora Atlas, 1999.

HALL, Stuart. **Globalização. In: _____. A identidade cultural na pós-modernidade**. Rio de Janeiro: DP&A, 2001. p. 67-89.

LAUDON, Kenneth C.; LAUDON, Jane P. **Sistemas de informação gerenciais: administrando a empresa digital**. São Paulo: Prentice Hall, 2004. p. 283 – 289.

MULLER, S. P. M. **Métodos para pesquisa em CI.** Brasília: Thesaurus, 2007.
NIST, Managing Information Security Risk: Organization, Mission, and Information System View; U. S. Department of Commerce, 2011.
O'BRIEN, James A. **Sistemas de informação e as decisões gerenciais na era da internet**; tradução Célio Knipel Moreira e Cid Knipel Moreira – 2ª Ed – São Paulo: Saraiva, 2004.

OTLET, **Paul. Traité de Documentation – Le Livre sur Le Livre**. **– Théorie ET Pratique**, I vol. Bruxelles, Editiones Mundaneum, Palais Mondial, Imp. Van Keerberghen & fils, 1934.

PELTIER, Thomas R. **Information Security Risk Analysis** - 2ª Ed – United States: CRC Press, Taylor & Francis Group, 2005.

RICHARDSON, Roberto Jarry. **Pesquisa Social: métodos e técnicas** – 3ª Ed. São Paulo: Editora Atlas S.A., 1999.

SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, Pilar Baptista. **Metodologia da Pesquisa**. 3ed. São Paulo: McGraw-Hill, 2006.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

SILVA, Antônio Carlos Ribeiro. **Metodologia da pesquisa aplicada à Contabilidade**. Rio de Janeiro: Atlas, 2010.

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de Sistemas de Informação: uma abordagem gerencial.** São Paulo: Pioneira Thompson Learning, 2006.

STONEBURNER, G.;GOGUEN, A.;FERINGA, A. **Risk management guide for information technology systems: recommendations of the National Institute of Standards and Technology**. U. S. Department of Commerce, 2002.

TURBAN, Efraim; RAINER JR, R. Kelly; POTTER, Richard E. **Administração de tecnologia da informação: teoria e prática**; tradução de Daniel Vieira - Rio de Janeiro: Elsevier, 2005 – 2ª reimpressão.

YIN, R.K. **Estudo de caso: planejamento e métodos**. 3. ed. Porto Alegre: Bookman, 2005.